UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Tesis de Licenciatura

ÁLGEBRAS DE HOPF Y APLICACIONES

Emiliano Francisco Acri

Director: Dr. Leandro Vendramin

18 de Noviembre de 2016

Índice general

Agradecimientos

A mi mamá Teresa, que siempre me escuchó cuando le contaba las cosas que me encantaban de la matemática que iba aprendiendo.

A mi papá Oscar, que me apoyó en mi elección de estudiar matemática cuando todos preguntaban: "¿y eso para qué sirve?".

A mi hermana Yanina, compañera de juegos de toda la vida, por soportarme.

A mis abuelos Vicente y María que aunque se fueron temprano me dejaron mucho y los recuerdo con mucho cariño todos los días.

A mi abuelo Francisco que no conocí pero siempre sentí cerca.

A mi abuela Rosa.

A mis amigos, por las charlas delirantes, los escapes y las salidas al teatro. Las conversaciones por Skype a horas intempestivas sin las cuales no hubiese sido posible aprobar más de una materia.

A mis profesores por todo lo que me enseñaron.

A mi director Leandro.

Al jurado por tomarse el trabajo de leer esta tesis.

Al infinito y más allá . . .

Introducción

> ¿Qué le dijo Papá Noel a la biálgebra $K[x]$?
> ¡Hopf, Hopf, Hopf! ¡Fuiste una mala biálgebra
> y no hay antípoda para vos![1]

El objetivo de esta tesis es dar una introducción a los fundamentos de las coálgebras, biálgebras y álgebras de Hopf así como presentar algunas aplicaciones. Para ello, hemos seguido como texto principal el libro de R. Underwood, *Fundamentals of Hopf Algebras*, [Und15]. Incluimos también ejemplos y propiedades de los textos clásicos de M. Sweedler [Swe69] y S. Montgomery [Mon93].

El desarrollo está organizado en cuatro capítulos. En el primero de ellos, comenzamos con un repaso de la construcción del producto tensorial para módulos sobre un anillo R conmutativo con unidad. Damos algunas de las propiedades básicas que serán de suma utilidad en lo sucesivo. Luego, presentamos los conceptos básicos relativos a las coálgebras y sus propiedades. En la última sección vamos a enfocarnos en el tratamiento del dual lineal. Veremos que si C es una coálgebra podemos darle una estructura natural de álgebra a su dual C^*. Sin embargo, la intención de realizar el mismo procedimiento para el dual de un álgebra A fallará. Definiremos entonces el concepto de dual finito A° que sí tendrá una estructura de coálgebra. Cerraremos el capítulo centrándonos en el dual finito del anillo de polinomios sobre un cuerpo $K[x]$ y, como primera aplicación importante, lo identificaremos con la colección de sucesiones recursivas lineales de todos los órdenes.

En el Capítulo 2, nos enfocaremos en el estudio de los espacios vectoriales con estructura de álgebra y coálgebra simultáneamente. Cuando estas estructuras se encuentren ligadas de cierta forma podremos hablar de biálgebras. Veremos que $K[x]$ tiene exactamente dos estructuras de biálgebra. Es como consecuencia de este hecho que podremos multiplicar sucesiones recursivas lineales de dos formas diferentes. Estas dos multiplicaciones son bien conocidas en la literatura especializada: se trata de los productos de Hadamard y Hurwitz. Finalizaremos el capítulo con una aplicación interesante de la teoría de biálgebras a los autómatas finitos, los lenguajes formales y el Teorema de Myhill–Nerode clásico de las ciencias de la computación. Más precisamente, generalizaremos el teorema a una versión algebraica en la cual cierta cierta función jugará el papel del lenguaje y una cierta biálgebra (una "biálgebra de Myhill–Nerode") se comportará como el autómata finito que acepta el lenguaje.

[1] Ver Ejemplo 3.1.5.

Se incluyen varios ejemplos de este tipo de biálgebra. Finalmente, introducimos el concepto de sucesión regular como una generalización de las sucesiones recursivas lineales sobre un cuerpo finito $\mathrm{GF}(p^m)$.

El Capítulo 3 se centra en las álgebras de Hopf (biálgebras con un morfismo adicional conocido como antípoda). Daremos varios ejemplos y propiedades de este tipo de álgebras. Dado que la antípoda es un endomorfismo del espacio vectorial subyacente al álgebra de Hopf, será lícito preguntarnos sobre el orden de dicho morfismo. Daremos una respuesta completa sobre el problema de determinar si la antípoda tiene orden 2.

Por último, el Capítulo 4 tratará exclusivamente sobre varias aplicaciones. Comenzaremos tratando las estructuras cuasitriangulares sobre biálgebras y álgebras de Hopf. Veremos como resultado importante que si H es un álgebra de Hopf cuasitriangular, entonces existe una solución a la versión cuántica de la ecuación de Yang-Baxter (QYBE, por sus siglas en inglés). Como segunda aplicación recordaremos brevemente el grupo de trenzas $\mathbb{B}_3$ en tres cuerdas (presentado mediante dos generadores y una sola relación) para mostrar que un álgebra de Hopf cuasitriangular de dimensión n determina una representación $\rho\colon \mathbb{B}_3 \to GL_{n^3}(K)$ de dimensión n^3 del grupo de trenzas.

La última aplicación relacionará las álgebras de Hopf con las variedades afines. Trabajaremos con el anillo de coordenadas $K[\Lambda]$ de una variedad afín Λ. Mediante el Teorema de la Base de Hilbert y una construcción dada por W. Waterhouse [Wat79, §1.2] identificaremos una variedad afín Λ con la colección de morfismos de K-álgebras $\mathrm{Hom}_{K-\text{álg}}(K[\Lambda], K)$. Esto nos permitirá darle a un objeto eminentemente geométrico como Λ una estructura puramente algebraica. Veremos que esta estructura resultará ser un monoide bajo cierta operación de convolución si el anillo de coordenadas $K[\Lambda]$ tiene estructura de biálgebra y que tendremos un grupo siempre que el anillo de coordenadas sea un álgebra de Hopf.

Capítulo 1

Álgebras y coálgebras

En este primer capítulo vamos a definir las estructuras básicas de álgebra y coálgebra. Para ello, comenzaremos generalizando la construcción del producto tensorial para una colección finita de módulos sobre un anillo conmutativo con unidad. Nos centraremos en el producto tensorial sobre un cuerpo K y daremos la definición de K-álgebra mediante diagramas conmutativos. Esto nos permitirá definir las coálgebras como objetos formados a partir de revertir las flechas de los diagramas que definen las álgebras.

Trataremos después las cuestiones que sobrevienen al considerar el dual lineal de los espacios vectoriales subyacentes. Al dual lineal de toda coálgebra podremos darle una estructura natural de álgebra y veremos que la construcción recíproca no es válida en general (salvo el caso de dimensión finita). Definiremos el dual finito de una K-álgebra para poder construir cierta coálgebra a partir de un álgebra de dimensión infinita.

Finalmente, como aplicación, identificaremos el dual finito del anillo de polinomios $K[x]$ con la colección de sucesiones recursivas lineales sobre K de todos los órdenes.

1.1. Producto tensorial

En esta sección vamos a extender la construcción del producto tensorial $M \otimes_R N$ a una cantidad finita de R-módulos y probaremos que este producto tensorial se puede identificar con los productos tensoriales iterados de forma natural. Para eso fijamos un anillo R conmutativo y con unidad a lo largo de toda esta sección.

Sea $n \geq 2$ un número natural y consideremos una cantidad finita de *R-módulos* $M_1, M_2, \ldots, M_n$. Consideremos además un *R-módulo* A.

Definición 1.1.1. Una función $f\colon M_1 \times M_2 \times \cdots \times M_n \to A$ se dice *R-n-lineal* si para todo índice i, $0 \leq i \leq n$, y para todos $a_i, a'_i \in M_i$, $r \in R$,

(i) $f(a_1, a_2, \ldots, a_i + a'_i, \ldots, a_n) = f(a_1, a_2, \ldots, a_i, \ldots, a_n) + f(a_1, a_2, \ldots, a'_i, \ldots, a_n)$

(ii) $f(a_1, a_2, \ldots, ra_i, \ldots, a_n) = rf(a_1, a_2, \ldots, a_i, \ldots, a_n)$

Definición 1.1.2. Un *producto tensorial de* $M_1, M_2, \ldots, M_n$ *sobre* R es un R-módulo que notamos como $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ junto con una función R-n-lineal

$$f\colon M_1 \times M_2 \times \cdots \times M_n \to M_1 \otimes M_2 \otimes \cdots \otimes M_n$$

tales que para todo R-módulo A y toda función R-n-lineal $h\colon M_1 \times M_2 \times \cdots \times M_n \to A$ existe una única función R-lineal $\tilde{h}\colon M_1 \otimes M_2 \otimes \cdots \otimes M_n \to A$ tal que $\tilde{h}f = h$; es decir, el siguiente diagrama conmuta:

$$\begin{tikzcd}
M_1 \times M_2 \times \cdots \times M_n \arrow[rr, "h"] \arrow[dr, "f"'] & & A \\
& M_1 \otimes M_2 \otimes \cdots \otimes M_n \arrow[ur, dashed, "\tilde{h}"'] &
\end{tikzcd}$$

Notemos que, como todo objeto definido por una propiedad universal, dicho producto tensorial resultará ser único salvo isomorfismo. Por esto, nos referiremos a él como “el” producto tensorial.

Observación. Una notación completa para el *producto tensorial* de la definición anterior debería ser $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n$ pero nosotros omitiremos el subíndice R siempre que el anillo involucrado sea obvio por el contexto.

Recordemos la construcción del producto tensorial. Consideramos el *R-módulo libre* $F\langle M_1 \times M_2 \times \cdots \times M_n\rangle$ con base en el *conjunto* $M_1 \times M_2 \times \cdots \times M_n$. Sea J el submódulo de $F\langle M_1 \times M_2 \times \cdots \times M_n\rangle$ generado por los elementos de la forma

$$(a_1, a_2, \ldots, a_i + a_i', \ldots, a_n) - (a_1, a_2, \ldots, a_i, \ldots, a_n) - (a_1, a_2, \ldots, a_i', \ldots, a_n)$$
$$(a_1, a_2, \ldots, ra_i, \ldots, a_n) - r(a_1, a_2, \ldots, a_i, \ldots, a_n)$$

para todo índice i, $1 \leq i \leq n$, y para todos $a_i, a_i' \in M$, $r \in R$. Consideramos

$$\iota\colon M_1 \times M_2 \times \cdots \times M_n \to F\langle M_1 \times M_2 \times \cdots \times M_n\rangle$$

la inclusión natural y sea

$$s\colon F\langle M_1 \times M_2 \times \cdots \times M_n\rangle \to F\langle M_1 \times M_2 \times \cdots \times M_n\rangle/J$$

el epimorfismo canónico. Tomemos $f = s\iota$. En estas condiciones, veremos que $F\langle M_1 \times M_2 \times \cdots \times M_n\rangle/J$ junto con f es el producto tensorial. La construcción nos dice que f es R-n-lineal. Para ver que se satisface la propiedad universal dada por la Definición 1.1.2 tenemos la siguiente proposición.

Proposición 1.1.3. *El R-módulo $F\langle M_1 \times M_2 \times \cdots \times M_n\rangle/J$ junto con la función f es el producto tensorial de $M_1, M_2 \ldots, M_n$ sobre R.*

Demostración. Veamos que las condiciones de la Definición 1.1.2 se satisfacen. Para eso, consideramos A un R-módulo y $h\colon M_1 \times M_2 \times \cdots \times M_n \to A$ una función R-n-lineal. Definimos un morfismo de R-módulos

$$\phi\colon F\langle M_1 \times M_2 \times \cdots \times M_n\rangle \to A$$

definido como $\phi(a_1, a_2, \ldots, a_n) = h(a_1, a_2, \ldots, a_n)$, para todo $(a_1, a_2, \ldots, a_n) \in M_1 \times M_2 \times \cdots \times M_n$. Dado que ϕ es R-n-lineal, se deduce que $J \subseteq \ker(\phi)$. Por la propiedad universal del cociente, existe un morfismo

$$\tilde{h}\colon F\langle M_1 \times M_2 \times \cdots \times M_n\rangle/J \to A$$

dado por $\tilde{h}((a_1, a_2, \ldots, a_n) + J) = \phi(a_1, a_2, \ldots, a_n) = h(a_1, a_2, \ldots, a_n)$. Ahora, para todo $(a_1, a_2, \ldots, a_n) \in M_1 \times M_2 \times \cdots \times M_n$, resulta que $\tilde{h}s\iota(a_1, a_2, \ldots, a_n) = h(a_1, a_2, \ldots, a_n)$, y entonces, $\tilde{h}f = h$. Más aún, $\tilde{h}$ es único porque

$$\{(a_1, a_2, \ldots, a_n) + J\colon (a_1, a_2, \ldots, a_n) \in M_1 \times M_2 \times \cdots \times M_n\}$$

es un conjunto de generadores de $F\langle M_1 \times M_2 \times \cdots \times M_n\rangle/J$. □

Notación. *Como consecuencia de la Proposición 1.1.3, vamos a notar*

$$F\langle M_1 \times M_2 \times \cdots \times M_n\rangle/J = M_1 \otimes M_2 \otimes \cdots \otimes M_n$$

y notamos las coclases $(a_1, a_2, \ldots, a_n) + J$ *como el* tensor $a_1 \otimes a_2 \otimes \cdots \otimes a_n$.

Proposición 1.1.4. *Sean M_1, M_2 dos R-módulos y sean N_1 un R-submódulo de M_1 y N_2 un R-submódulo de M_2. Entonces,*

$$M_1/N_1 \otimes M_2/N_2 \cong (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2)$$

como R-módulos.

Demostración. Notemos primero que tenemos una función R-bilineal

$$h\colon M_1 \times M_2 \to M_1/N_1 \otimes M_2/N_2$$

dada por $h(a, b) = (a + N_1) \otimes (b + N_2)$. Como $M_1 \otimes M_2$ es un producto tensorial, existe un morfismo de R-módulos

$$\tilde{h}\colon M_1 \otimes M_2 \to M_1/N_1 \otimes M_2/N_2$$

definido como

$$\tilde{h}(a \otimes b) = (a + N_1) \otimes (b + N_2).$$

Es evidente que $N_1 \otimes M_2 + M_1 \otimes N_2 \subseteq \ker(\tilde{h})$, por lo cual, gracias a la propiedad universal del cociente, existe un morfismo de R-módulos

$$\alpha\colon (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2) \to M_1/N_1 \otimes M_2/N_2$$

con $\alpha(a \otimes b + (N_1 \otimes M_2 + M_1 \otimes N_2)) = (a + N_1) \otimes (b + N_2)$. Consideremos ahora la aplicación

$$l\colon M_1/N_1 \times M_2/N_2 \to (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2)$$

dada por

$$l(a + N_1, b + N_2) = a \otimes b + (N_1 \otimes M_2 + M_1 \otimes N_2)$$

para todo $a \in M_1$, $b \in M_2$. Veamos que es una función bien definida. Para ello, consideramos $x = a + n$, $y = b + n'$ para ciertos $n \in N_1$, $n' \in N_2$. Luego,

$$\begin{aligned} l(x + N_1, y + N_2) &= x \otimes y + (N_1 \otimes M_2 + M_1 \otimes N_2) \\ &= (a + n) \otimes (b + n') + (N_1 \otimes M_2 + M_1 \otimes N_2) \\ &= a \otimes b + a \otimes n' + n \otimes b + n \otimes n' + (N_1 \otimes M_2 + M_1 \otimes N_2), \end{aligned}$$

y entonces $l(a + N_1, b + N_2) - l(x + N_1, y + N_2) \in N_1 \otimes M_2 + M_1 \otimes N_2$. Se sigue que l es una función bien definida sobre $M_1/N_1 \times M_2/N_2$. Por la definición de la función l, resulta ser R-bilineal, por lo cual tenemos un morfismo de R-módulos

$$\tilde{l}\colon M_1/N_1 \otimes M_2/N_2 \to (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2)$$

definido como $\tilde{l}((a + N_1) \otimes (b + N_2)) = a \otimes b + (N_1 \otimes M_2 + M_1 \otimes N_2)$. Es claro que $\alpha^{-1} = \tilde{l}$, y entonces $\tilde{l}$ es un isomorfismo y eso completa la prueba. □

Vamos a probar ahora que el producto tensorial satisface una *propiedad asociativa.*

Proposición 1.1.5. *Sean M_1, M_2, M_3 R-módulos. Se tiene un isomorfismo de R-módulos $M_1 \otimes (M_2 \otimes M_3) \cong (M_1 \otimes M_2) \otimes M_3$.*

Demostración. Sea $h\colon M_1 \times M_2 \times M_3 \to (M_1 \otimes M_2) \otimes M_3$ la función definida como $(a_1, a_2, a_3) \mapsto (a_1 \otimes a_2) \otimes a_3$. Veamos que h es lineal en la primera coordenada. Para ello, notemos que

$$\begin{aligned} h(a_1 + a_1', a_2, a_3) &= ((a_1 + a_1') \otimes a_2) \otimes a_3 = (a_1 \otimes a_2 + a_1' \otimes a_2) \otimes a_3 \\ &= (a_1 \otimes a_2) \otimes a_3 + (a_1' \otimes a_2) \otimes a_3 = h(a_1, a_2, a_3) + h(a_1', a_2, a_3). \end{aligned}$$

Además, si $r \in R$, se tiene

$$\begin{aligned} h(ra_1, a_2, a_3) &= (ra_1 \otimes a_2) \otimes a_3 = r(a_1 \otimes a_2) \otimes a_3 \\ &= r((a_1 \otimes a_2) \otimes a_3) = rh(a_1, a_2, a_3). \end{aligned}$$

De forma completamente análoga, se prueba que es lineal en las otras dos coordenadas. Esto nos dice que h es una función R-3-lineal. Como $M_1 \otimes M_2 \otimes M_3$ es un producto tensorial, por la Definición 1.1.2 existe un único morfismo de R-módulos

$$\tilde{h}\colon M_1 \otimes M_2 \otimes M_3 \to (M_1 \otimes M_2) \otimes M_3$$

definido por $a_1 \otimes a_2 \otimes a_3 \mapsto (a_1 \otimes a_2) \otimes a_3$. Claramente, $\tilde{h}$ es un isomorfismo. De forma análoga construimos el isomorfismo

$$\tilde{g}\colon M_1 \otimes M_2 \otimes M_3 \to M_1 \otimes (M_2 \otimes M_3)$$

dado por $a_1 \otimes a_2 \otimes a_3 \mapsto a_1 \otimes (a_2 \otimes a_3)$. Sea ahora

$$\phi\colon M_1 \otimes (M_2 \otimes M_3) \cong (M_1 \otimes M_2) \otimes M_3$$

la composición $\phi = \tilde{h} \circ \tilde{g}^{-1}$ dada por $a_1 \otimes (a_2 \otimes a_3) \mapsto (a_1 \otimes a_2) \otimes a_3$. En conclusión, ϕ es un isomorfismo de R-módulos. $\square$

Cuando hablamos de un *producto tensorial iterado* nos referimos a un producto tensorial cuyos factores son, asimismo, productos tensoriales que a su vez pueden estar formados por productos tensoriales, etc. Por ejemplo, si M_1, M_2, M_3 y M_4 son R-módulos,

$$(M_1 \otimes M_2) \otimes (M_3 \otimes M_4) \quad \text{y} \quad M_1 \otimes (M_2 \otimes M_3) \otimes M_4$$

son productos tensoriales iterados. En cualquier caso, la Proposición 1.1.5 nos da un isomorfismo natural con el producto tensorial de la Definición 1.1.2 mediante la adición de paréntesis. Por ejemplo, tenemos un isomorfismo natural $M_1 \otimes M_2 \otimes M_3 \to (M_1 \otimes M_2) \otimes M_3$ dado por $a_1 \otimes a_2 \otimes a_3 \mapsto (a_1 \otimes a_2) \otimes a_3$. Vamos a ver el caso general, para ello necesitamos un lema previo.

Lema 1.1.6. *Sean $r, s \geq 1$ enteros y sean $M_1, M_2, \ldots, M_{r+s}$ R-módulos. Entonces, se tiene*

$$M_1 \otimes M_2 \otimes \cdots \otimes M_{r+s} \cong (M_1 \otimes M_2 \otimes \cdots \otimes M_r) \otimes (M_{r+1} \otimes M_{r+2} \otimes \cdots \otimes M_{r+s}).$$

Demostración. Procedemos por inducción en s. El caso base $s = 1$ es completamente análogo a la demostración de que $\tilde{h}$ es isomorfismo en la Proposición 1.1.5. Para el paso inductivo, suponemos cierta la propiedad para $s' < s$ y notamos que el caso base dice que tenemos un isomorfismo

$$(M_{r+1} \otimes M_{r+2} \otimes \cdots \otimes M_{r+s-1}) \otimes M_{r+s} \cong M_{r+1} \otimes M_{r+2} \otimes \cdots \otimes M_{r+s}$$

pues sólo separo el último R-módulo. Usando este isomorfismo, tenemos

$$\begin{aligned}&(M_1 \otimes M_2 \otimes \cdots \otimes M_r) \otimes (M_{r+1} \otimes M_{r+2} \otimes \cdots \otimes M_{r+s}) \\ &\qquad \cong (M_1 \otimes M_2 \otimes \cdots \otimes M_r) \otimes (M_{r+1} \otimes M_{r+2} \otimes \cdots \otimes M_{r+s-1}) \otimes M_{r+s}\end{aligned}$$

Usando ahora la hipótesis inductiva, tenemos el isomorfismo con

$$(M_1 \otimes M_2 \otimes \cdots \otimes M_{r+s-1}) \otimes M_{r+s}$$

Usando ahora el caso base nuevamente, probamos el isomorfismo con

$$M_1 \otimes M_2 \otimes \cdots \otimes M_{r+s-1} \otimes M_{r+s}.$$

Y esto concluye la prueba. $\square$

Ahora sí, estamos en condiciones de probar la siguiente proposición:

Proposición 1.1.7. *Sean $M_1, M_2, \dots, M_n$ R-módulos y sea S un producto tensorial iterado de $M_1, M_2, \dots, M_n$. Entonces existe un isomorfismo natural*

$$M_1 \otimes M_2 \otimes \cdots \otimes M_n \cong S.$$

Demostración. Procederemos por inducción en n. El caso base es $n = 2$ que claramente vale pues hay un solo producto tensorial iterado y es el propio producto tensorial. Para el paso inductivo, supongamos cierto el enunciado para cualquier colección de R-módulos $M_1, M_2, \dots M_s$ con $1 \leq s < n$. Debe existir un entero r con $2 \leq r < n$ tal que $S = T \otimes U$ donde T es un producto tensorial iterado de $M_1, M_2, \dots, M_r$ y U es un producto tensorial iterado de $M_{r+1}, M_{r+2}, \dots, M_n$. Esto es así por la definición misma de producto tensorial iterado que nos dice que se trata de un producto tensorial cuyos factores son, a su vez, productos tensoriales. Por la hipótesis inductiva,

$$S \cong (M_1 \otimes M_2 \otimes \cdots \otimes M_r) \otimes (M_{r+1} \otimes M_{r+2} \otimes \cdots \otimes M_n),$$

y entonces, $S \cong M_1 \otimes M_2 \otimes \cdots \otimes M_n$ usando el Lema 1.1.6. □

La Proposición 1.1.7 nos permite "ignorar los paréntesis" y considerar el producto tensorial iterado y el producto tensorial como un mismo objeto en virtud del isomorfismo natural entre ellos. Veamos ahora algunas propiedades sobre las funciones definidas entre productos tensoriales que serán de especial utilidad en lo sucesivo.

Proposición 1.1.8. *Sean $M_1, M_2, \dots, M_n, M'_1, M'_2, \dots, M'_n$ R-módulos y $f_i \colon M_i \to M'_i$, para $1 \leq i \leq n$, morfismos de R-módulos. Entonces existe un único morfismo de R-módulos*

$$f_1 \otimes f_2 \otimes \cdots \otimes f_n \colon M_1 \otimes M_2 \otimes \cdots \otimes M_n \to M'_1 \otimes M'_2 \otimes \cdots \otimes M'_n$$

definido como

$$(f_1 \otimes f_2 \otimes \cdots \otimes f_n)(a_1 \otimes a_2 \otimes \cdots \otimes a_n) = f_1(a_1) \otimes f_2(a_2) \otimes \cdots \otimes f_n(a_n)$$

para cualesquiera $a_i \in M_i$.

Demostración. Existe una función R-n-lineal

$$f_1 \times f_2 \times \cdots \times f_n \colon M_1 \times M_2 \times \cdots \times M_n \to M'_1 \otimes M'_2 \otimes \cdots \otimes M'_n$$

dada por

$$(f_1 \times f_2 \times \cdots \times f_n)(a_1 \times a_2 \times \cdots \times a_n) = f_1(a_1) \otimes f_2(a_2) \otimes \cdots \otimes f_n(a_n)$$

para todo $a_i \in M_i$. Por definición de producto tensorial tenemos un morfismo de R-módulos inducido

$$\tilde{h} \colon M_1 \otimes M_2 \otimes \cdots \otimes M_n \to M'_1 \otimes M'_2 \otimes \cdots \otimes M'_n$$

de la forma

$$\tilde{h}(a_1 \otimes a_2 \otimes \cdots \otimes a_n) = f_1(a_1) \otimes f_2(a_2) \otimes \cdots \otimes f_n(a_n)$$

para todo $a_i \in M_i$. Tomamos entonces $f_1 \otimes f_2 \otimes \cdots \otimes f_n = \tilde{h}$ y eso completa la prueba. □

El siguiente corolario nos será de mucha utilidad para definir lo que se conoce como *álgebra dual de una coálgebra.*

Corolario 1.1.9. *Sea K un cuerpo y sean $V_i, 1 \leq i \leq n$, una colección finita de K-espacios vectoriales. Entonces,*

$$V_1^* \otimes V_2^* \otimes \cdots \otimes V_n^* \subseteq (V_1 \otimes V_2 \otimes \cdots \otimes V_n)^*.$$

Demostración. Consideramos $f_i\colon V_i \to K, 1 \leq i \leq n$, un conjunto de morfismos de K-módulos (es decir, $f_i \in V_i^*, \forall i$). Por la Proposición 1.1.8 tomando $V_i' = K$, para todo i, tenemos un único morfismo de K-módulos

$$(f_1 \otimes f_2 \otimes \cdots \otimes f_n)(a_1 \otimes a_2 \otimes \cdots \otimes a_n) = f_1(a_1) \otimes f_2(a_2) \otimes \cdots \otimes f_n(a_n).$$

Ahora, como $K \otimes_K K \cong K$ mediante el morfismo $r \otimes s \mapsto rs$, tenemos

$$f_1(a_1) \otimes f_2(a_2) \otimes \cdots \otimes f_n(a_n) = f_1(a_1)f_2(a_2) \ldots f_n(a_n) \in K.$$

Esto nos da la inclusión buscada. □

Observación. La contención contraria en el Corolario 1.1.9 para el caso $n > 1$ se tiene si y sólo si cada V_i es un K-espacio vectorial de dimensión finita.

1.2. Álgebra y coálgebra

En esta sección vamos a presentar la definición de álgebra a partir de diagramas conmutativos y compararemos ésta con la definición usual. Trataremos sobre las álgebras cociente y los morfismos de álgebras. A continuación podremos definir las coálgebras como co-objetos de las álgebras construidos invirtiendo todas las flechas de los diagramas que definen a las álgebras. Daremos varios ejemplos de ambas estructuras. Introduciremos una notación especial para la imagen de la comultiplicación debida a M. Sweedler [Swe69] que se conoce como "notación de Sweedler" o "notación sigma". Por último, definiremos coideales, coálgebras cociente y morfismos de coálgebras.

Consideraremos siempre K un cuerpo y el producto tensorial lo haremos sobre K. Notaremos por I_A a la aplicación lineal identidad de A.

Definición 1.2.1. Una *K-álgebra* es una terna (A, m_A, λ_A) que consiste en un K-espacio vectorial A y transformaciones K-lineales $m_A\colon A \otimes A \to A$ y $\lambda_A\colon K \to A$ que satisfacen las siguientes condiciones:

(i) El siguiente diagrama conmuta:

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

La transformación $I_A \otimes m_A \colon A \otimes A \otimes A \to A \otimes A$ viene dada por la asignación $a \otimes (b \otimes c) \mapsto a \otimes m_A(b \otimes c)$ y la aplicación $m_A \otimes I_A$ se define de forma análoga. Equivalentemente, la conmutatividad del diagrama pide que valga la siguiente igualdad para todo $a, b, c \in A$

$$m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(m_A \otimes I_A)(a \otimes b \otimes c) \tag{1.1}$$

(ii) El siguiente diagrama también conmuta:

$$\begin{tikzcd}
A \otimes K \arrow[r, "I_A \otimes \lambda_A"] \arrow[d, "s_2"'] & A \otimes A \arrow[d, "\lambda_A \otimes I_A"] \arrow[dl, "m_A"'] \\
A & K \otimes A \arrow[l, "s_1"]
\end{tikzcd}$$

La transformación $I_A \otimes \lambda_A$ se define como $a \otimes r \mapsto a \otimes \lambda_A(r)$ para todo $r \in K, a \in A$. De forma análoga se define la transformación $\lambda_A \otimes I_A$. Además definimos las aplicaciones s_1 y s_2 como

$$s_1 \colon K \otimes A \to A, r \otimes a \mapsto ra \quad \text{y} \quad s_2 \colon A \otimes K \to A, a \otimes r \mapsto ra.$$

Equivalentemente, estamos pidiendo que para todo $r \in K, a \in A$,

$$m_A(I_A \otimes \lambda_A)(a \otimes r) = ra = m_A(\lambda_A \otimes I_A)(r \otimes a). \tag{1.2}$$

Observación. La transformación m_A se llama **multiplicación** y λ_A es la **unidad**. La Propiedad (1.1) es la **propiedad asociativa** y la (1.2) es la **propiedad de la unidad**.

Recordemos la definición usual de una K-álgebra.

Definición 1.2.2. Una K-*álgebra* es un anillo A con unidad 1_A junto con un morfismo de anillos $\lambda_A\colon K \to A$ que satisface $\lambda_A(r)a = a\lambda_A(r)$ para todo $a \in A, r \in K$. Luego, A es un espacio vectorial sobre K con la multiplicación por escalares dada por

$$ra = \lambda_A(r)a = a\lambda_A(r) \tag{1.3}$$

para todo $r \in K, a \in A$.

Vamos a ver que nuestra definición con diagramas conmutativos no se trata de una nueva sino que es equivalente a ésta.

Proposición 1.2.3. *Las K-álgebras de la Definición 1.2.1 y las de la Definición 1.2.2 coinciden.*

Demostración. Sea A una K-álgebra como en la Definición 1.2.2. Sea $B\colon A\times A \to A$ la función definida por $(a, b) \mapsto ab$ donde ab es la multiplicación del anillo A. Por las propiedades asociativa y distributiva de la multiplicación en A, B resulta ser K-bilineal. Como $A \otimes A$ es un producto tensorial, existe una única transformación K-lineal $m_A\colon A \otimes A \to A$ definida como

$$m_A\left(\sum a \otimes b\right) = \sum B(a, b) = \sum ab.$$

La propiedad asociativa de la multiplicación en A implica que

$$m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(m_A \otimes I_A)(a \otimes b \otimes c)$$

para todo $a, b, c \in A$. Luego, la función m_A satisface la Condición (1.1).

Veamos ahora que el morfismo de anillos $\lambda_A\colon K \to A$ satisface la Condición (1.2). Para $r, s \in K$ se cumple que $\lambda_A(rs) = \lambda_A(r)\lambda_A(s) = r\lambda_A(s)$; luego, λ_A es K-lineal. De (1.3), tenemos que

$$m_A(I_A \otimes \lambda_A)(a \otimes r) = a\lambda_A(r) = ra$$

y

$$m_A(\lambda_A \otimes I_A)(r \otimes a) = \lambda_A(r)a = ra$$

lo que muestra que se cumple la Condición (1.2).

Recíprocamente, supongamos que (A, m_A, λ_A) es una K-álgebra como en la Definición 1.2.1. Definimos la multiplicación en A como $ab := m_A(a\otimes b)$ para $a, b \in A$. Luego, A es un anillo. Por (1.2) para $r \in K, a \in A$,

$$a\lambda_A(r) = ra = \lambda_A(r)a,$$

luego $\lambda_A(K)$ está contenido en el centro de A. Tomando $r = 1_K$, vemos que $1_A = \lambda_A(1_K)$ hace de A un anillo con unidad 1_A. Tomando $a = \lambda_A(s)$ para $s \in K$ vemos que λ_A es morfismo de anillos. Además la multiplicación por escalares en A está definida mediante λ_A y entonces A es una K-álgebra en el sentido de la Definición 1.2.2. $\square$

Como es usual, simplificamos la notación de la K-álgebra (A, m_A, λ_A) escribiendo simplemente A. Diremos que la K-álgebra A es **conmutativa** si

$$m_A \tau = m_A$$

donde τ es el morfismo de **intercambio** (o **twist**) definido por $\tau(a \otimes b) = b \otimes a$ para $a, b \in A$.

Ejemplo 1.2.4. El cuerpo K es una K-álgebra con multiplicación $m_K \colon K \otimes K \to K$ definida por $r \otimes s \mapsto rs$ y unidad $\lambda_K \colon K \to K$ dada por $r \mapsto r$ para todo $r, s \in K$.

Ejemplo 1.2.5. El anillo de polinomios $K[x]$ es una K-álgebra con la multiplicación usual de polinomios y $\lambda_{K[x]} \colon K \to K[x]$ dada por $r \mapsto r1$, para todo $r \in K$.

Ejemplo 1.2.6. Sea G un grupo finito con neutro 1. El anillo del grupo KG es una K-álgebra con m_{KG} definida como $g \otimes h \mapsto gh$ y $\lambda_{KG} \colon K \to KG$ dada por $r \mapsto r1$, para todo $g, h \in G, r \in K$.

Ejemplo 1.2.7. Sea $L = K(\alpha)$ una extensión algebraica de K. L es una K-álgebra con m_L dada por la multiplicación de L y $\lambda_L \colon K \to L$ definida como la inclusión $r \mapsto r$, para todo $r \in K$.

Claramente, las K-álgebras de los Ejemplos 1.2.4, 1.2.5 y 1.2.7 son conmutativas mientras que KG es conmutativa si y sólo si G es abeliano.

Consideremos ahora dos K-álgebras A y B y dotemos a $A \otimes B$ de estructura de K-álgebra con la multiplicación

$$m_{A \otimes B} \colon (A \otimes B) \otimes (A \otimes B) \to A \otimes B$$

dada por

$$\begin{aligned} m_{A \otimes B}((a \otimes b) \otimes (c \otimes d)) &= (m_A \otimes m_B)(I_A \otimes \tau \otimes I_B)(a \otimes (b \otimes c) \otimes d) \\ &= (m_A \otimes m_B)(a \otimes (c \otimes b) \otimes d) \\ &= (m_A \otimes m_B)((a \otimes c) \otimes (b \otimes d)) \\ &= ac \otimes bd \end{aligned}$$

para $a, c \in A$, y $b, d \in B$. La unidad $\lambda_{A \otimes B} \colon K \to A \otimes B$ está dada por

$$\lambda_{A \otimes B}(r) = \lambda_A(r) \otimes 1_B$$

para $r \in K$.

Observación. Una K-álgebra es un anillo A con la adición dada por la suma de A y la multiplicación m_A. Esto nos permite hablar de ideales de una K-álgebra mirando la estructura de anillo inducida.

Proposición 1.2.8. *Sea A una K-álgebra e I un ideal de A. El espacio vectorial cociente A/I es una K-álgebra.*

Demostración. Debemos definir una multiplicación y una unidad en A/I. Consideremos el epimorfismo canónico $s\colon A \to A/I$. La compoosición

$$sm_A\colon A \otimes A \to A/I$$

es una transformación K-lineal definida como $(sm_A)(a \otimes b) = ab + I$. Notemos que $I \otimes A + A \otimes I$ es un subespacio de $A \otimes A$. Tomemos un elemento arbitrario $a \otimes b + c \otimes d \in I \otimes A + A \otimes I$ donde $a, d \in I, b, c \in A$. Como I es un ideal, se tiene que $m_A(a \otimes b + c \otimes d) = ab + cd \in I$. Por lo tanto, $I \otimes A + A \otimes I \subseteq \ker(sm_A)$. Por la propiedad universal del cociente, tenemos una transformación lineal

$$\overline{sm_A}\colon (A \otimes A)/(I \otimes A + A \otimes I) \to A/I$$

definida como

$$\overline{sm_A}(a \otimes b + (I \otimes A + A \otimes I)) = ab + I.$$

Por la Proposición 1.1.4, hay un isomorfismo de espacios vectoriales

$$\tilde{\beta}\colon A/I \otimes A/I \to (A \otimes A)/(I \otimes A + A \otimes I)$$

dado por

$$\tilde{\beta}((a + I) \otimes (b + I)) = a \otimes b + (I \otimes A + A \otimes I).$$

Sea $m_{A/I}$ la composición $\overline{sm_A}\tilde{\beta}$. Veamos ahora que la transformación

$$m_{A/I}\colon A/I \otimes A/I \to A/I,$$

dada por $(a + I) \otimes (b + I) \mapsto ab + I$ sirve como multiplicación. Es decir, debemos verificar que se satisfacen las propiedades asociativa y de la unidad. En efecto, por un lado

$$\begin{aligned} m_{A/I}(I_{A/I} \otimes m_{A/I})(a + I \otimes b + I \otimes c + I) &= m_{A/I}(a + I \otimes bc + I) \\ &= a(bc) + I, \end{aligned}$$

y por otro lado

$$\begin{aligned} m_{A/I}(m_{A/I} \otimes I_{A/I})(a + I \otimes b + I \otimes c + I) &= m_{A/I}(ab + I \otimes c + I) \\ &= (ab)c + I. \end{aligned}$$

Puesto que la multiplicación de A es asociativa, se cumple que $a(bc)+I = (ab)c+I$ y se tiene que $m_{A/I}$ satisface la propiedad asociativa. Veamos esta igualdad con más formalidad:

$$\begin{aligned} a(bc) + I = sm_A(a \otimes bc) &= sm_A(I_A \otimes m_A)(a \otimes b \otimes c) \\ &= sm_A(m_A \otimes I_A)(a \otimes b \otimes c) \qquad \text{por la asociatividad de } m_A \\ &= sm_A(ab \otimes c) = (ab)c + I. \end{aligned}$$

Para definir la unidad, sea $\lambda_{A/I} = s\lambda_A \colon K \to A/I$. Veamos que satisface la propiedad de la unidad usando la propiedad de la unidad para λ_A. Tenemos, por una parte

$$\begin{aligned} m_{A/I}(I_{A/I} \otimes \lambda_{A/I})(a + I \otimes r) &= m_{A/I}(a + I \otimes \lambda_A(r) + I) \\ &= a\lambda_A(r) + I = ar + I = r(a + I), \end{aligned}$$

y por otra

$$\begin{aligned} m_{A/I}(\lambda_{A/I} \otimes I_{A/I})(r \otimes a + I) &= m_{A/I}(\lambda_A(r) + I \otimes a + I) \\ &= \lambda_A(r)a + I = r(a + I). \end{aligned}$$

Luego, $\lambda_{A/I}$ sirve como unidad de A/I. En consecuencia, $(A/I, m_{A/I}, \lambda_{A/I})$ es K-álgebra. $\square$

La K-álgebra A/I es el **álgebra cociente de A por I**.

Definición 1.2.9. Sean (A, m_A, λ_A) y (B, m_B, λ_B) dos K-álgebras. Un *morfismo de K-álgebras* de A en B es una transformación lineal $\phi \colon A \to B$ que satisface:

(i) $\phi(m_A(a \otimes a')) = m_B(\phi(a) \otimes \phi(a'))$ para todo $a, a' \in A$

(ii) $\phi(\lambda_A(r)) = \lambda_B(r)$ para todo $r \in K$.

Observación. La condición (ii) de la definición nos dice que, en particular, $\phi(1_A) = 1_B$.

Vamos a definir ahora objetos duales, en algún sentido, a las álgebras. Los obtendremos, básicamente, invirtiendo todas las flechas en los diagramas que definen a las álgebras. Estos objetos se llamarán "coálgebras". Sea C un K-espacio vectorial. La multiplicación por escalares de C nos da dos transformaciones lineales $s_1 \colon K \otimes C \to C$, $r \otimes c \mapsto rc$ y $s_2 \colon C \otimes K \to C$, $c \otimes r \mapsto rc$ como antes.

Definición 1.2.10. Una *K-coálgebra* es una terna $(C, \Delta_C, \epsilon_C)$ que consiste en un K-espacio vectorial C y transformaciones lineales $\Delta_C \colon C \to C \otimes C$ y $\epsilon_C \colon C \to K$ que satisfacen las siguientes condiciones:

(i) El siguiente diagrama conmuta:

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

La transformación $I_C \otimes \Delta_C \colon C \otimes C \to C \otimes C \otimes C$ viene dada por $a \otimes b \mapsto a \otimes \Delta_C(b)$ y la aplicación $\Delta_C \otimes I_C$ se define de forma análoga. Equivalentemente, la conmutatividad del diagrama pide que valga la siguiente igualdad para todo $c \in C$

$$(I_C \otimes \Delta_C)\Delta_C(c) = (\Delta_C \otimes I_C)\Delta_C(c) \tag{1.4}$$

(ii) El siguiente diagrama también conmuta:

$$\begin{tikzcd}
C \otimes K & C \otimes C \arrow[l, "I_C \otimes \epsilon_C"'] \arrow[d, "\epsilon_C \otimes I_C"] \\
C \arrow[u, "- \otimes 1"] \arrow[ur, "\Delta_C"] \arrow[r, "1 \otimes -"'] & K \otimes C
\end{tikzcd}$$

Las transformaciones lineales $- \otimes 1$ y $1 \otimes -$ se definen como $c \mapsto c \otimes 1$ y $c \mapsto 1 \otimes c$ respectivamente. Equivalentemente, estamos pidiendo que para todo $c \in C$,

$$(\epsilon_C \otimes I_C)\Delta_C(c) = 1 \otimes c, \quad (I_C \otimes \epsilon_C)\Delta_C(c) = c \otimes 1. \tag{1.5}$$

Las transformaciones Δ_C y ϵ_C se llaman **comultiplicación** y **counidad** de la coálgebra C, respectivamente. La Condición (1.4) se conoce como la **propiedad coasociativa** y la (1.5), como la **propiedad de la counidad**.

Observación. Los diagramas que definen a una coálgebra son similares a los que describen a un álgebra invirtiendo todas las flechas y cambiando la unidad y la multiplicación por sus versiones "dualizadas". Notemos que la transformación $1 \otimes -$ es la inversa de $s_1 \colon K \otimes C \to C,\ r \otimes c \mapsto rc$; una situación análoga ocurre con $- \otimes 1$ y s_2.

De forma similar a como definimos un álgebra conmutativa, diremos que una coálgebra C es **coconmutativa** si

$$\tau(\Delta_C(c)) = \Delta_C(c)$$

para todo $c \in C$.

Notación de Sweedler

Introducimos la notación de Sweedler [Swe69, Sección 1.2] para expresar la comultiplicación. Dado $c \in C$, tenemos $\Delta_C(c) = \sum_{i=1}^{n} c_{1i} \otimes c_{2i}$ para algún n natural y $c_{ji} \in C$. Escribiremos en forma resumida

$$\Delta_C(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}$$

suprimiendo el índice i. Dado que $s_1(1 \otimes c) = c = s_2(c \otimes 1)$, la Condición (1.5) en la notación de Sweedler se escribe como:

$$\sum_{(c)} \epsilon_C(c_{(1)})c_{(2)} = c = \sum_{(c)} \epsilon_C(c_{(2)})c_{(1)}. \tag{1.6}$$

Veamos qué ocurre con la Condición (1.4). Sea $c \in C$,

$$\begin{aligned}(I_C \otimes \Delta_C)\Delta_C(c) &= (I_C \otimes \Delta_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) \\ &= \sum_{(c)} c_{(1)} \otimes \Delta_C(c_{(2)}) \\ &= \sum_{(c,c_{(2)})} c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}}.\end{aligned} \tag{1.7}$$

De forma totalmente análoga, tenemos

$$\begin{aligned}(\Delta_C \otimes I_C)\Delta_C(c) &= (\Delta_C \otimes I_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) \\ &= \sum_{(c)} \Delta_C(c_{(1)}) \otimes c_{(2)} \\ &= \sum_{(c,c_{(1)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)}.\end{aligned} \tag{1.8}$$

Por la Condición (1.4), $(I_C \otimes \Delta_C)\Delta_C = (\Delta_C \otimes I_C)\Delta_C$ y, entonces, las expresiones (1.7) y (1.8) deben coincidir. Al valor común de ambas lo notamos por

$$\sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)}.$$

Podemos generalizar la coasociatividad de la misma manera que generalizamos la asociatividad del producto a muchos factores. Notamos por Δ_0 a Δ_C y definimos inductivamente $\Delta_n \colon C \to C^{\otimes(n+2)}$ por $\Delta_n = (\Delta_C \otimes I_C^n)\Delta_{n-1}$ para todo $n \geq 1$ donde $C^{\otimes n}$ denota el producto tensorial de n copias de C. Es decir, comultiplicamos el primer factor después de aplicar Δ_{n-1}. Por la coasociatividad, podemos aplicar la comultiplicación a cualquier factor para llegar al mismo resultado. Notamos ese valor común por

$$\Delta_n(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes \cdots \otimes c_{(n+2)}.$$

Veamos ahora algunos ejemplos de coálgebras.

Ejemplo 1.2.11. El cuerpo K como espacio vectorial es una K-coálgebra con $\Delta_K \colon K \to K \otimes K$ dada por $\Delta_K(a) = a \otimes 1$ y $\epsilon \colon K \to K$, $\epsilon_K(a) = a$. Esta es la **coálgebra trivial**.

Los siguientes dos ejemplos están tomados de [Swe69].

Ejemplo 1.2.12. Sea S un conjunto. Notamos por KS el K-espacio vectorial que tiene al conjunto S como base. Definimos $\Delta_{KS}\colon KS \to KS \otimes KS$ sobre la base como $\Delta_{KS}(s) = s \otimes s$ y $\epsilon_{KS}\colon KS \to K$ como $\epsilon(s) = 1$. Veamos que se cumplen las Condiciones (1.4) y (1.5). Para la primera, notemos que

$$\begin{aligned}(I_{KS} \otimes \Delta_{KS})\Delta_{KS}(s) = (I_{KS} \otimes \Delta_{KS})(s \otimes s) = s \otimes s \otimes s\\ (\Delta_{KS} \otimes I_{KS})\Delta_{KS}(s) = (\Delta_{KS} \otimes I_{KS})(s \otimes s) = s \otimes s \otimes s\end{aligned}$$

para todo $s \in S$. Para la segunda, tenemos

$$\begin{aligned}(\epsilon_{KS} \otimes I_{KS})\Delta_{KS}(s) = (\epsilon_{KS} \otimes I_{KS})(s \otimes s) = 1 \otimes s\\ (I_{KS} \otimes \epsilon_{KS})\Delta_{KS}(s) = (I_{KS} \otimes \epsilon_{KS})(s \otimes s) = s \otimes 1\end{aligned}$$

para todo $s \in S$. Luego, $(KS, \Delta_{KS}, \epsilon_{KS})$ es una coálgebra que suele denominarse **coálgebra tipo grupo** (o *grouplike*) **sobre el conjunto** S.

Ejemplo 1.2.13. Sea $\{S, \preccurlyeq\}$ un conjunto parcialmente ordenado localmente finito. Es decir, si $x, y \in S$ y $x \preccurlyeq y$, entonces sólo existen finitos $z \in S$ tales que $x \preccurlyeq z \preccurlyeq y$. Sea $T = \{(x, y) \in S \times S | x \preccurlyeq y\}$. Sea V el K-espacio vectorial que tiene a T por base. Definimos Δ_V como la aplicación

$$(x, y) \mapsto \sum_{x \preccurlyeq z \preccurlyeq y} (x, z) \otimes (z, y)$$

y ϵ_V como

$$\epsilon_V(x, y) = \begin{cases} 0 & si \quad x \neq y \\ 1 & si \quad x = y \end{cases}$$

Luego, $(V, \Delta_V, \epsilon_V)$ es una coálgebra.

Ejemplo 1.2.14. Sea x una indeterminada y sea $C = K \oplus Kx$ la suma directa de K-espacios vectoriales. C es coálgebra con

$$\Delta_C(1) = 1 \otimes 1, \qquad \Delta_C(x) = x \otimes x, \qquad \epsilon_C(1) = \epsilon_C(x) = 1.$$

Ejemplo 1.2.15. Sea, igual que antes, x una indeterminada y consideramos el mismo espacio vectorial $C = K \oplus Kx$. Tenemos otra estructura de coálgebra sobre C dada por

$$\Delta_C(1) = 1 \otimes 1, \qquad \Delta_C(x) = 1 \otimes x + x \otimes 1, \qquad \epsilon_C(1) = 1, \qquad \epsilon_C(x) = 0.$$

El Ejemplo 1.2.12 nos da como caso particular dos ejemplos importantes.

Ejemplo 1.2.16. Sea V un K-espacio vectorial con base $\{b_1, b_2, \ldots, b_n\}$. Sean $\Delta_V\colon V \to V \otimes V$ y $\epsilon_V\colon V \to K$ definidas sobre la base como:

$$\Delta_V(b_i) = b_i \otimes b_i \qquad \epsilon_V(b_i) = 1.$$

Ejemplo 1.2.17. Sea $K[x]$ el K-espacio vectorial de los polinomios en una variable. Tomamos $\Delta_{K[x]}$ y $\epsilon_{K[x]}$ definidas sobre la base $\{1, x, x^2, \dots\}$ como

$$\Delta_{K[x]}(x^m) = x^m \otimes x^m \qquad\qquad \epsilon_{K[x]}(x^m) = 1.$$

Podemos definir otra estructura de coálgebra sobre $K[x]$.

Ejemplo 1.2.18. Sea $K[x]$ el espacio vectorial de los polinomios en una variable. Consideremos $\Delta_{K[x]} \colon K[x] \to K[x] \otimes K[x]$ y $\epsilon_{K[x]} \colon K[x] \to K$ definidas sobre la base $\{1, x, x^2, \dots\}$ como

$$\Delta_{K[x]}(x^m) = \sum_{i=o}^{m} \binom{m}{i} x^i \otimes x^{m-i} \qquad\qquad \epsilon_{K[x]}(x^m) = \delta_{0,m}.$$

Veamos que se cumple la propiedad de la coasociatividad. Por un lado tenemos:

$$\begin{aligned}
(\Delta_{K[x]} \otimes I_{K[x]})\Delta_{K[x]}(x^m) &= \sum_{i=0}^{m} \binom{m}{i} \Delta_{K[x]}(x^i) \otimes x^{m-i} \\
&= \sum_{i=0}^{m} \sum_{j=0}^{i} \binom{m}{i}\binom{i}{j} x^j \otimes x^{i-j} \otimes x^{m-i}.
\end{aligned}$$

Por otro lado:

$$\begin{aligned}
(I_{K[x]} \otimes \Delta_{K[x]})\Delta_{K[x]}(x^m) &= \sum_{i=0}^{m} x^i \otimes \Delta_{K[x]}(x^{m-i}) \\
&= \sum_{i=0}^{m} \sum_{j=0}^{m-i} \binom{m}{i}\binom{m-i}{j} x^i \otimes x^j \otimes x^{m-i-j} \\
&= \sum_{i=0}^{m} \sum_{k=i}^{m} \binom{m}{i}\binom{m-i}{k-i} x^i \otimes x^{k-i} \otimes x^{m-k}
\end{aligned}$$

donde hicimos el cambio de variables $k = i + j$ en la última línea. Para conseguir una expresión similar a la anterior reasignamos las variables mediante el cambio $k \mapsto i, i \mapsto j$ de donde resulta:

$$\sum_{j=0}^{m} \sum_{i=j}^{m} \binom{m}{j}\binom{m-j}{i-j} x^j \otimes x^{i-j} \otimes x^{m-i}$$

Comparemos ahora el coeficiente del tensor $x^j \otimes x^{i-j} \otimes x^{m-i}$ de ambas expresiones. En la primera es $\sum_{i=0}^{m} \binom{m}{i}\binom{i}{j}$ y en la segunda es $\sum_{i=j}^{m} \binom{m}{j}\binom{m-j}{i-j}$. Notemos que en la primera expresión sólo tienen sentido los números combinatorios con $i \geq j$. Desarrollando los coeficientes binomiales se verifica inmediatamente que:

$$\sum_{i=j}^{m} \binom{m}{i}\binom{i}{j} = \sum_{i=j}^{m} \binom{m}{j}\binom{m-j}{i-j}$$

que prueba la coasociatividad.

Esta coálgebra se conoce como la **coálgebra de potencias divididas**.

Vamos a definir ahora la estructura análoga a la de ideal de un anillo.

Definición 1.2.19. Sea C una K-coálgebra. Decimos que un subespacio $I \subseteq C$ es un *coideal de* C (o *coideal bilátero de* C) si

$$\Delta_C(I) \subseteq I \otimes C + C \otimes I$$

y $\epsilon_C(I) = 0$.

Observación. Notemos que para el caso de un ideal en un álgebra considerando su estructura de anillo, pediríamos como una condición

$$m_A(I \otimes A + A \otimes I) \subseteq I.$$

Además tenemos que $0 \in I$ que en nuestro lenguaje será $\lambda_A(0) \in I$. "Dualizando" estas condiciones tenemos la definición de coideal.

Proposición 1.2.20. *Sea $I \subseteq C$ un coideal de C. Entonces el espacio vectorial cociente C/I es una K-coálgebra.*

Demostración. Sea $s\colon C \otimes C \to (C \otimes C)/(I \otimes C + C \otimes I)$ el epimorfismo canónico y consideramos la composición

$$s\Delta_C\colon C \to (C \otimes C)/(I \otimes C + C \otimes I).$$

Como I es coideal, se tiene $\Delta_C(I) \subseteq I \otimes C + C \otimes I$ y entonces $I \subseteq \ker(s\Delta_C)$. Por la propiedad universal del cociente, existe una transformación lineal

$$\overline{s\Delta_C}\colon C/I \to (C \otimes C)/(I \otimes C + C \otimes I)$$

dada por $\overline{s\Delta_C}(c + I) = \Delta_C(c) + (I \otimes C + C \otimes I)$ para todo $c \in C$. Sea ahora

$$\alpha\colon (C \otimes C)/(I \otimes C + C \otimes I) \to C/I \otimes C/I$$

el isomorfismo de la demostración de la Proposición 1.1.4, definido como

$$\alpha(a \otimes b + (I \otimes C + C \otimes I)) = (a + I) \otimes (b + I),$$

y sea la composición

$$\Delta_{C/I} = \alpha\overline{s\Delta_C}\colon C/I \to C/I \otimes C/I$$

que resulta ser tal que

$$\Delta_{C/I}(c + I) = \sum_{(c)} (c_{(1)} + I) \otimes (c_{(2)} + I).$$

Debemos ver que $\Delta_{C/I}$ satisface la propiedad coasociativa usando la hipótesis de que Δ_C es comultiplicación. En efecto, para todo $c \in C$,

$$\begin{aligned}
(\Delta_{C/I} \otimes I_{C/I})\Delta_{C/I}(c+I) &= (\Delta_{C/I} \otimes I_{C/I}) \left(\sum_{(c)} (c_{(1)} + I) \otimes (c_{(2)} + I) \right) \\
&= \sum_{(c, c_{(1)})} (c_{(1)_{(1)}} + I) \otimes (c_{(1)_{(2)}} + I) \otimes (c_{(2)} + I) \\
&= (s \otimes s \otimes s) \left(\sum_{(c, c_{(1)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)} \right) \\
&= (s \otimes s \otimes s) \left(\sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)} \right) \\
&= \sum_{(c)} (c_{(1)} + I) \otimes (c_{(2)} + I) \otimes (c_{(3)} + I)
\end{aligned}$$

En forma completamente análoga llegamos a la misma expresión partiendo de $(I_{C/I} \otimes \Delta_{C/I})\Delta_{C/I}(c+I)$. Debemos definir ahora una counidad. Por definición, $I \subseteq \ker(\epsilon_C)$ y, en consecuencia, existe una transformación lineal $\overline{\epsilon_C} \colon C/I \to K$, definida por $\overline{\epsilon_C}(c+I) = \epsilon_C(c)$. Tomamos $\epsilon_{C/I} = \overline{\epsilon_C}$. Veamos ahora que se satisface la propiedad de la counidad sabiendo que ϵ_C lo hace. En efecto, para todo $c \in C$, tenemos

$$\begin{aligned}
(\epsilon_{C/I} \otimes I_{C/I})\Delta_{C/I}(c+I) &= (\overline{\epsilon_C} \otimes I_{C/I}) \left(\sum_{(c)} (c_{(1)} + I) \otimes (c_{(2)} + I) \right) \\
&= \sum_{(c)} \overline{\epsilon_C}(c_{(1)} + I) \otimes (c_{(2)} + I) = \sum_{(c)} \epsilon_C(c_{(1)})(c_{(2)} + I) \\
&= \sum_{(c)} \big(\epsilon_C(c_{(1)})c_{(2)}\big) + I = \left(\sum_{(c)} (\epsilon_C(c_{(1)})c_{(2)} \right) + I \\
&= c + I.
\end{aligned}$$

Por otro lado:

$$\begin{aligned}
(I_{C/I} \otimes \epsilon_{C/I})\Delta_{C/I}(c+I) &= (I_{C/I} \otimes \overline{\epsilon_C}) \left(\sum_{(c)} (c_{(1)} + I) \otimes (c_{(2)} + I) \right) \\
&= \sum_{(c)} (c_{(1)} + I) \otimes \overline{\epsilon_C}(c_{(2)} + I) = \sum_{(c)} \epsilon_C(c_{(2)})(c_{(1)} + I) \\
&= \sum_{(c)} \big(\epsilon_C(c_{(2)})c_{(1)}\big) + I = \left(\sum_{(c)} \epsilon_C(c_{(2)})c_{(1)} \right) + I \\
&= c + I.
\end{aligned}$$

En conclusión, $(C/I, \Delta_{C/I}, \epsilon_{C/I})$ es una K-coálgebra. $\square$

La coálgebra C/I se llama **coálgebra cociente de C por I**. Veamos un ejemplo de coálgebra cociente.

Ejemplo 1.2.21. Sea $K[x]$ la coálgebra del Ejemplo 1.2.17. Para $m \geq 1$, sea I el subespacio de $K[x]$ generado por la base

$$\{x^m - 1, x^{m+1} - 1, x^{m+2} - 1, \dots\}.$$

Para $i \geq 0$,

$$\begin{aligned}
\Delta_{K[x]}(x^i - 1) &= x^i \otimes x^i - 1 \otimes 1 \\
&= (x^i - 1 + 1) \otimes (x^i - 1 + 1) - 1 \otimes 1 \\
&= (x^i - 1) \otimes (x^i - 1) + (x^i - 1) \otimes 1 + 1 \otimes (x^i - 1) + 1 \otimes 1 - 1 \otimes 1 \\
&= (x^i - 1) \otimes 1 + 1 \otimes (x^i - 1) + (x^i - 1) \otimes (x^i - 1).
\end{aligned}$$

Luego, $\Delta_{K[x]}(I) \subseteq I \otimes K[x] + K[x] \otimes I$. Además,

$$\epsilon_{K[x]}(x^i - 1) = \epsilon_{K[x]}(x^i) - \epsilon_{K[x]}(1) = 1 - 1 = 0,$$

entonces $\epsilon_{K[x]}(I) = 0$. Luego, I es un coideal de $K[x]$. La coálgebra cociente $K[x]/I$ es un K-espacio vectorial de dimensión m con base $\{1, x, x^2, \dots, x^{m-1}\}$.

Sea C un K-coálgebra. Un elemento $c \neq 0$ de C tal que $\Delta_C(c) = c \otimes c$ se dice **elemento de tipo grupo** de C.

Proposición 1.2.22. *Si c es un elemento de tipo grupo de una K-coálgebra C, entonces $\epsilon_C(c) = 1$.*

Demostración. Si c es de tipo grupo, entonces

$$\begin{aligned}
c &= s_1(\epsilon_C \otimes I_C)\Delta_C(c) \qquad \text{por (1.6)} \\
&= s_1(\epsilon_C \otimes I_C)(c \otimes c) \\
&= \epsilon_C(c)c.
\end{aligned}$$

En consecuencia, $\epsilon_C(c)c = c = 1c$, con lo cual $(\epsilon_C(c) - 1)c = 0$. Como K es un cuerpo y $c \neq 0$, debe ser $\epsilon_C(c) - 1 = 0$ y, entonces, $\epsilon_C(c) = 1$. $\square$

En el Ejemplo 1.2.12, los elementos de tipo grupo son precisamente los elementos de S. En particular, en los Ejemplos 1.2.16 y 1.2.17 los elementos de tipo grupo son los elementos de la base dada en cada caso.

Proposición 1.2.23. *Si $K[x]$ es la K-coálgebra del Ejemplo 1.2.18, entonces 1 es el único elemento de tipo grupo en $K[x]$.*

Demostración. Supongamos que $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ es un elemento de tipo grupo. Procedamos por inducción en n. Para el caso $n = 0$ tenemos que $f = a_0$. Por la Proposición 1.2.22, resulta $\epsilon_{K[x]}(a_0) = 1$ pero por linealidad, debe ser $\epsilon_{K[x]}(a_0) = a_0\epsilon_{K[x]}(1)$. Como 1 es un elemento de tipo grupo, tenemos $\epsilon_{K[x]}(1) = 1$. Luego $a_0 = 1$. Para el paso inductivo, escribimos $f = g + a_nx^n$ con $g = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$. Por hipótesis,

$$\begin{aligned}\Delta_{K[x]}(f) &= f \otimes f = (g + a_nx^n) \otimes (g + a_nx^n) \\ &= g \otimes g + a_n(g \otimes x^n + x^n \otimes g) + a_n^2(x^n \otimes x^n).\end{aligned} \tag{1.9}$$

Por otro lado, por linealidad,

$$\begin{aligned}\Delta_{K[x]}(f) &= \Delta_{K[x]}(g) + a_n\Delta_{K[x]}(x^n) \\ &= \Delta_{K[x]}(g) + a_n \left(\sum_{i=o}^{n} \binom{n}{i} x^i \otimes x^{n-i} \right)\end{aligned} \tag{1.10}$$

Dado que g tiene grado menor que n, en (1.9) el tensor $x^n \otimes x^n$ tiene como coeficiente a_n^2 y en (1.10) tiene coeficiente nulo. Luego, $a_n^2 = 0$; es decir, $a_n = 0$. Entonces, uniendo las dos ecuaciones: $\Delta_{K[x]}(g) = g \otimes g$. Como g tiene grado menor que n, aplicamos la hipótesis inductiva para concluir que $g = 1$ y entonces $f = 1$.

□

La siguiente proposición de [Swe69, Proposición 3.2.1] nos será de utilidad más adelante.

Proposición 1.2.24. *Si C es una coálgebra y denotamos al conjunto de los elementos de tipo grupo por $G(C)$, entonces $G(C)$ es un subconjunto de C linealmente independiente sobre K.*

Demostración. Supongamos que $G(C)$ no es un conjunto linealmente independiente. Como $0 \notin G(C)$ y K es un cuerpo, cualquier elemento de $G(C)$ forma un conjunto linealmente independiente. Sea $n \in \mathbb{Z}$ mínimo tal que cualquier subconjunto de n elementos de $G(C)$ es linealmente independiente y existe un subconjunto de $n + 1$ elementos de $G(C)$ linealmente dependiente. Entonces, existe una relación de la forma

$$g = \lambda_1 g_1 + \cdots + \lambda_n g_n$$

con $g, g_1, \ldots, g_n \in G(C)$ distintos, $\lambda_1, \ldots, \lambda_n \neq 0$ para todo $1 \leq i \leq n$ y $n \geq 1$. Entonces, por linealidad tenemos

$$\Delta_C(g) = \sum_{i=1}^{n} \lambda_i \Delta_C(g_i) = \sum_{i=1}^{n} \lambda_i g_i \otimes g_i.$$

Por hipótesis,

$$\Delta_C(g) = g \otimes g = \sum_{i,j=1}^{n} \lambda_i \lambda_j g_i \otimes g_j.$$

Tenemos que $\{g_i \otimes g_j\}_{1\leq i,j\leq n}$ es un conjunto linealmente independiente pues, por hipótesis, $\{g_1,\ldots,g_n\}$ es un conjunto linealmente independiente. Entonces, para cada $i \neq j$, debemos tener $\lambda_i\lambda_j = 0$ pero sabemos que todos los λ_i son no nulos. Esto sólo puede ocurrir si $n = 1$. Luego, $g = \lambda_1 g_1$. Como $\epsilon_C(g) = 1$ por la Proposición 1.2.22, tenemos

$$1 = \epsilon_C(g) = \lambda_1\epsilon_C(g_1) = \lambda_1.$$

Entonces, $g = g_1$ lo cual es una contradicción. Luego, $G(C)$ es linealmente independiente sobre K. $\square$

La independencia lineal de los elementos de tipo grupo la usaremos cuando consideremos las biálgebras de Myhill-Nerode.

Definición 1.2.25. Sean $(C, \Delta_C, \epsilon_C)$ y $(D, \Delta_D, \epsilon_D)$ coálgebras. Un *morfismo de coálgebras* es una transformación lineal $\phi\colon C \to D$ tal que

(i) $(\phi\otimes\phi)\Delta_C(c) = \Delta_D(\phi(c))$ para todo $c \in C$; y

(ii) $\epsilon_C(c) = \epsilon_D(\phi(c))$ para todo $c \in C$.

En notación de Sweedler, la primera condición se escribe:

$$\sum_{(c)} \phi(c_{(1)}) \otimes \phi(c_{(2)}) = \sum_{(\phi(c))} (\phi(c))_{(1)} \otimes (\phi(c))_{(2)}.$$

Proposición 1.2.26. *Sea C una K-coálgebra. La counidad $\epsilon_C\colon C \to K$ es morfismo de K-coálgebras.*

Demostración. Para $c \in C$,

$$\begin{aligned}(\epsilon_C\otimes\epsilon_C)\Delta_C(c) &= (\epsilon_C\otimes I_K)(I_C\otimes\epsilon_C)\Delta_C(c) = (\epsilon_C\otimes I_K)\left(\sum_{(c)} c_{(1)}\otimes\epsilon_C(c_{(2)})\right)\\ &= (\epsilon_C\otimes I_K)(c\otimes 1) = \Delta_K(\epsilon_C(c)).\end{aligned}$$

Además, $\epsilon_C(c) = \epsilon_K(\epsilon_C(c))$ pues $\epsilon_K(r) = r$ para todo $r \in K$. Luego, ϵ_C es morfismo de coálgebras. $\square$

Un morfismo de coálgebras inyectivo y sobreyectivo es un **isomorfismo de coálgebras**.

Proposición 1.2.27. *Sea $\phi\colon C \to D$ un morfismo de K-coálgebras. Si $c \in G(C)$, entonces $\phi(c) \in G(D)$.*

Demostración. Como ϕ es morfismo de coálgebras, tenemos

$$\Delta_D(\phi(c)) = (\phi\otimes\phi)\Delta_C(c),$$

y como $c \in G(C)$,

$$(\phi\otimes\phi)\Delta_C(c) = (\phi\otimes\phi)(c\otimes c) = \phi(c)\otimes\phi(c).$$

Luego, $\phi(c) \in G(D)$. $\square$

Si notamos por $K[x]$ a la coálgebra del Ejemplo 1.2.17 y por $K[x]'$ a la del Ejemplo 1.2.18, podemos afirmar que no existe isomorfismo de coálgebras entre $K[x]$ y $K[x]'$ pues, por la Proposición 1.2.27, tendríamos una biyección entre $G(K[x])$ y $G(K[x]')$ pero sabemos que $G(K[x]) = \{1, x, \dots\}$ y, por la Proposición 1.2.23, $G(K[x]') = \{1\}$.

De forma similar a lo que ocurría para el producto tensorial de K-álgebras, el producto tensorial de dos coálgebras C y D es coálgebra con comultiplicación dada por

$$\Delta_{C\otimes D}\colon C \otimes D \to (C \otimes D) \otimes (C \otimes D)$$

definida por

$$\begin{aligned}
\Delta_{C\otimes D}(c \otimes d) &= (I_C \otimes \tau \otimes I_D)(\Delta_C \otimes \Delta_D)(c \otimes d)\\
&= (I_C \otimes \tau \otimes I_D)(\Delta_C(c) \otimes \Delta_D(d))\\
&= (I_C \otimes \tau \otimes I_D)\left(\sum_{(c),(d)} c_{(1)} \otimes c_{(2)} \otimes d_{(1)} \otimes d_{(2)}\right)\\
&= \sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)})
\end{aligned}$$

para $c \in C, d \in D$. La counidad $\epsilon_{C\otimes D}\colon C \otimes D \to K$ se define como

$$\epsilon_{C\otimes D}(c \otimes d) = \epsilon_C(c)\epsilon_D(d)$$

para $c \in C, d \in D$.

Ejemplo 1.2.28. Sean C la K-coálgebra del Ejemplo 1.2.14 y D la K-coálgebra del Ejemplo 1.2.15. Entonces $C \otimes D$ es K-coálgebra con base $\{1\otimes 1, 1\otimes x, x\otimes 1, x\otimes x\}$. La comultiplicación

$$\Delta_{C\otimes D}\colon C \otimes D \to (C \otimes D) \otimes (C \otimes D)$$

está definida como

$$\Delta_{C\otimes D}(1 \otimes 1) = (1 \otimes 1) \otimes (1 \otimes 1),$$

$$\begin{aligned}
\Delta_{C\otimes D}(1 \otimes x) &= (I_C \otimes \tau \otimes I_D)(\Delta_C(1) \otimes \Delta_D(x))\\
&= (I_C \otimes \tau \otimes I_D)((1 \otimes 1) \otimes (1 \otimes x + x \otimes 1))\\
&= (I_C \otimes \tau \otimes I_D)(1 \otimes 1 \otimes 1 \otimes x + 1 \otimes 1 \otimes x \otimes 1)\\
&= (1 \otimes 1) \otimes (1 \otimes x) + (1 \otimes x) \otimes (1 \otimes 1).
\end{aligned}$$

De la misma manera, obtenemos

$$\begin{aligned}
\Delta_{C\otimes D}(x \otimes 1) &= (x \otimes 1) \otimes (x \otimes 1),\\
\Delta_{C\otimes D}(x \otimes x) &= (x \otimes 1) \otimes (x \otimes x) + (x \otimes x) \otimes (x \otimes 1).
\end{aligned}$$

Por otro lado, la counidad $\epsilon_{C\otimes D}\colon C \otimes_K D \to K$ está dada por

$$\begin{aligned}
\epsilon_{C\otimes D}(1 \otimes 1) &= 1, & \epsilon_{C\otimes D}(1 \otimes x) &= 0,\\
\epsilon_{C\otimes D}(x \otimes 1) &= 1, & \epsilon_{C\otimes D}(x \otimes x) &= 0.
\end{aligned}$$

1.3. Dualidad

En esta sección nos enfocamos en el tratamiento del dual lineal de las álgebras y coálgebras. Veremos que el dual de una coálgebra C es un álgebra C^* con las transformaciones inducidas por las traspuestas de Δ_C y ϵ_C. Veremos que la construcción recíproca no es válida. Sin embargo, si reemplazamos el dual A^* de un álgebra A por cierto subespacio A° que se conoce como el dual finito de A, veremos que A° es coálgebra. Como aplicación veremos que $K[x]^\circ$ se puede identificar con la colección de sucesiones recursivas lineales de todos los órdenes sobre K.

Sea C una K-coálgebra y notemos por C^* su dual lineal.

Proposición 1.3.1. *Si C es una coálgebra, entonces C^* es un álgebra.*

Demostración. Debemos construir una multiplicación y una unidad que satisfagan las propiedades asociativa y de la unidad respectivamente. La aplicación traspuesta de Δ_C es una transformación lineal

$$\Delta_C^*\colon (C \otimes C)^* \to C^*$$

definida como

$$\Delta_C^*(\psi)(c) = \psi(\Delta_C(c)),$$

para $\psi \in (C \otimes C)^*, c \in C$. Por el Corolario 1.1.9, $C^* \otimes C^* \subseteq (C \otimes C)^*$. Luego, Δ_C^* se restringe a una transformación lineal que notaremos por $m_{C^*}\colon C^* \otimes C^* \to C^*$ definida como

$$m_{C^*}(f \otimes g)(c) = \Delta_C^*(f \otimes g)(c) = (f \otimes g)(\Delta_C(c))) = \sum_{(c)} f(c_{(1)})g(c_{(2)}).$$

para todos $f, g \in C^*, c \in C$. Sea $I_{C^*}\colon C^* \to C^*$ la identidad. Veamos que m_{c^*} satisface la propiedad asociativa. Esto se deduce de la *coasociatividad de* Δ_C. Sean $f, g, h \in C^*, c \in C$,

$$\begin{aligned}
m_{C^*}(I_{C^*} \otimes m_{C^*})(f \otimes g \otimes h)(c) &= \Delta_{C^*}(I_{C^*} \otimes \Delta_C^*)(f \otimes g \otimes h)(c)\\
&= \Delta_C^*(f \otimes \Delta_C^*(g \otimes h))(c)\\
&= (f \otimes \Delta_C^*(g \otimes h))\Delta_C(c)\\
&= \sum_{(c)} f(c_{(1)})\Delta_C^*(g \otimes h)(c_{(2)})\\
&= \sum_{(c)} f(c_{(1)})(g \otimes h)\Delta_C(c_{(2)})\\
&= \sum_{(c)} f(c_{(1)}) \sum_{(c_{(2)})} g(c_{(2)_{(1)}})h(c_{(2)_{(2)}}).
\end{aligned}$$

Ahora,

$$
\begin{aligned}
\sum_{(c)} f(c_{(1)}) \sum_{(c_{(2)})} g(c_{(2)_{(1)}})h(c_{(2)_{(2)}}) &= \sum_{(c,c_{(2)})} f(c_{(1)})g(c_{(2)_{(1)}})h(c_{(2)_{(2)}}) \\
&= (f \otimes g \otimes h)\left(\sum_{(c,c_{(2)})} c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}}\right) \\
&= (f \otimes g \otimes h)\left(\sum_{(c,c_{(1)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)}\right) \\
&= \sum_{(c,c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)}).
\end{aligned}
$$

Para pasar de la segunda línea a la tercera hemos usado la coasociatividad de Δ_C. Obtuvimos la siguiente igualdad

$$
m_{C^*}(I_{C^*} \otimes m_{C^*})(f \otimes g \otimes h)(c) = \sum_{(c,c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)}).
$$

Para terminar,

$$
\begin{aligned}
m_{C^*}(I_{C^*} \otimes m_{C^*})(f \otimes g \otimes h)(c) &= \sum_{(c,c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)}) \\
&= \sum_{(c)} (f \otimes g)\Delta_C(c_{(1)})h(c_{(2)}) \\
&= \sum_{(c)} \Delta_C^*(f \otimes g)(c_{(1)})h(c_{(2)}) \\
&= (\Delta_C^*(f \otimes g) \otimes h)\Delta_C(c) \\
&= \Delta_C^*(\Delta_C^*(f \otimes g) \otimes h)(c) \\
&= \Delta_C^*(\Delta_C^* \otimes I_{C^*})(f \otimes g \otimes h)(c) \\
&= m_{C^*}(m_{C^*} \otimes I_{C^*})(f \otimes g \otimes h)(c).
\end{aligned}
$$

Luego, m_{C^*} satisface la propiedad asociativa.

Debemos definir ahora una unidad. De forma similar, consideramos la traspuesta de ϵ_C

$$
\epsilon_C^* \colon K^* \to C^*
$$

dada por $\epsilon_C^*(f)(c) = f(\epsilon_C(c))$ para $f \in K^*, c \in C$. Identificando $K = K^*$, tenemos $\epsilon_C^* \colon K \to C^*$ dada por

$$
\epsilon_C^*(r)(c) = r(\epsilon_C(c)) = r\epsilon_C(c),
$$

para $r \in K, c \in C$. Definimos $\lambda_{C^*} = \epsilon_C^*$. Veamos que la propiedad de la counidad de

ϵ_C implica la propiedad de la unidad para λ_{C^*}. Sean $f \in C^*, r \in K, c \in C$,

$$\begin{aligned} m_{c^*}(I_{C^*} \otimes \lambda_{C^*})(f \otimes r)(c) &= \Delta_C^*(I_{C^*} \otimes \epsilon_C^*)(f \otimes r)(c) \\ &= \Delta_C^*(f \otimes \epsilon_C^*(r))(c) = (f \otimes \epsilon_C^*(r))(\Delta_C(c)) \\ &= \sum_{(c)} f(c_{(1)})\epsilon_C^*(r)(c_{(2)}) = \sum_{(c)} f(c_{(1)})r(\epsilon_C(c_{(2)})). \end{aligned}$$

Hemos probado que

$$m_{c^*}(I_{C^*} \otimes \lambda_{C^*})(f \otimes r)(c) = r \sum_{(c)} f(c_{(1)})\epsilon_C(c_{(2)}).$$

Continuando, tenemos

$$\begin{aligned} m_{c^*}(I_{C^*} \otimes \lambda_{C^*})(f \otimes r)(c) &= r \sum_{(c)} f(c_{(1)})\epsilon_C(c_{(2)}) = r \sum_{(c)} \epsilon_C(c_{(2)})f(c_{(1)}) \\ &= r \sum_{(c)} f(\epsilon_C(c_{(2)})c_{(1)}) = rf\left(\sum_{(c)} \epsilon_C(c_{(2)})c_{(1)}\right) = rf(c). \end{aligned}$$

Para pasar de la cuarta a la quinta línea usamos la propiedad de la counidad para ϵ_C. Mediante un cálculo totalmente análogo, obtenemos

$$m_{c^*}(\lambda_{C^*} \otimes I_{C^*})(r \otimes f) = rf.$$

Esto conluye la prueba. $\square$

Observación. Tenemos que $\lambda_{C^*}(1_K)(c) = \epsilon_C(c), \forall c$. Como $1_{C^*} = \lambda_{C^*}(1_K)$, resulta que $1_{C^*} = \epsilon_C$. Es decir, ϵ_C es el único elemento de C^* que cumple $\epsilon_C f = f = f\epsilon_C$ para todo $f \in C^*$.

Por lo anterior, podemos preguntarnos si, dada (A, m_A, λ_A) una K-álgebra, es cierto que A^* es una K-coálgebra. Si quisiéramos repetir un argumento similar al empleado para el dual de una coálgebra, deberíamos considerar la aplicación traspuesta de la multiplicación, $m_A^*\colon A^* \to (A \otimes A)^*$. Supongamos que A es de dimensión infinita. En este caso, $A^* \otimes A^*$ es un subespacio propio de $(A \otimes A)^*$. De aquí que m_A^* puede no inducir la comultiplicación requerida $m_A^*\colon A^* \to A^* \otimes A^*$. De hecho, tenemos un ejemplo que nos muestra que $m_A^*(A^*) \nsubseteq A^* \otimes A^*$.

Ejemplo 1.3.2. Sea $A = K[x]$ la K-álgebra de polinomios en x. Sea $m_{K[x]}$ la multiplicación usual con traspuesta $m_{K[x]}^*\colon K[x]^* \to (K[x] \otimes K[x])^*$. Consideremos la sucesión en K dada por

$$1, 0, 0, 1, 1, 1, 0, 0, 0, 0, \ldots$$

(esto es, un 1, seguido de dos 0, seguido de tres 1, etc.). Sea f el elemento de $K[x]^*$ definido como

$$\begin{aligned} f =& 1e_0 + 0e_1 + 0e_2 + 1e_3 + 1e_4 + 1e_5 + 0e_6 + 0e_7 + 0e_8 + 0e_9 \\ &+ 1e_{10} + 1e_{11} + 1e_{12} + 1e_{13} + 1e_{14} + \ldots \end{aligned}$$

donde $e_i(x^j) = \delta_{i,j}, i, j \geq 0$. Entonces $m^*_{K[x]}(f) \notin K[x]^* \otimes K[x]^*$.

En efecto, supongamos que $m^*_{K[x]}(f) = \sum_{i=1}^{r} \phi_i \otimes \psi_i$ con ϕ_i y $\psi_i \in K[x]^*$ y $r \in \mathbb{N}$. Como $\mathrm{codim}(\mathrm{Ker}(\phi_i)) = 1$ para todo $1 \leq i \leq r$, entonces $\mathrm{codim}(\bigcap_{i=1}^{r} \mathrm{Ker}(\phi_i))$ es finita. Luego, existe un polinomio $p(x) \in \bigcap_{i=1}^{r} \mathrm{Ker}(\phi_i)$ de grado positivo. Escribamos $p(x) = \sum_{j=0}^{n} a_j x^j$ con $a_n \neq 0$. Elijamos $k \in \mathbb{N}$ tal que la sucesión dada tiene una tira de n ceros seguida de un uno. Es decir, busco k tal que los términos desde la posición k hasta la $k + n - 1$ son ceros y en la $k + n$ hay un uno. Tenemos que:

$$m^*_{K[x]}(f)(p(x) \otimes x^k) = f(p(x)x^k) = f\left(\sum_{j=0}^{n} a_j x^{j+k}\right) = \sum_{j=0}^{n} a_j f(x^{j+k}) = a_n \neq 0.$$

Lo cual es absurdo pues, por la elección de $p(x)$, se verifica que:

$$\left(\sum_{i=1}^{r} \phi_i \otimes \psi_i\right)(p(x) \otimes x^k) = \sum_{i=1}^{r} \phi_i(p(x)) \otimes \psi_i(x^k) = 0.$$

Para poder asegurar que m^*_A nos sirve como multiplicación, debemos considerar un subespacio de A^* llamado el "dual finito" A° de A. Sea (A, m_A, λ_A) una K-álgebra. Entonces A es un K-espacio vectorial y un anillo. Un ideal I de A es de **codimensión finita** (o **cofinito**) si el espacio cociente A/I es de dimensión finita. Sea f un elemento de A^* y sea S un subconjunto de A. Decimos que f **se anula sobre** S si $f(s) = 0$ para todo $s \in S$.

Definición 1.3.3. Sea A una K-álgebra. El *dual finito* A° *de* A es el subespacio de A^* definido por

$$A^\circ = \{f \in A^* \colon f \text{ se anula sobre algún ideal } I \subseteq A \text{ de codimensión finita}\}$$

Ejemplo 1.3.4. Sea $e_i \in K[x]^*$ definido como $e_i(x^j) = \delta_{i,j}$ para $i, j \geq 0$. Entonces $e_i \in K[x]^\circ$ puesto que e_i se anula sobre el ideal (x^{i+1}) y $\dim(K[x]/(x^{i+1})) = i + 1$.

Proposición 1.3.5. *Si A es un K-espacio vectorial de dimensión finita, entonces $A^\circ = A^*$.*

Demostración. Se sigue de que $\{0\}$ es ideal de A, $f(0) = 0, \forall f \in A^*$ y que $A/\{0\} = A$ que es de dimensión finita por hipótesis. □

Nuestro objetivo, ahora, es probar que A° es coálgebra (ver Proposición 1.3.9). Para ello, necesitamos tres proposiciones previas.

Proposición 1.3.6. *Sea I un ideal de A y $s \colon A \to A/I$ el epimorfismo canónico de espacios vectoriales. Sea $s^* \colon (A/I)^* \to A^*$ la traspuesta definida por $s^*(f)(a) = f(s(a))$, para todo $f \in (A/I)^*, a \in A$. Entonces s^* es inyectiva.*

Demostración. Sean $f, g \in (A/I)^*$. Para $a \in A$, $s^*(f)(a) = s^*(g)(a)$ implica que $f(s(a)) = g(s(a))$. Por lo cual, $f(a + I) = g(a + I)$, y entonces $f = g$. □

Proposición 1.3.7. *Sea $f \in A^\circ$ y supongamos que f se anula sobre el ideal I de A. Entonces, existe un único elemento $\bar{f} \in (A/I)^*$ para el cual $s^*(\bar{f}) = f$.*

Demostración. La unicidad va a venir dada por el hecho de que s^* es inyectiva por la Proposición 1.3.6. Debemos ver la existencia. El elemento $f \in A^\circ \subseteq A^*$ es un morfismo de K-módulos $f\colon A \to K$ y, como $f(I) = 0$ resulta que $I \subseteq \ker(f)$. Sea $s\colon A \to A/I$ el epimorfismo canónico. Por la propiedad universal del cociente existe un morfismo de K-módulos $\bar{f}\colon A/I \to K$ tal que $\bar{f}(s(a)) = f(a)$ para todo $a \in A$. Por esto, $s^*(\bar{f})(a) = f(a)$ para todo $a \in A$. $\square$

Proposición 1.3.8. $m_A^*(A^\circ) \subseteq A^\circ \otimes A^\circ$.

Demostración. Sea $f \in A^\circ$. Luego, f se anula sobre algún ideal $I \subseteq A$ de codimensión finita. Por la Proposición 1.3.7, existe un único elemento $\bar{f} \in (A/I)^*$ que cumple $s^*(\bar{f}) = f$. Sea

$$m_{A/I}\colon A/I \otimes A/I \to A/I,$$

dada por $(a + I) \otimes (b + I) \mapsto ab + I$, la multiplicación de la K-álgebra A/I (cf. Proposición 1.2.8). La traspuesta de $m_{A/I}$ es

$$m_{A/I}^*\colon (A/I)^* \to (A/I \otimes A/I)^*$$

que, dado que A/I es de dimensión finita, se transforma en

$$m_{A/I}^*\colon (A/I)^* \to (A/I)^* \otimes (A/I)^*.$$

Ahora,

$$\begin{aligned} m_A^*(f)(a \otimes b) &= m_A^*(s^*(\bar{f}))(a \otimes b) = s^*(\bar{f})(m_A(a \otimes b)) \\ &= s^*(\bar{f})(ab) = \bar{f}(s(ab)) = \bar{f}(ab + I) \\ &= \bar{f}(m_{A/I}((a + I) \otimes (b + I))). \end{aligned}$$

Continuando, tenemos

$$\begin{aligned} m_A^*(f)(a \otimes b) &= \bar{f}(m_{A/I}((a + I) \otimes (b + I))) \\ &= m_{A/I}^*(\bar{f})((a + I) \otimes (b + I)) \\ &= m_{A/I}^*(\bar{f})(s(a) \otimes s(b)). \end{aligned}$$

Notemos que $m_{A/I}^*(\bar{f}) = \sum_{i=1}^m f_i \otimes g_i$ para ciertos $f_i, g_i \in (A/I)^*$. Luego,

$$\begin{aligned} m_A^*(f)(a \otimes b) &= m_{A/I}^*(\bar{f})(s(a) \otimes s(b)) = \left(\sum_{i=1}^m f_i \otimes g_i\right)(s(a) \otimes s(b)) \\ &= \sum_{i=1}^m f_i(s(a)) \otimes g_i(s(b)) = \sum_{i=1}^m s^*(f_i)(a) \otimes s^*(g_i)(b) \\ &= \left(\sum_{i=1}^m s^*(f_i) \otimes s^*(g_i)\right)(a \otimes b). \end{aligned}$$

Hemos probado la siguiente igualdad

$$m_A^*(f) = \sum_{i=1}^{m} s^*(f_i) \otimes s^*(g_i).$$

Resta ver que $s^*(f_i), s^*(g_i) \in A^\circ$. Para ello, sea $q \in I$, es claro que $s^*(f_i)(q) = f_i(s(q)) = f_i(I) = 0 \in K$, y entonces $s^*(f_i)$ se anula sobre I, por lo cual $s^*(f_i) \in A^\circ$. De forma análoga, $s^*(g_i) \in A^\circ$. Esto concluye la prueba. □

La traspuesta de la aplicación

$$I_A \otimes m_A \colon A \otimes A \otimes A \to A \otimes A$$

restringida a $A^* \otimes A^*$ es la transformación

$$I_A^* \otimes m_A^* = I_{A^*} \otimes m_A^* \colon A^* \otimes A^* \to (A \otimes A \otimes A)^*.$$

De la misma forma, la traspuesta de $m_A \otimes I_A$ restringida a $A^* \otimes A^*$ es

$$m_A^* \otimes I_A^* = m_A^* \otimes I_{A^*} = m_A^* \otimes I_{A^*} \colon A^* \otimes A^* \to (A \otimes A \otimes A)^*.$$

Proposición 1.3.9. *Si A es un álgebra, entonces A° es una coálgebra.*

Demostración. Sea $m_A^* \colon A^* \to (A \otimes A)^*$ la traspuesta de la multipliación de A. Por la Proposición 1.3.8, $m_A^*(A^\circ) \subseteq A^\circ \otimes A^\circ$. Notemos por Δ_{A° a la restricción de m_A^* a A°. La función $\Delta_{A^\circ} \colon A^\circ \to A^\circ \otimes A^\circ$ es una transformación K-lineal definida como $\Delta_{A^\circ}(f) = m_A^*(f)$ para toda $f \in A^\circ$. Veamos en primer lugar que la asociatividad de m_A implica la coasociatividad de Δ_{A°. Sean $f \in A^\circ, a, b, c \in A$, tenemos

$$\begin{aligned}
(I_{A^\circ} \otimes \Delta_{A^\circ})\Delta_{A^\circ}(f)(a \otimes b \otimes c) &= (I_A^* \otimes m_A^*)m_A^*(f)(a \otimes b \otimes c) \\
&= m_A^*(f)(I_A \otimes m_A)(a \otimes b \otimes c) \\
&= m_A^*(f)(a \otimes bc) = f(m_A(a \otimes bc)) \\
&= f(a(bc)) = f((ab)c).
\end{aligned}$$

En la última línea usamos la propiedad de asociatividad del producto en A. Ahora,

$$\begin{aligned}
(I_{A^\circ} \otimes \Delta_{A^\circ})\Delta_{A^\circ}(f)(a \otimes b \otimes c) &= f((ab)c) = f(m_A(ab \otimes c)) = m_A^*(f)(ab \otimes c) \\
&= m_A^*(f)(m_A \otimes I_A)(a \otimes b \otimes c) \\
&= (m_A^* \otimes I_A^*)m_A^*(f)(a \otimes b \otimes c) \\
&= (\Delta_{A^\circ} \otimes I_{A^\circ})\Delta_{A^\circ}(f)(a \otimes b \otimes c).
\end{aligned}$$

Esto prueba la coasocitividad de Δ_{A°. Para definir la counidad de A°, consideramos la aplicación dual $\lambda_A^* \colon A^* \to K^* = K$. Notemos por $\epsilon_{A^\circ} \colon A^\circ \to K$ a la restricción de λ_A^* a A°. Sea $f \in A^\circ, r \in K$,

$$\epsilon_{A^\circ}(f)(r) = f(\lambda_A(r)) = f(r1_A) = rf(1_A) = f(1_A)(r)$$

y, entonces, $\epsilon_{A^\circ}(f) = f(1_A)$. Veamos que la propiedad de la unidad para λ_A implica la propiedad de la counidad para ϵ_{A°. Sean $f \in A^\circ, r \in K, a \in A$,

$$\begin{aligned}(\epsilon_{A^\circ} \otimes I_{A^\circ})\Delta_{A^\circ}(f)(r \otimes a) &= (\lambda_A^* \otimes I_A^*)m_A^*(f)(r \otimes a) = m_A^*(f)(\lambda_A \otimes I_A)(r \otimes a)\\ &= f(m_A(\lambda_A \otimes I_A)(r \otimes a)) = f(ra) = rf(a)\\ &= (1 \otimes f)(r \otimes a).\end{aligned}$$

Para pasar de la línea 3 a la 4 hemos aplicado la propiedad de la unidad de λ_A. Hemos probado que

$$(\epsilon_{A^\circ} \otimes I_{A^\circ})\Delta_{A^\circ}(f) = 1 \otimes f.$$

En forma análoga, obtenemos

$$(I_{A^\circ} \otimes \epsilon_{A^\circ})\Delta_{A^\circ}(f) = f \otimes 1.$$

Luego, ϵ_{A° satisface la condición de counidad y se sigue que $(A^\circ, \Delta_{A^\circ}, \epsilon_{A^\circ})$ es una coálgebra. □

Ejemplo 1.3.10. Sea $A = M_n(K)$ el álgebra de las matrices cuadradas de $n \times n$ con coeficientes en K. Notamos por E_{ij} a la matriz elemental que tiene un 1 en el lugar ij y 0 en los demás. El conjunto de matrices $\{E_{ij} \colon 1 \le i, j \le n\}$ es una base para A. Si tomamos su base dual $\{x_{ij}\}$, entonces A^* es coálgebra con

$$\Delta_{A^*}(x_{ij}) = \sum_{k=1}^{n} x_{ik} \otimes x_{kj} \qquad\qquad \epsilon_{A^*}(x_{ij}) = \delta_{ij}.$$

En efecto:

$$\epsilon_{A^*}(x_{ij}) = x_{ij}(\lambda_A(1)) = x_{ij}(\sum_k E_{kk}) = \sum_k \delta_{ik}\delta_{kj} = \delta_{ij}$$

y

$$\begin{aligned}\Delta_{A^*}(x_{ij})(E_{kl} \otimes E_{mn}) &= x_{ij}(\lambda_A(E_{kl} \otimes E_{mn})) = \delta_{lm}x_{ij}(E_{kn}) = \delta_{lm}\delta_{ik}\delta_{jn}\\ &= \sum_p \delta_{ik}\delta_{lp}\delta_{pm}\delta_{jn} = \sum_p x_{ip}(E_{kl})x_{pj}(E_{mn})\\ &= \left(\sum_p x_{ip} \otimes x_{pj}\right)(E_{kl} \otimes E_{mn}).\end{aligned}$$

Si A es una K-álgebra de dimensión finita como K-espacio vectorial, entonces $A^\circ = A^*$ y A^* es una K-coálgebra. Para $a, b \in A, f \in A^*$, tenemos la fórmula

$$\begin{aligned}f(ab) &= f(m_A(a \otimes b)) = m_A^*(f)(a \otimes b)\\ &= \left(\sum_{(f)} f_{(1)} \otimes f_{(2)}\right)(a \otimes b) = \sum_{(f)} f_{(1)}(a)f_{(2)}(b).\end{aligned} \tag{1.11}$$

Vamos a ver a continuación una aplicación de la fórmula (1.11). Sea S un monoide finito de cardinal m, y sea KS el anillo del monoide. La K-álgebra KS es de dimensión finita sobre K con base $\{1 = g_0, g_1, \ldots, g_{m-1}\}$. Por otro lado, $KS^\circ = KS^*$ tiene base $\{e_1, e_{g_1}, \ldots, e_{g_{m-1}}\}$ donde $e_{g_i}(g_j) = \delta_{i,j}$.

Proposición 1.3.11. *Sea $(KS^*, \Delta_{KS^*}, \epsilon_{KS^*})$ la coálgebra como en lo anterior. Entonces,*

$$\Delta_{KS^*}(e_{g_i}) = \sum_{g_j g_k = g_i} e_{g_j} \otimes e_{g_k},$$

para $i = 0, 1, \ldots, m-1$.

Demostración. Notemos que $\{e_{g_j} \otimes e_{g_k}\}$ con $0 \leq j, k \leq m-1$, es base de $KS^* \otimes KS^*$ como K-espacio vectorial. Fijemos $i \in \{0, \ldots, m-1\}$. Existen elementos $a_{i,j',k'} \in K$ para los cuales

$$\Delta_{KS^*}(e_{g_i}) = \sum_{j',k'=0}^{m-1} a_{i,j',k'}(e_{g_{j'}} \otimes e_{g_{k'}}).$$

Sean j, k tales que $g_i = g_j g_k$. Por (1.11),

$$1 = e_{g_i}(g_i) = e_{g_i}(g_j g_k) = \sum_{j',k'=0}^{m-1} a_{i,j',k'} e_{g_{j'}}(g_j) e_{g_{k'}}(g_k) = a_{i,j,k}.$$

De forma similar, si i, j son tales que $g_i \neq g_j g_k$, entonces

$$0 = e_{g_i}(g_j g_k) = \sum_{j',k'=0}^{m-1} a_{i,j',k'} e_{g_{j'}}(g_j) e_{g_{k'}}(g_k) = a_{i,j,k}.$$

Se sigue que

$$\Delta_{KS^*}(e_{g_i}) = \sum_{g_j g_k = g_i} e_{g_j} \otimes e_{g_k},$$

para $i = 0, 1, \ldots, m-1$. □

La siguiente proposición relaciona la (co)conmutatividad de una (co)álgebra con la coconmutatividad (conmutatividad) de la versión dual correspondiente.

Proposición 1.3.12. *Sean (A, m_A, λ_A) un álgebra y $(C, \Delta_C, \epsilon_C)$ una coálgebra.*

(i) Si A es conmutativa, entonces $(A^\circ, \Delta_{A^\circ}, \epsilon_{A^\circ})$ es coálgebra coconmutativa.

(ii) Si C es coconmutativa, entonces $(C^*, m_{C^*}, \lambda_{C^*})$ es álgebra conmutativa.

Demostración. Sea $\tau\colon A \otimes A \to A \otimes A$ dada por $a \otimes b \mapsto b \otimes a$ el morfismo de intercambio. La traspuesta τ^* restringida a $A^* \otimes A^*$ es el morfismo de intercambio de $A^* \otimes A^*$. Para probar la primera afirmación, sean $f \in A^\circ, a, b \in A$. Entonces,

$$\Delta_{A^\circ}(f)(a \otimes b) = f(m_A(a \otimes b)) = f(m_A(\tau(a \otimes b)) = \tau^*(\Delta_{A^\circ}(f))(a \otimes b).$$

Luego, $\Delta_{A^\circ} = \tau^* \Delta_{A^\circ}$. Es decir, A° es coconmutativa. Para la segunda parte, sean $f, g \in C^*, c \in C$. Entonces,

$$\begin{aligned} m_{C^*}(f \otimes g)(c) &= (f \otimes g)(\Delta_C(c)) = (f \otimes g)(\tau \Delta_C(c)) \\ &= m_{C^*}(\tau^*(f \otimes g))(c) = m_{C^*}\tau^*(f \otimes g)(c). \end{aligned}$$

Luego, $m_{C^*} = m_{C^*}\tau^*$. Es decir, C^* es conmutativa. □

En la siguiente subsección aplicaremos lo visto sobre coálgebras duales al estudio de las sucesiones recursivas lineales sobre un cuerpo K.

1.3.1. Aplicación del dual finito a las sucesiones recursivas lineales

Notemos por $K[x]$ al álgebra de polinomios sobre el cuerpo K como es usual. Como en el Ejemplo 1.3.2, la colección de sucesiones $\{s_n\}_{n=0}^{\infty}$ sobre K se puede identificar con el dual lineal $K[x]^*$. De hecho, la sucesión $\{s_n\}_{n=0}^{\infty}$ se corresponde con la suma infinita $s = \sum_{n=0}^{\infty} s_n e_n$, donde $e_n(x^j) = \delta_{n,j}, \forall n, j$. La siguiente proposición vincula el dual finito con las sucesiones recursivas lineales.

Proposición 1.3.13. *Sea K un cuerpo. La colección de sucesiones recursivas lineales sobre K de todos los órdenes se identifica con el dual finito de $K[x]$.*

Demostración. Sea $\{s_n\}$ una sucesión recursiva lineal de orden $k > 0$ sobre K con relación de recurrencia dada por

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_1 s_{n+1} + a_0 s_n, \quad n \geq 0, \tag{1.12}$$

y polinomio característico

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0, \tag{1.13}$$

para $a_0, a_1, \ldots, a_{k-1} \in K$. Identificamos a $\{s_n\}$ con el elemento $s = \sum_{n=0}^{\infty} s_n e_n$ de $K[x]^*$. Ahora,

$$\begin{aligned} s(f(x)) &= \left(\sum_{n=0}^{\infty} s_n e_n\right)(x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0) \\ &= s_k - a_{k-1}s_{k-1} - a_{k-2}s_{k-2} - \cdots - a_1 s_1 - a_0 s_0 = 0. \end{aligned}$$

Veamos que como consecuencia de esto $s(g(x)f(x)) = 0$ para todo $g(x) \in K[x]$. De hecho, por linealidad, basta verlo para polinomios de la forma $g(x) = x^m$.

$$\begin{aligned} s(x^m f(x)) &= \left(\sum_{n=0}^{\infty} s_n e_n\right)(x^{m+k} - a_{k-1}x^{m+k-1} - a_{k-2}x^{m+k-2} - \cdots - a_1 x^{m+1} - a_0 x^m) \\ &= s_{m+k} - a_{k-1}s_{m+k-1} - a_{k-2}s_{m+k-2} - \cdots - a_1 s_{m+1} - a_0 s_m = 0. \end{aligned}$$

Entonces s se anula sobre el ideal principal $I = (f(x))$ de $K[x]$. Además, sabemos que $\dim(K[x]/I) = k$. Luego $s \in K[x]^\circ$.

Por otra parte, dado $s = \sum_{n=0}^{\infty} s_n e_n \in K[x]^\circ$, s se anula sobre algún ideal $I \subseteq K[x]$ de codimensión finita. Como $K[x]$ es DIP, $I = (f(x))$ para cierto polinomio mónico $f(x)$ sobre K de grado k. Veamos que $\{s_n\}$ es recursiva de orden k. En efecto, como $s(x^m f(x)) = 0$ para todo m, de forma análoga a la cuenta anterior tenemos

$$\begin{aligned} 0 &= s(x^m f(x)) \\ &= \left(\sum_{n=0}^{\infty} s_n e_n\right)(x^{m+k} - a_{k-1}x^{m+k-1} - a_{k-2}x^{m+k-2} - \cdots - a_1 x^{m+1} - a_0 x^m) \\ &= s_{m+k} - a_{k-1}s_{m+k-1} - a_{k-2}s_{m+k-2} - \cdots - a_1 s_{m+1} - a_0 s_m. \end{aligned}$$

Más aún, la recurrencia tiene como polinomio característico al propio $f(x)$. □

Por la Proposición 1.3.9, sabemos que la colección de sucesiones recursivas lineales sobre K de todos los órdenes es una coálgebra $(K[x]^\circ, \Delta_{K[x]^\circ}, \epsilon_{K[x]^\circ})$. En este punto nos preguntamos: dada la sucesión $s = \{s_n\} \in K[x]^\circ$, ¿cómo calculamos $\Delta_{K[x]^\circ}(s) \in K[x]^\circ \otimes K[x]^\circ$?

Supongamos que s se anula sobre el ideal $I = (f(x))$ de $K[x]$ donde $f(x)$ es el polinomio característico de s. Sea $c\colon K[x] \to K[x]/(f(x))$ el epimorfismo canónico. En vista del método usado en la demostración de la Proposición 1.3.8, primero debemos hallar $\bar{s} \in (K[x]/(f(x)))^*$ tal que $c^*(\bar{s}) = s$. Luego, calculamos

$$m^*_{K[x]/(f(x))}(\bar{s}) = \sum_{i=1}^{m} f_i \otimes g_i,$$

donde $f_i, g_i \in (K[x]/(f(x)))^*$. Finalmente, tenemos

$$\Delta_{K[x]^\circ}(s) = \sum_{i=1}^{m} c^*(f_i) \otimes c^*(g_i) \in K[x]^\circ \otimes K[x]^\circ.$$

Veamos cómo funciona este método en un ejemplo sencillo.

Ejemplo 1.3.14. Sea $K = GF(2)$ el cuerpo finito de dos elementos. Consideremos la sucesión $s = \{s_n\}$ recursiva de orden 2 en K con polinomio característico $f(x) = x^2 + x + 1$ y vector inicial $\mathbf{s}_0 = 11$ (una sucesión de Fibonacci). Sea α una raíz de $f(x)$. Entonces, $\{1, \alpha\}$ es base de $K[x]/(f(x)) = GF(4)$ sobre K y $\{\varepsilon_1, \varepsilon_\alpha\}$ es una base de $(K[x]/(f(x)))^* = GF(4)^*$ con $\varepsilon_{\alpha^i}(\alpha^j) = \delta_{i,j}$ para $0 \leq i, j \leq 1$. Ahora, si $\{e_i\}$ es tal que $e_i(x^j) = \delta_{i,j}$ para $i, j \geq 0$, la sucesión $s = \{s_n\}$ se puede escribir como un elemento de $K[x]^\circ$ de la forma:

$$s = 1 \cdot e_0 + 1 \cdot e_1 + 0 \cdot e_2 + 1 \cdot e_3 + 1 \cdot e_4 + \dots$$

Sea $\bar{s} = 1 \cdot \varepsilon_1 + 1 \cdot \varepsilon_\alpha$. Veamos que $c^*(\bar{s}) = s$. Para eso, debemos verificar que $c^*(\bar{s})(x^j) = s_j$ para todo $j \geq 0$.

$$c^*(\bar{s})(x^j) = \bar{s}(c(x^j)) = \bar{s}(x^j + (f(x))) = \bar{s}(\alpha^j) = s_j.$$

El próximo paso es calcular $m^*_{GF(4)}(\bar{s})$. Pero notemos que

$$m^*_{GF(4)}(\bar{s}) = m^*_{GF(4)}(\varepsilon_1) + m^*_{GF(4)}(\varepsilon_\alpha)$$

y entonces, debemos calcular por separado $m^*_{GF(4)}(\varepsilon_1)$ y $m^*_{GF(4)}(\varepsilon_\alpha)$. Para ello, usaremos la fórmula (1.11) y la idea de la Proposición 1.3.11. Primero notemos que

$$m^*_{GF(4)}(\varepsilon_1) = c_{0,0,0}(\varepsilon_1 \otimes \varepsilon_1) + c_{0,0,1}(\varepsilon_1 \otimes \varepsilon_\alpha) + c_{0,1,0}(\varepsilon_\alpha \otimes \varepsilon_1) + c_{0,1,1}(\varepsilon_\alpha \otimes \varepsilon_\alpha),$$

para ciertos $c_{0,i,j} \in \{0, 1\}$ para todo $0 \leq i, j \leq 1$. Entonces,

$$\varepsilon_1(ab) = c_{0,0,0}\varepsilon_1(a)\varepsilon_1(b) + c_{0,0,1}\varepsilon_1(a)\varepsilon_\alpha(b) + c_{0,1,0}\varepsilon_\alpha(a)\varepsilon_1(b) + c_{0,1,1}\varepsilon_\alpha(a)\varepsilon_\alpha(b),$$

para todo $a, b \in GF(4)$. Ahora, como

$$1 = 1 \cdot 1 = \alpha(1+\alpha) = (1+\alpha)\alpha,$$

y

$$\alpha = 1 \cdot \alpha = \alpha \cdot 1 = (1+\alpha)(1+\alpha),$$

en $GF(4)$, concluimos que

$$m^*_{GF(4)}(\varepsilon_1) = \varepsilon_1 \otimes \varepsilon_1 + \varepsilon_\alpha \otimes \varepsilon_\alpha.$$

De forma análoga, obtenemos

$$m^*_{GF(4)}(\varepsilon_\alpha) = \varepsilon_1 \otimes \varepsilon_\alpha + \varepsilon_\alpha \otimes \varepsilon_1 + \varepsilon_\alpha \otimes \varepsilon_\alpha.$$

Entonces,

$$m^*_{GF(4)}(\bar{s}) = \varepsilon_1 \otimes \varepsilon_1 + \varepsilon_1 \otimes \varepsilon_\alpha + \varepsilon_\alpha \otimes \varepsilon_1.$$

Finalmente,

$$\begin{aligned}\Delta_{K[x]^\circ}(s) &= c^*(\varepsilon_1) \otimes c^*(\varepsilon_1) + c^*(\varepsilon_1) \otimes c^*(\varepsilon_\alpha) + c^*(\varepsilon_\alpha) \otimes c^*(\varepsilon_1)\\ &= r \otimes r + r \otimes t + t \otimes r,\end{aligned}$$

donde $r = \{r_n\}$ y $t = \{t_n\}$ son sucesiones de Fibonacci en $GF(2)$ con vectores iniciales $\mathbf{r}_0 = 10$ y $\mathbf{t}_0 = 01$, respectivamente. Esto es porque se cumple que

$$\begin{aligned}r_{n-2} + r_{n-1} &= c^*(\varepsilon_1(\alpha^{n-2})) + c^*(\varepsilon_1(\alpha^{n-1})) = c^*(\varepsilon_1(\alpha^{n-2} + \alpha^{n-1}))\\ &= c^*(\varepsilon_1(\alpha^{n-2}(1+\alpha))) = c^*(\varepsilon_1(\alpha^{n-2}\alpha^2)) = c^*(\varepsilon_1(\alpha^n)) = r_n.\end{aligned}$$

Una situación análoga ocurre con $t = \{t_n\}$. Los vectores iniciales los obtenemos por un cálculo directo de los primeros términos de cada sucesión.

Capítulo 2

Biálgebras

En este segundo capítulo vamos a considerar biálgebras, es decir espacios vectoriales que son a la vez álgebras y coálgebras con cierta compatibilidad. Daremos algunos ejemplos básicos y veremos que B° es biálgebra si B lo es. Como propiedad interesante, veremos que $K[x]$ es biálgebra sólo de dos formas diferentes y entonces $K[x]^\circ$ es biálgebra en dos sentidos distintos. En consecuencia, por lo que vimos en el capítulo anterior, podemos multiplicar sucesiones recursivas lineales de dos formas que son bien conocidas: una de ellas es el producto de Hadamard y la otra es el producto de Hurwitz.

Daremos una aplicación importante de biálgebra a la computación teórica. Introduciremos los autómatas finitos y probaremos el teorema de Myhill–Nerode que nos dirá exactamente cuándo un lenguaje es aceptado por un autómata finito. Generalizaremos el teorema a una versión algebraica en el cual cierta biálgebra de dimensión finita (las biálgebras de Myhill–Nerode) juega el papel de un autómata finito que acepta el lenguaje. Veremos que toda biálgebra de Myhill–Nerode determina un autómata finito y que todo autómata determina una biálgebra de Myhill–Nerode.

En la última sección de este capítulo introducimos el concepto de sucesión regular. Se trata de sucesiones que generalizan sucesiones recursivas lineales sobre cuerpos finitos.

2.1. Introducción

En esta sección introducimos los conceptos de biálgebras, biideales, biálgebras cociente y morfismos de biálgebras. Mostraremos cómo una biálgebra B actúa sobre un álgebra A dándole estructura de B-módulo álgebra a izquierda y sobre una coálgebra C dándole estructura de B-módulo coálgebra a derecha. Definiremos cierta acción a derecha de B sobre el álgebra B^* conocida como el traslado a derecha $f \leftharpoonup a$ de $f \in B^*$ por $a \in B$. Daremos una caracterización que nos permita decidir cuándo $f \in B^\circ$. Como consecuencia inmediata, veremos que si B es biálgebra entonces B° es biálgebra.

Mostraremos que $K[x]$ tiene sólo dos estructuras de biálgebra y luego $K[x]^\circ$ tiene dos estructuras distintas de biálgebra que permiten multiplicar las sucesiones recursivas lineales de dos formas diferentes.

Definición 2.1.1. Una K-*biálgebra* es un K-espacio vectorial B junto con transformaciones lineales m_B, λ_B, Δ_B y ϵ_B que satisfacen las siguientes condiciones:

(i) (B, m_B, λ_B) es una K-álgebra;

(ii) $(B, \Delta_B, \epsilon_B)$ es una K-coálgebra; y

(iii) Δ_B y ϵ_B son morfismos de K-álgebras.

Notemos que (iii) es equivalente a la condición:

(iii') m_B y λ_B son morfismos de K-coálgebras.

Observación. La condición de que $\Delta_B\colon B \to B \otimes B$ sea morfismo de álgebras implica que

$$\begin{aligned}\Delta_B(ab) &= \sum_{(ab)} (ab)_{(1)} \otimes (ab)_{(2)} = \Delta_B(a)\Delta_B(b) \\ &= \left(\sum_{(a)} a_{(1)} \otimes a_{(2)}\right)\left(\sum_{(b)} b_{(1)} \otimes b_{(2)}\right) = \sum_{(a,b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)},\end{aligned}$$

para $a, b \in B$.

Sea B una biálgebra. Un elemento $b \in B$ tal que $\Delta_B(b) = 1 \otimes b + b \otimes 1$ es un **elemento primitivo** de B.

Ejemplo 2.1.2. Sean K un cuerpo y S un monoide. Entonces el anillo del monoide KS es una K-álgebra con multiplicación dada por $m_{KS}(a \otimes b) = ab$ y con unidad $\lambda_{KS}(r) = r$ para todo $a, b \in KS, r \in K$. Sea $\Delta_{KS}\colon KS \to KS \otimes KS$ la aplicación dada por

$$\Delta_{KS}\left(\sum_{s \in S} r_s s\right) = \sum_{s \in S} r_s(s \otimes s),$$

y sea $\epsilon_{KS}\colon KS \to K$ la transformación

$$\epsilon_{KS}\left(\sum_{s \in S} r_s s\right) = \sum_{s \in S} r_s.$$

Entonces, $(KS, \Delta_{KS}, \epsilon_{KS})$ es K-coálgebra por el Ejemplo 1.2.12. Más aún, veamos que Δ_{KS} y ϵ_{KS} son morfismos de K-álgebras. Ambas aplicaciones son lineales, por lo cual basta con verificar las condiciones para los elementos de la base, es decir, de S. Para lo primero,

$$\begin{aligned}\Delta_{KS}(m_{KS}(a \otimes b)) &= \Delta_{KS}(ab) = ab \otimes ab \\ &= m_{KS \otimes KS}((a \otimes a) \otimes (b \otimes b)) = m_{KS \otimes KS}(\Delta_{KS}(a) \otimes \Delta_{KS}(b))\end{aligned}$$

para todo $a, b \in S$. Además,

$$\begin{aligned}\Delta_{KS}(\lambda_{KS}(r)) &= \Delta_{KS}(r) = r(1_{KS} \otimes 1_{KS}) \\ &= r \otimes 1_{KS} = \lambda_{KS}(r) \otimes 1_{KS} = \lambda_{KS\otimes KS}(r)\end{aligned}$$

para todo $r \in K$. Por otro lado,

$$\epsilon_{KS}(m_{KS}(a \otimes b)) = \epsilon_{KS}(ab) = 1_K = m_K(1_K \otimes 1_K) = m_K(\epsilon_{KS}(a) \otimes \epsilon_{KS}(b))$$

para todo $a, b \in S$. Además,

$$\epsilon_{KS}(\lambda_{KS}(r)) = \epsilon_{KS}(r) = r = \lambda_K(r)$$

para todo $r \in K$. Tenemos entonces que $(KS, m_{KS}, \lambda_{KS}, \Delta_{KS}, \epsilon_{KS})$ es una K-biálgebra. Se conoce como la **biálgebra del monoide**.

Ejemplo 2.1.3. Consideremos la K-álgebra de polinomios $K[x]$ con estructura de K-coálgebra como en el Ejemplo 1.2.17. Veamos que las transformaciones $\Delta_{K[x]}$ y $\epsilon_{K[x]}$ son morfismos de álgebras. Sean $n, m \in \mathbb{N}_0$,

$$\begin{aligned}\Delta_{K[x]}(m_{K[x]}(x^n \otimes x^m)) &= \Delta_{K[x]}(x^{n+m}) = x^{n+m} \otimes x^{n+m} \\ &= m_{K[x]\otimes K[x]}((x^n \otimes x^n) \otimes (x^m \otimes x^m)) \\ &= m_{K[x]\otimes K[x]}(\Delta_{K[x]}(x^n) \otimes \Delta_{K[x]}(x^m)).\end{aligned}$$

Además,

$$\Delta_{K[x]}(\lambda_{K[x]}(r)) = \Delta_{K[x]}(r) = r(1 \otimes 1) = r \otimes 1 = \lambda_{K[x]\otimes K[x]}(r)$$

para todo $r \in K$. Por otro lado,

$$\epsilon_{K[x]}(m_{K[x]}(x^n \otimes x^m)) = \epsilon_{K[x]}(x^{n+m}) = 1 = m_K(1 \otimes 1) = m_K(\epsilon_{K[x]}(x^n) \otimes \epsilon_{K[x]}(x^m)).$$

Además,

$$\epsilon_{K[x]}(\lambda_{K[x]}(r)) = \epsilon_{K[x]}(r) = r = \lambda_K(r)$$

para todo $r \in K$. Luego, $(K[x], m_{K[x]}, \lambda_{K[x]}, \Delta_{K[x]}, \epsilon_{K[x]})$ es K-biálgebra. Como $\Delta_{K[x]}(x) = x \otimes x$, se la llama **biálgebra de polinomios con x de tipo grupo**.

Ejemplo 2.1.4. Consideremos ahora $K[x]$ con la estructura de K-coálgebra del Ejemplo 1.2.18. Las aplicaciones de la estructura de coálgebra son morfismos de álgebras, pues:

$$\Delta_{K[x]}(m_{K[x]}(x^n \otimes x^m)) = \Delta_{K[x]}(x^{n+m}) = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k \otimes x^{n+m-k}.$$

Por otro lado,

$$
\begin{aligned}
m_{K[x]}(\Delta_{K[x]}(x^n)\otimes\Delta_{K[x]}(x^m)) &= \left(\sum_{i=0}^{n}\binom{n}{i}x^i\otimes x^{n-i}\right)\left(\sum_{j=0}^{m}\binom{m}{j}x^j\otimes x^{m-j}\right)\\
&= \sum_{i=0}^{n}\sum_{j=0}^{m}\binom{n}{i}\binom{m}{j}x^{i+j}\otimes x^{n+m-(i+j)} = \sum_{k=0}^{n+m}\sum_{i=0}^{k}\binom{n}{i}\binom{m}{k-i}x^k\otimes x^{n+m-k}\\
&= \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k}\binom{n}{i}\binom{m}{k-i}\right)x^k\otimes x^{n+m-k} = \sum_{k=0}^{n+m}\binom{n+m}{k}x^k\otimes x^{n+m-k}.
\end{aligned}
$$

Además,

$$\Delta_{K[x]}(\lambda_{K[x]}(r)) = \Delta_{K[x]}(r) = r(1\otimes 1) = r\otimes 1 = \lambda_{K[x]\otimes K[x]}(r)$$

para todo $r\in K$. Luego, $\Delta_{K[x]}$ es morfismo de K-álgebras. Ahora,

$$
\begin{aligned}
\epsilon_{K[x]}(m_{K[x]}(x^n\otimes x^m)) &= \epsilon_{K[x]}(x^{n+m}) = \delta_{0,n+m} = \delta_{0,n}\delta_{0,m}\\
&= \epsilon_{K[x]}(x^n)\epsilon_{K[x]}(x^m) = m_K(\epsilon_{K[x]}(x^n)\otimes\epsilon_{K[x]}(x^m)).
\end{aligned}
$$

Además,

$$\epsilon_{K[x]}(\lambda_{K[x]}(r)) = \epsilon_{K[x]}(r) = r = \lambda_K(r)$$

para todo $r\in K$. Luego, $(K[x], m_{K[x]}, \lambda_{K[x]}, \Delta_{K[x]}, \epsilon_{K[x]})$ es K-biálgebra. Como $\Delta_{K[x]}(x) = 1\otimes x + x\otimes 1$, se llama **biálgebra de polinomios con x primitivo**.

Definición 2.1.5. Sea B una K-biálgebra. Un *biideal* I es un subespacio vectorial de B que es ideal y coideal a la vez.

Proposición 2.1.6. *Sea $I\subseteq B$ un biideal de B. Entonces, B/I es una K-biálgebra.*

Demostración. Por la Proposición 1.2.8, tenemos que B/I es K-álgebra. Por la Proposición 1.2.20, B/I es K-coálgebra. Veamos primero que $\Delta_{B/I}$ es morfismo de K-álgebras. Sean $c, d\in B$

$$
\begin{aligned}
\Delta_{B/I}(m_{B/I}((c+I)\otimes(d+I))) = \Delta_{B/I}(cd+I) &= \left(\sum_{(cd)}((cd)_{(1)}+I)\otimes((cd)_{(2)}+I)\right)\\
&= \left(\sum_{(c)}(c_{(1)}+I)\otimes(c_{(2)}+I)\right)\left(\sum_{(d)}(d_{(1)}+I)\otimes(d_{(2)}+I)\right)\\
&= m_{B/I\otimes B/I}((\Delta_{B/I}(c+I)\otimes(\Delta_{B/I}(d+I)))
\end{aligned}
$$

donde hemos usado que Δ_B es morfismo de K-álgebras en el pasaje de la segunda a la tercera línea. Además, sea $r\in K$

$$
\begin{aligned}
\Delta_{B/I}(\lambda_{B/I}(r)) = \Delta_{B/I}(\lambda_B(r)+I) &= \Delta_{B/I}(r(\lambda_B(1)+I)) = r\Delta_{B/I}(1_B+I)\\
&= r(1_B+I)\otimes(1_B+I) = (r1_B+I)\otimes(1_B+I)\\
&= (\lambda_B(r)+I)\otimes(1_B+I) = \lambda_{B/I}(r)\otimes 1_{B/I}.
\end{aligned}
$$

Aquí usamos que $\Delta_B(1_B) = 1_B \otimes 1_B$ porque es morfismo de K-álgebras ($\Delta_B(1_B) = \Delta_B(1_B 1_B) = \Delta_B(1_B)\Delta_B(1_B)$, entonces $\Delta_B(1_B)$ es el neutro de $B \otimes B$ que es el $1_B \otimes 1_B$). Entonces, $\Delta_{B/I}$ es morfismo de K-álgebras. Por otro lado, sean $c, d \in B$

$$\begin{aligned}\epsilon_{B/I}(m_{B/I}((c+I) \otimes (d+I))) &= \epsilon_{B/I}(cd+I) = \epsilon_B(cd) \\ &= \epsilon_B(c)\epsilon_B(d) = m_K(\epsilon_B(c) \otimes \epsilon_B(d))\end{aligned}$$

donde usamos que ϵ_B es morfismo de K-álgebras para pasar de la primera a la segunda línea. Además, sea $r \in K$

$$\epsilon_{B/I}(\lambda_{B/I}(r)) = \epsilon_{B/I}(\lambda_B(r) + I) = \epsilon_B(\lambda_B(r)) = \lambda_K(r)$$

donde, en la última igualdad, volvimos a usar que ϵ_B es morfismo de K-álgebras. En consecuencia, B/I tiene estructura de K-biálgebra. □

Definición 2.1.7. Sean B, B' biálgebras. Una transformación lineal $\phi \colon B \to B'$ es un *morfismo de biálgebras* si ϕ es morfismo de álgebras y de coálgebras a la vez.

Observación. Un morfismo de biálgebras biyectivo es un **isomorfismo de biálgebras**.

Es notable destacar que las estructuras de biálgebra dadas en los Ejemplos 2.1.3 y 2.1.4 son las únicas estructuras de biálgebras que se pueden definir sobre $K[x]$ salvo isomorfismo de álgebras.

Proposición 2.1.8. *Supongamos que el álgebra usual de polinomios en una variable $K[x]$ tiene estructura de biálgebra. Entonces, existe $z \in K[x]$ tal que $K[z] \cong K[x]$ con z un elemento o bien de tipo grupo o bien primitivo (el isomorfismo es de álgebras).*

Demostración. Sea $K[x]$ una biálgebra y supongamos que

$$\Delta_{K[x]}(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} x^i \otimes x^j \in K[x] \otimes K[x],$$

para $b_{i,j} \in K$. Es decir, $\Delta_{K[x]}(x)$ es una suma finita de tensores $b_{i,j}x^i \otimes x^j$ donde i es el grado de x en el factor izquierdo del tensor y j es el grado de x en el factor derecho del tensor. Denotemos por l al mayor grado de x que aparece en los factores izquierdos de los tensores de la suma $\Delta_{K[x]}$. Entonces, $b_{l,j} \neq 0$ para ciertos $j, 0 \leq j \leq n$. Sea j' el mayor índice j tal que $b_{l,j} \neq 0$. Ahora,

$$(I_{K[x]} \otimes \Delta_{K[x]})\Delta_{K[x]}(x) \in K[x] \otimes K[x] \otimes K[x]$$

es una suma finita de tensores de la forma $cx^i \otimes x^j \otimes x^k, c \in K$; i es el grado de x en el factor izquierdo del tensor y k es el grado del factor derecho del tensor. Notemos que l es el mayor grado de x en el factor izquierdo de esta nueva suma puesto que, en la primera coordenada, aplicamos la identidad. Por otro lado,

$$\begin{aligned}(\Delta_{K[x]} \otimes I_{K[x]})\Delta_{K[x]}(x) &= (\Delta_{K[x]} \otimes I_{K[x]}) \left(\sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} x^i \otimes x^j \right) \\ &= \sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} \Delta_{K[x]}(x^i) \otimes x^j = \sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} (\Delta_{K[x]}(x))^i \otimes x^j\end{aligned}$$

pues $\Delta_{K[x]}$ es morfismo de álgebras, y entonces

$$\begin{aligned}(\Delta_{K[x]} \otimes I_{K[x]})\Delta_{K[x]}(x) &= \sum_{i=0}^{m} \sum_{j=0}^{n} b_{i,j} \left(\sum_{\alpha=0}^{m} \sum_{\beta=0}^{n} b_{\alpha,\beta} x^\alpha \otimes x^\beta \right)^i \otimes x^j \\ &= b_{l,j'}^{l+1} x^{l^2} \otimes x^{lj'} \otimes x^{j'} + T,\end{aligned}$$

donde T es una suma de tensores en $K[x] \otimes K[x] \otimes K[x]$ de la forma $cx^i \otimes x^j \otimes x^k$ con $i \leq l^2$. Como $b_{l,j'} \neq 0$, la mayor potencia de x que aparece en los factores izquierdos de los tensores de la suma $(\Delta_{K[x]} \otimes I_{K[x]})\Delta_{K[x]}(x)$ es l^2. Por la coasociatividad del $\Delta_{K[x]}$, tenemos $l^2 = l$. Luego, $l = 0$ o $l = 1$. Argumentando de la misma manera, llamando r al mayor grado de x que aparece en los factores derechos de los tensores de la suma $\Delta_{K[x]}(x)$, llegamos a $r = 0$ o $r = 1$. En consecuencia, tenemos

$$\Delta_{K[x]}(x) = b_{0,0}(1 \otimes 1) + b_{0,1}(1 \otimes x) + b_{1,0}(x \otimes 1) + b_{1,1}(x \otimes x),$$

para $b_{0,0}, b_{0,1}, b_{1,0}, b_{1,1} \in K$. Sea $y = x - \epsilon_{K[x]}(x)$ y sea $\Delta_{K[x]}(y) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{i,j} y^i \otimes y^j$. Comparando las expresiones $(\Delta_{K[x]} \otimes I_{K[x]})\Delta_{K[x]}(y)$ y $(I_{K[x]} \otimes \Delta_{K[x]})\Delta_{K[x]}(y)$ como antes, concluimos que $a_{i,j} = 0$ si $i > 1$ o $j > 1$. Como $\epsilon_{K[x]}(y) = 0$, aplicamos la propiedad de la counidad a y y tenemos que $a_{0,0} = 0$ y $a_{0,1} = a_{1,0} = 1$. Entonces,

$$\Delta_{K[x]}(y) = 1 \otimes y + y \otimes 1 + ay \otimes y$$

para algún $a \in K$. Si $a = 0$, entonces tomamos $z = y$ y $K[z] \cong K[x]$ con z primitivo. Si $a \neq 0$, tomamos $z = 1 + ay$ y entonces $K[z] \cong K[x]$ con z de tipo grupo. $\square$

Sea B una biálgebra y A un álgebra con estructura de B-módulo a izquierda con la acción notada por "$\cdot$". Entonces decimos que A es un **B-módulo álgebra a izquierda** si

$$b \cdot (aa') = \sum_{(b)} (b_{(1)} \cdot a)(b_{(2)} \cdot a') \qquad \text{y} \qquad b \cdot 1_A = \epsilon_B(b) 1_A$$

para todos $a, a' \in A, b \in B$. Sean A y A' K-álgebras. Una transformación K-lineal $\phi\colon A \to A'$ es un **morfismo de B-módulo álgebras a izquierda** si ϕ es morfismo de álgebras y morfismo de B-módulos a izquierda simultáneamente. Sea

C una coálgebra que es B-módulo a derecha con la acción notada por "$\cdot$". Entonces decimos que C es **B-módulo coálgebra a derecha** si

$$\Delta_C(c \cdot b) = \sum_{(c,b)} c_{(1)} \cdot b_{(1)} \otimes c_{(2)} \cdot b_{(2)} \qquad \text{y} \qquad \epsilon_C(c \cdot b) = \epsilon_C(c)\epsilon_B(b)$$

para todos $c \in C, b \in B$. Sean C y C' K-coálgebras. Una transformación K-lineal $\phi\colon C \to C'$ es **morfismo de B-módulo coálgebras a derecha** si ϕ es morfismo de coálgebras y morfismo de B-módulos a derecha simultáneamente.

Sea B una biálgebra. Existe una estructura de B-módulo a izquierda en B^* definida como

$$(a \rightharpoonup f)(b) = f(ba)$$

para $a, b \in B, f \in B^*$. Para $a \in B$ y $f \in B^*$, el elemento $a \rightharpoonup f$ se dice **traslado a izquierda de f por a**. La acción del traslado a izquierda le da a B^* estructura de B-módulo álgebra a izquierda. En efecto, definimos para $f, g \in B^*, a, b \in B$

$$\begin{aligned}(a \rightharpoonup fg)(b) &= (fg)(ba) = m_{B^*}(f \otimes g)(ba) = (f \otimes g)\Delta_B(ba)\\ &= (f \otimes g)\left(\sum_{(b,a)} b_{(1)}a_{(1)} \otimes b_{(2)}a_{(2)}\right) = \sum_{(b,a)} f(b_{(1)}a_{(1)})g(b_{(2)}a_{(2)})\\ &= \sum_{(b,a)} (a_{(1)} \rightharpoonup f)(b_{(1)})(a_{(2)} \rightharpoonup g)(b_{(2)}) = \left(\sum_{(a)} (a_{(1)} \rightharpoonup f) \otimes (a_{(2)} \rightharpoonup g)\right)(\Delta_B(b))\\ &= m_{B^*}\left(\sum_{(a)} (a_{(1)} \rightharpoonup f) \otimes (a_{(2)} \rightharpoonup g)\right)(b) = \left(\sum_{(a)} (a_{(1)} \rightharpoonup f)(a_{(2)} \rightharpoonup g)\right)(b).\end{aligned}$$

Más aún,

$$(a \rightharpoonup 1_{B^*})(b) = 1_{B^*}(ba) = \epsilon_B(ba) = \epsilon_B(b)\epsilon_B(a) = (\epsilon_B(a)1_{B^*})(b).$$

De forma análoga, hay una estructura de B-módulo a derecha en B^* dada por

$$(f \leftharpoonup a)(b) = f(ab)$$

par todo $a, b \in B, f \in B^*$. Para $a \in B$ y $f \in B^*$, el elemento $f \leftharpoonup a$ se dice **traslado a derecha de f por a**. Notemos que $f \leftharpoonup B = \{f \leftharpoonup b\colon b \in B\}$ es un subespacio de B^*. Por ejemplo, sea $K[x]$ la biálgebra de polinomios con x de tipo grupo. Hay una estructura de $K[x]$-módulo a derecha en $K[x]^*$ definida por

$$(f \leftharpoonup x^j)(x^k) = f(x^{j+k})$$

para $f \in K[x]^*$ y $k, j \geq 0$. Si notamos por e_i la aplicación definida por $e_i(x^j) = \delta_{i,j}$, tenemos

$$(e_i \leftharpoonup x^j)(x^k) = e_i(x^{j+k}) = \delta_{i,j+k}.$$

Luego,

$$e_i \leftharpoonup x^j = \begin{cases} e_{i-j} & si \quad i \geq j \\ 0 & si \quad i < j. \end{cases}$$

Notemos que $e_i \leftharpoonup K[x]$ es el subespacio de $K[x]^*$ generado por $\{e_0, e_1, \dots, e_i\}$. Por lo tanto, $\dim(e_i \leftharpoonup K[x]) = i + 1$.

Recordemos ahora una definición del álgebra lineal para fijar la notación.

Definición 2.1.9. Sea V un espacio vectorial,

(i) si $W \subseteq V$ es un subespacio, definimos $W^\perp = \{f \in V^* : f(W) = 0\}$;

(ii) si $U \subseteq V^*$ es un subespacio, definimos $U^\perp = \{v \in V : v \in \ker(f), \forall f \in U\}$.

Podemos probar el siguiente Lema que es parte de una demostración mayor en [Mon93, Lema 9.1.1]:

Lema 2.1.10. *Sea B una K-biálgebra. Sea $f \in B^*$. Son equivalentes:*

(i) $dim(f \leftharpoonup B) < \infty$

(ii) $f \in B^\circ$

Demostración. $\underline{(i) \Rightarrow (ii)}$: Sea $I = (f \leftharpoonup B)^\perp$. Veamos que I es un ideal cofinito. Para ello, consideremos la aplicación $\Phi \colon B \to (f \leftharpoonup B)^*$ definida como

$$\begin{aligned} a \mapsto \Phi(a) \colon (f \leftharpoonup B) &\to K \\ f \leftharpoonup b &\longmapsto (f \leftharpoonup b)(a) = f(ba). \end{aligned}$$

Esta aplicación está bien definida y es una transformación K-lineal. Notemos ahora que

$$\ker(\Phi) = \{a \in B \colon f(ba) = 0, \forall b \in B\} = (f \leftharpoonup B)^\perp = I$$

Tenemos entonces, por la propiedad universal del cociente, un isomorfismo $B/I \cong (f \leftharpoonup B)^*$. Como $\dim(f \leftharpoonup B)$ es finita por hipótesis, I es un ideal cofinito. Resta ver que f se anula sobre I. En efecto, dado $b \in (f \leftharpoonup B)^\perp$, resulta que $b \in \ker(f \leftharpoonup a), \forall a \in B$; es decir, $f(ab) = 0, \forall a \in B$. En particular, para $a = 1_B$ tenemos que $f(b) = 0$. Luego, $I \in \ker(f)$. En consecuencia, $f \in B^\circ$.

$\underline{(ii) \Rightarrow (i)}$: Sea I un ideal cofinito tal que $f(I) = 0$. Para todo $b \in B$, se cumple que $bI \subseteq I$. Luego, $f(bI) = 0$; es decir, $(f \leftharpoonup b)(I) = 0$. De esto se deduce que $f \leftharpoonup b \in I^\perp, \forall b \in B$. Entonces, $f \leftharpoonup B \subseteq I^\perp$. Como $I^\perp$ es de dimensión finita, la contención prueba lo que queríamos. $\square$

Podemos ilustrar una parte del Lema 2.1.10 con un pequeño ejemplo. Como antes, $\dim(e_i \leftharpoonup K[x]) = i + 1$, y entonces $e_i \in K[x]^\circ$. De hecho, e_i se corresponde con la sucesión recursiva lineal de orden $i + 1$ en K con polinomio característico $f(x) = x^{i+1}$ y vector inicial $\underbrace{000\dots1}_{i+1}$. Además, e_i se anula sobre el ideal (x^{i+1}) de codimensión $i + 1$. El Lema 2.1.10 es muy importante para probar la siguiente proposición.

Proposición 2.1.11. *Si B es una biálgebra, entonces B° es una biálgebra.*

Demostración. Veamos primero que B° es un álgebra. Para ello, necesitamos construir una multiplicación m_{B° y una unidad λ_{B° que satisfagan las propiedades asociativa y de la unidad, respectivamente.

Por la Proposición 1.3.1, B^* es álgebra con multiplicación $m_{B^*} = \Delta_B^*$ y unidad $\lambda_{B^*} = \epsilon_B^*$. Notemos por m_{B° la restricción de m_{B^*} a B°. Debemos ver que nos queda bien definida la aplicación $m_{B^\circ}\colon B^\circ \otimes B^\circ \to B^\circ$. Para ello, sean $f, g \in B^\circ$ y $a, b \in B$. Luego,

$$\begin{aligned}(fg \leftharpoonup a)(b) &= (m_{B^*}(f\otimes g) \leftharpoonup a)(b) = m_{B^*}(f\otimes g)(ab) = (f\otimes g)\Delta_B(ab)\\ &= (f\otimes g)\left(\sum_{(a),(b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)}\right) = \sum_{(a),(b)} f(a_{(1)}b_{(1)})g(a_{(2)}b_{(2)})\\ &= \sum_{(a),(b)} (f \leftharpoonup a_{(1)})(b_{(1)})(g \leftharpoonup a_{(2)})(b_{(2)}).\end{aligned}$$

Más aún,

$$\begin{aligned}&\textstyle\sum_{(a),(b)}(f \leftharpoonup a_{(1)})(b_{(1)})(g \leftharpoonup a_{(2)})(b_{(2)}) = \displaystyle\sum_{(a),(b)} ((f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}))(b_{(1)} \otimes b_{(2)})\\ &= \sum_{(a)}((f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}))\left(\sum_{(b)} b_{(1)} \otimes b_{(2)}\right)\\ &= \sum_{(a)}((f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}))\Delta_B(b) = \sum_{(a)} m_{B^*}((f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}))(b)\\ &= \left(\sum_{(a)}(f \leftharpoonup a_{(1)})(g \leftharpoonup a_{(2)})\right)(b).\end{aligned}$$

En consecuencia, $fg \leftharpoonup B \subseteq \operatorname{span}((f \leftharpoonup B)(g \leftharpoonup B))$. Por el Lema 2.1.10 tenemos que $\dim(f \leftharpoonup B) < \infty$ y $\dim(g \leftharpoonup B) < \infty$, entonces $\dim(\operatorname{span}((f \leftharpoonup B)(g \leftharpoonup B))) < \infty$. En consecuencia, $\dim(fg \leftharpoonup B) < \infty$. Se sigue entonces, por el mismo lema, que $fg \in B^\circ$. Esto nos da la buena definición. Además, como m_{B^*} satisface la propiedad asociativa, m_{B° también.

Ahora, vamos a ver cómo es la unidad. Elegimos como candidato natural a $\lambda_{B^*}\colon K \to B^*$ pero debemos ver que $\lambda_{B^*}(K) \subseteq B^\circ$. Notemos que $\lambda_{B^*}(r) = r\lambda_{B^*}(1_K) = r1_{B^*} = r\epsilon_B$. Ahora, $\ker(\epsilon_B)$ es un ideal de B de codimensión finita pues el codominio de ϵ_B es K. Luego, $\epsilon_B \in B^\circ$ y entonces $\lambda_{B^*}\colon K \to B^\circ$ como queríamos. Tomamos pues $\lambda_{B^\circ} = \lambda_{B^*}$ y tenemos que $(B^\circ, m_{B^\circ}, \lambda_{B^\circ})$ es una K-álgebra.

Por la Proposición 1.3.9, B° es una coálgebra con comultiplicación Δ_{B° y counidad ϵ_{B°. Debemos ver que estas transformaciones son morfismos de álgebras para verificar que B° es biálgebra. Sean $f, g \in B^\circ$ y $a, b \in B$:

$$\begin{aligned}
\Delta_{B^\circ}(fg)(a \otimes b) &= \Delta_{B^\circ}(m_{B^\circ}(f \otimes g))(a \otimes b) = m_{B^\circ}(f \otimes g)(m_B(a \otimes b)) \\
&= m_{B^\circ}(f \otimes g)(ab) = (f \otimes g)\Delta_B(ab) \\
&= (f \otimes g)\left(\sum_{(a),(b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)}\right) = \sum_{(a),(b)} f(a_{(1)}b_{(1)})g(a_{(2)}b_{(2)}).
\end{aligned} \tag{2.1}$$

Ahora,

$$\begin{aligned}
\sum_{(a),(b)} f(a_{(1)}b_{(1)})g(a_{(2)}b_{(2)}) &= \sum_{(a),(b)} f(m_B(a_{(1)} \otimes b_{(1)}))g(m_B(a_{(2)} \otimes b_{(2)})) \\
&= \sum_{(a),(b)} \Delta_{B^\circ}(f)(a_{(1)} \otimes b_{(1)})\Delta_{B^\circ}(g)(a_{(2)} \otimes b_{(2)}) \\
&= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(I \otimes \tau \otimes I)\left(\sum_{(a),(b)} (a_{(1)} \otimes a_{(2)} \otimes b_{(1)} \otimes b_{(2)})\right) \\
&= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(I \otimes \tau \otimes I)(\Delta_B \otimes \Delta_B)(a \otimes b) \\
&= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))\Delta_{B \otimes B}(a \otimes b).
\end{aligned} \tag{2.2}$$

Luego,

$$\begin{aligned}
(\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))\Delta_{B \otimes B}(a \otimes b) &= \Delta^*_{B^* \otimes B^*}(\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(a \otimes b) \\
&= m_{B^\circ \otimes B^\circ}(\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(a \otimes b) = (\Delta_{B^\circ}(f)\Delta_{B^\circ}(g))(a \otimes b).
\end{aligned} \tag{2.3}$$

A partir de (2.1), (2.2) y (2.3) obtenemos

$$\Delta_{B^\circ}(fg) = \Delta_{B^\circ}(f)\Delta_{B^\circ}(g),$$

y entonces Δ_{B° es morfismo de álgebras. Para terminar, veamos lo que ocurre con ϵ_{B°. Sea $r \in K$,

$$\begin{aligned}
\epsilon_{B^\circ}(fg)(r) &= (fg)\lambda_B(r) = (m_{B^\circ}(f \otimes g))(\lambda_B(r1_K)) \\
&= r(m_{B^\circ}(f \otimes g))(1_B) = r(f \otimes g)(\Delta_B(1_B)) \\
&= r(f \otimes g)(1_B \otimes 1_B) = rf(1_B)g(1_B).
\end{aligned}$$

Por la demostración de la Proposición 1.3.9 tenemos la igualdad

$$\epsilon_{B^\circ}(f) = f(1_B),$$

luego

$$rf(1_B)g(1_B) = r\epsilon_{B^\circ}(f)\epsilon_{B^\circ}(g) = (\epsilon_{B^\circ}(f)\epsilon_{B^\circ}(g))(r).$$

En consecuencia,

$$\epsilon_{B^\circ}(fg) = \epsilon_{B^\circ}(f)\epsilon_{B^\circ}(g)$$

y entonces ϵ_{B° es un morfismo de álgebras. Esto completa la prueba. □

Proposición 2.1.12. *Si B es coconmutativa, entonces B° es conmutativa. Si B es conmutativa, B° es coconmutativa.*

Demostración. Se trata de un caso particular de la Proposición 1.3.12. □

Proposición 2.1.13. *Supongamos que B es un K-espacio vectorial de dimensión finita. Entonces, B es una biálgebra si y sólo si B^* es una biálgebra.*

Demostración. Como B de dimensión finita, $B^\circ = B^*$. Si B es una biálgebra, entonces B^* es biálgebra por la Proposición 2.1.11. Ahora, si B^* es una biálgebra, entonces $(B^*)^\circ$ es una biálgebra por la Proposición 2.1.11. Pero, como $\dim(B^*) = \dim(B) < \infty, (B^*)^\circ = B^{**}$ (el doble dual) que se identifica con B. Entonces B es una biálgebra. □

2.1.1. Aplicación de la teoría de biálgebras a las sucesiones recursivas lineales

Como hemos visto en el capítulo anterior, si $K[x]$ es el álgebra de polinomios entonces la coálgebra $K[x]^\circ$ es la colección de sucesiones recursivas lineales sobre K de todos los órdenes. Como vimos en los Ejemplos 1.2.17 y 1.2.18, hay dos estructuras de coálgebra que hacen de $K[x]$ una biálgebra. De hecho, por la Proposición 2.1.8 hay exactamente dos estructuras de biálgebras en $K[x]$ salvo isomorfismo de álgebras. En consecuencia, por la Proposición 2.1.11, tenemos dos estructuras de biálgebra en $K[x]^\circ$.

Esto significa que podemos multiplicar sucesiones recursivas lineales de dos formas diferentes (y obtener una sucesión recursiva lineal). Vamos a ver en detalle cómo son estas dos multiplicaciones.

En primer lugar, si $K[x]$ es la biálgebra con x un elemento de tipo grupo, entonces $K[x]^\circ$ es la biálgebra con multiplicación definida a partir de la comultiplicación de $K[x]$ como se describe a continuación y que notaremos por "$\cdot$".

Para $\{s_n\}$, $\{t_n\} \in K[x]^\circ$, si $g(x) = \sum_{i=0}^{l} a_i x^i \in K[x]$,

$$\begin{aligned}
(\{s_n\} \cdot \{t_n\})(g(x)) &= (m_{K[x]^\circ}(\{s_n\} \otimes \{t_n\}))(g(x)) = (\{s_n\} \otimes \{t_n\})\Delta_{K[x]}(g(x)) \\
&= (\{s_n\} \otimes \{t_n\})\Delta_{K[x]}\left(\sum_{i=0}^{l} a_i x^i\right) = (\{s_n\} \otimes \{t_n\}) \sum_{i=0}^{l} a_i (x^i \otimes x^i) \\
&= \sum_{i=0}^{l} a_i \{s_n\}(x^i)\{t_n\}(x^i) = \sum_{i=0}^{l} a_i s_i t_i \\
&= \{s_n t_n\}(g(x)).
\end{aligned}$$

Esto es lo que se conoce como **producto de Hadamard** para sucesiones recursivas lineales. El producto $\{s_n\} \cdot \{t_n\} = \{s_n t_n\}$ es una sucesión recursiva lineal, pero ¿cómo hallamos su polinomio característico? Consideraremos la situación en que ambas sucesiones son geométricas. Sea $\{s_n\}$ una sucesión geométrica con polinomio característico $f(x) = x - \alpha, \alpha \in K$ y vector inicial s_0; y sea $\{t_n\}$ una sucesión geométrica con polinomio característico $g(x) = x - \beta, \beta \in K$ y vector inicial t_0. Entonces, el producto de Hadamard es

$$\{s_n\} \cdot \{t_n\} = \{s_n t_n\} = \{s_0 \alpha^n t_0 \beta^n\} = \{s_0 t_0 (\alpha\beta)^n)$$

que es una sucesión geométrica con polinomio característico $h(x) = x - \alpha\beta$ y vector inicial $s_0 t_0$.

Si ahora notamos por $K[x]'$ a la biálgebra de polinomios con x primitivo, entonces $K[x]'^{\circ}$ es una biálgebra y la multiplicación se llama **producto de Hurwitz** que notaremos por "$*$".

Para $\{s_n\}, \{t_n\} \in K[x]'^{\circ}, g(x) = \sum_{i=0}^{l} a_i x^i \in K[x]$,

$$\begin{aligned}
(\{s_n\} * \{t_n\})(g(x)) &= (m_{K[x]'^{\circ}}(\{s_n\} \otimes \{t_n\}))(g(x)) = (\{s_n\} \otimes \{t_n\})\Delta_{K[x]'}(g(x)) \\
&= (\{s_n\} \otimes \{t_n\})\Delta_{K[x]'}\left(\sum_{i=0}^{l} a_i x^i\right) \\
&= (\{s_n\} \otimes \{t_n\}) \sum_{i=0}^{l} a_i \sum_{j=0}^{i} \binom{i}{j} (x^j \otimes x^{i-j}) \\
&= \sum_{i=0}^{l} a_i \sum_{j=0}^{i} \binom{i}{j} \{s_n\}(x^j)\{t_n\}(x^{i-j}) = \sum_{i=0}^{l} a_i \sum_{j=0}^{i} \binom{i}{j} s_j t_{i-j} \\
&= \left\{ \sum_{j=0}^{n} \binom{n}{j} s_j t_{n-j} \right\} (g(x)).
\end{aligned}$$

Nuevamente podemos preguntarnos cómo hallar el polinomio característico del producto. Consideremos $\{s_n\}, \{t_n\}$ sucesiones geométricas como antes. Tenemos

$$\begin{aligned}
\{s_n\} * \{t_n\} &= \left\{ \sum_{j=0}^{n} \binom{n}{j} s_j t_{n-j} \right\} = \left\{ \sum_{j=0}^{n} \binom{n}{j} s_0 \alpha^j t_0 \beta^{n-j} \right\} \\
&= \left\{ s_0 t_0 \sum_{j=0}^{n} \binom{n}{j} \alpha^j \beta^{n-j} \right\} = \{s_0 t_0 (\alpha + \beta)^n\},
\end{aligned}$$

que es una sucesión geométrica con polinomio característico $h(x) = x - (\alpha + \beta)$ y vector inicial $s_0 t_0$.

Estas son las ideas esenciales detrás de las siguientes proposiciones que damos sin demostración por profundizar en ideas que no forman parte del objetivo de esta tesis. Fueron tomadas de [Und15] que a su vez las adapta de [CG93] y [ZM73].

Proposición 2.1.14. *Sea K un cuerpo que contiene a $\mathbb{Q}$. Sea $\{s_n\}$ una sucesión recursiva lineal de orden k sobre K con polinomio característico $f(x)$ y $\{t_n\}$ una sucesión recursiva lineal de orden l sobre K con polinomio característico $g(x)$. Supongamos que tanto $f(x)$ como $g(x)$ tienen raíces distintas en alguna extensión $L|K$. Si α_i con $0 \leq i \leq k$ denota las raíces distintas de $f(x)$ y β_j con $0 \leq j \leq l$*

denota las de $g(x)$, entonces el polinomio característico del producto de Hadamard $\{s_n\} \cdot \{t_n\} = \{s_n t_n\}$ es

$$h(x) = \prod_{\substack{1 \le i \le k, \\ 1 \le j \le l, \\ \alpha_i \beta_j \text{ distintos}}} (x - \alpha_i \beta_j).$$

Proposición 2.1.15. *Con las mismas hipótesis de la proposición anterior, tenemos que el polinomio característico del producto de Hurwitz*

$$\{s_n\} * \{t_n\} = \left\{ \sum_{j=0}^{n} \binom{n}{j} s_j t_{n-j} \right\}$$

es

$$h(x) = \prod_{\substack{1 \le i \le k, \\ 1 \le j \le l, \\ \alpha_i + \beta_j \text{ distintos}}} (x - (\alpha_i + \beta_j)).$$

Ejemplo 2.1.16. Sea $\{s_n\}$ la sucesión de Fibonacci en $\mathbb{Q}$ con polinomio característico $f(x) = x^2 - x - 1$ y vector inicial $s_0 = (0, 1)$. El producto de Hadamard $\{s_n\} \cdot \{s_n\} = \{s_n^2\}$ es

$$0, 1, 1, 4, 9, 25, 64, 169, \ldots$$

Las raíces de $f(x)$ son $\alpha = \frac{1+\sqrt{5}}{2}$ y $1-\alpha = \frac{1-\sqrt{5}}{2}$; entonces el polinomio característico del producto es

$$\begin{aligned} h(x) &= (x - \alpha^2)(x - \alpha(1 - \alpha))(x - (1 - \alpha)^2) = (x - \alpha^2)(x + 1)(x - (2 - \alpha)) \\ &= (x + 1)(x^2 - 3x + 1) = x^3 - 2x^2 - 2x + 1. \end{aligned}$$

De hecho, el producto es una sucesión $\{r_n\}$ recursiva lineal de orden 3 con relación de recurrencia dada por

$$r_{n+3} = 2r_{n+2} + 2r_{n+1} - r_n$$

y vector inicial $r_0 = (0, 1, 1)$.

Ejemplo 2.1.17. Sea $\{s_n\}$ la sucesión del ejemplo anterior. Entonces, el producto de Hurwitz $\{s_n\} * \{s_n\}$ es

$$0, 0, 2, 6, 22, 70, 230, \ldots$$

Las raíces de $f(x)$ son las mismas de antes. Entonces, el polinomio característico del producto de Hurwitz es

$$h(x) = (x - 2\alpha)(x - 1)(x - (2 - 2\alpha)) = x^3 - 3x^2 - 2x + 4.$$

De hecho, el producto es una sucesión$\{r_n\}$ recursiva lineal de orden 3 con recurrencia

$$r_{n+3} = 3r_{n+2} + 2r_{n+1} - 4r_n$$

y vector inicial $r_0 = (0, 0, 2)$.

2.2. Biálgebras de Myhill–Nerode

En esta sección vamos a aplicar la teoría de biálgebras a los lenguajes formales y los autómatas finitos. Probaremos el Teorema de Myhill–Nerode que nos dice cuándo un lenguaje es aceptado por un autómata finito. Generalizaremos este teorema a una versión algebraica en la que cierta biálgebra (una biálgebra de Myhill–Nerode) de dimensión finita juega el papel de autómata que acepta el lenguaje. Construiremos varios ejemplos y, por último, veremos que todo autómata finito determina una biálgebra de Myhill–Nerode que a su vez determina un autómata finito (no necesariamente el mismo).

Sea $\Sigma = \{a_1, a_2, \dots, a_k\}$ un alfabeto finito y notemos por Σ^* la colección de palabras de longitud finita en las letras de Σ. Una **palabra** $x \in \Sigma^*$ se escribe como

$$x = a_{i_1} a_{i_2} \dots a_{i_m}$$

donde $i_1, i_2, \dots, i_m$ es una sucesión finita de enteros en $\{1, 2, 3, \dots, k\}$. Asumiremos que Σ^* contiene a la palabra vacía e de longitud 0. Además, Σ^* con la concatenación de palabras forma un monoide. Un **lenguaje** es un subconjunto $L \subseteq \Sigma^*$. Informalmente, un autómata finito es un tipo de computadora que lee palabras en Σ^* y entrega un estado. La definición formal es la siguiente:

Definición 2.2.1. Un *autómata finito* es una 5-upla $M = (Q, \Sigma, \delta, q_0, F)$ que consiste en un conjunto finito Q de *estados*, un *alfabeto de entrada* Σ, una *función de transición* $\delta\colon Q \times \Sigma \to Q$, un *estado inicial* $q_0 \in Q$ y un conjunto de *estados aceptables* $F \subseteq Q$.

El autómata finito comienza en el estado inicial q_0. Para la palabra de entrada $x = a_{i_1} a_{i_2} \dots a_{i_m} \in \Sigma^*$, la máquina se mueve a un nuevo estado de la siguiente forma. Lee primero la letra de la izquierda a_{i_1} y cambia de estado a $q^{(1)} = \delta(q_0, a_{i_1})$. Luego, lee la siguiente letra a_{i_2} y se mueve al estado $q^{(2)} = \delta(q^{(1)}, a_{i_2})$. Luego, lee a_{i_3} y se mueve al estado $q^{(3)} = \delta(q^{(2)}, a_{i_3})$ y así sucesivamente. Cuando lee la última letra a_{i_m} se mueve al estado final $q^{(m)} = \delta(q^{(m-1)}, a_{i_m})$.

Si el autómata finito M está en el estado q y salta al estado q' después de leer la palabra $x \in \Sigma^*$, escribimos $q' = \hat{\delta}(q, x)$. De esta forma, lo anterior se transforma en

$$\begin{aligned} q^{(m)} &= \hat{\delta}(q_0, a_{i_1} a_{i_2} \dots a_{i_m}) \\ &= \hat{\delta}(q_1, a_{i_2} a_{i_3} \dots a_{i_m}) \\ &\ \ \vdots \\ &= \hat{\delta}(q^{(m-1)}, a_{i_m}). \end{aligned}$$

Notemos que $\hat{\delta}(q, a) = \delta(q, a)$ para todo $q \in Q, a \in \Sigma$.

Una palabra $x \in \Sigma^*$ es **aceptada** por un autómata finito M si con la entrada x comenzando en el estado inicial q_0, el autómata alcanza un estado de F. En otras palabras, el autómata acepta la palabra x si y sólo si $\hat{\delta}(q_0, x) \in F$. Un lenguaje L es **aceptado por** M si la máquina alcanza un estado aceptable a partir de todas las entradas $x \in L$.

Los autómatas finitos se pueden utilizar para realizar varias tareas. Por ejemplo, se pueden usar para decidir cuándo una palabra en Σ^* tiene, o no, cierta propiedad. Un autómata de "paridad" (o *parity-check machine*) decide cuándo una palabra en $\{0, 1\}^*$ tiene una cantidad par de unos.

Ejemplo 2.2.2 (Autómata de paridad)**.** La máquina decide cuándo una palabra dada en $\{0, 1\}^*$ tiene una cantidad par de 1's. Tomamos $\Sigma = \{0, 1\}$ y definimos el autómata $M = (Q, \Sigma, \delta, q_0, F)$ de la siguiente manera. El conjunto de estados $Q = \{q_0, q_1\}$, el estado inicial es q_0 y el conjunto de estados aceptables es $F = \{q_0\}$. La función de transición $\delta \colon Q \times \Sigma \to Q$ está dada por la siguiente tabla.

	0	1
q_0	q_0	q_1
q_1	q_1	q_0

Veamos qué hace el autómata con la entrada 1001. Leyendo de izquierda a derecha, el autómata lee el 1 y se mueve desde el estado inicial q_0 al estado $q_1 = \delta(q_0, 1)$. Luego, lee 0 y permanece en el estado $q_1 = \delta(q_1, 0)$ y vuelve a leer 0 permaneciendo en el estado $q_1 = \delta(q_1, 0)$. Finalmente, lee 1 y salta al estado final $q_0 = \delta(q_1, 1)$. Como $q_0 \in F$, q_0 es un estado aceptable. La máquina alcanzó un estado aceptable precisamente porque 1001 tiene una cantidad par de 1's. Por otro lado, para la entrada 111 empezando en el estado q_0, la máquina lee 1 y se mueve al estado $q_1 = \delta(q_0, 1)$, lee 1 y se mueve a $q_0 = \delta(q_1, 1)$. Luego, lee por última vez 1 y se mueve al estado final $q_1 = \delta(q_0, 1)$ que es un estado no aceptable. Esto ocurre porque 111 tiene una cantidad impar de 1's.

En general, para una entrada $x \in \Sigma^*$, el autómata de paridad va a alcanzar el estado q_0 si y sólo si x tiene una cantidad par de 1's. El lenguaje aceptado por el autómata es precisamente el conjunto de palabras en $\{0, 1\}^*$ con una cantidad par de 1's. Precisamente, aceptando sólo esas palabras, el autómata finito "decide" qué palabras tienen una cantidad par de 1's.

Podemos representar un autómata finito usando un **diagrama de transición de estados** que es un tipo de grafo dirigido cuyos vértices son los estados y las aristas, orientadas y etiquetadas con letras del alfabeto, representan a la función de transición. Es decir, la transición $\delta(q_i, a) = q_j$ para los estados q_i, q_j y la letra $a \in \Sigma$ se indica etiquetando con a la arista dirigida desde el vértice q_i al q_j. Los estados aceptables se indican con un doble trazo en la circunferencia que rodea al vértice.

La figura 2.1 representa el diagrama de transición de estados del autómata de paridad. Calculemos, por ejemplo, el estado final a partir de la entrada $x = 10011$ observando el diagrama. Comenzando en la flecha de la izquierda que apunta al estado inicial, la máquina lee el dígito 1 y se mueve por la arista correspondiente al estado q_1. Luego, lee los dos ceros y permanece en el mismo estado. Después, lee un 1 y se mueve al estado q_0. Por último, lee el 1 y se mueve al estado q_1.

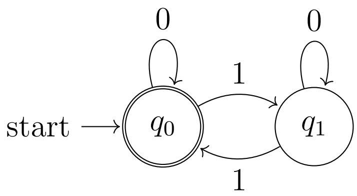

Figura 2.1: Diagrama de transición de estados para el Autómata de Paridad. El único estado aceptable es el q_0.

Para nuestro próximo ejemplo, construimos un autómata finito que decide si una palabra en $\{0,1\}^*$ termina en 11. El lenguaje aceptado por el autómata será el conjunto de palabras en $\{0,1\}^*$ que terminan en 11.

Ejemplo 2.2.3 (Test de palabra terminada en 11)**.** Sea $(M, \Sigma, \delta, q_0, F)$ con estados $Q = \{q_0, q_1, q_2\}$, estado inicial q_0 y estados aceptables $F = \{q_2\}$. Definimos la función de transición $\delta\colon Q \times \Sigma \to Q$ por la tabla

	0	1
q_0	q_0	q_1
q_1	q_0	q_2
q_2	q_0	q_2

El diagrama de transición de estados está dado por la Figura 2.2.

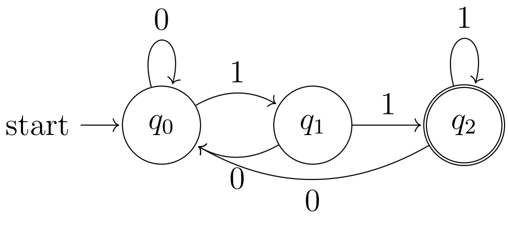

Figura 2.2: Diagrama de transición de estados para Test de palabra terminada en 11. El único estado aceptable es el q_2

Por ejemplo, $x = 01011$ termina en 11 y la máquina alcanza el estado q_2 (un estado aceptable) como se pide. Por otro lado, para la entrada 101 la máquina alcanza el estado q_1 y entonces no es una palabra aceptada por M.

Ejemplo 2.2.4. Consideremos $\Sigma = \{a, b\}$. Sea $(M, \Sigma, \delta, q_0, F)$ con conjunto de estados $Q = \{q_0, q_1\}$, estado inicial q_0 y estados aceptables $F = \{q_1\}$. La función de transición está dada por

	a	b
q_0	q_1	q_0
q_1	q_1	q_1

El diagrama de transición de estados corresponde al de la Figura 2.3.

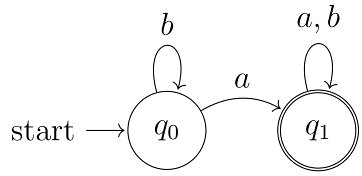

Figura 2.3: Diagrama de transición de estados para el Autómata del Ejemplo 2.2.4.

Notemos que este autómata reconoce las palabras que contienen al menos una letra a como veremos en el Ejemplo 2.2.7.

Es evidente que un autómata finito $M = (Q, \Sigma, \delta, q_0, F)$ acepta el lenguaje L formado por las palabras $x \in \Sigma^*$ tales que $\hat{\delta}(q_0, x)$ pertenece a F.

Ahora nos preguntamos: dado un alfabeto Σ y un lenguaje $L \subseteq \Sigma^*$, ¿existe un autómata finito que acepte al lenguaje L? Las respuesta viene dada por el Teorema de Myhill–Nerode.

Sea Σ un alfabeto finito y sea $L \subseteq \Sigma^*$ un lenguaje. En el conjunto Σ^* definimos una relación de equivalencia $\sim_L$ como sigue: para $x, y \in \Sigma^*$,

$$x \sim_L y \text{ si y sólo si } xz \in L \text{ exactamente cuando } yz \in L \text{ para todo } z \in \Sigma^*.$$

La relación de equivalencia $\sim_L$ tiene **índice finito** si hay una cantidad finita de clases de equivalencia bajo la relación.

Proposición 2.2.5 (Teorema de Myhill–Nerode)**.** *Sea Σ un alfabeto finito y sea $L \subseteq \Sigma^*$ un lenguaje. Son equivalentes:*

(i) La relación de equivalencia $\sim_L$ tiene índice finito;

(ii) Existe un autómata finito que acepta el lenguaje L.

Demostración. (i) $\Rightarrow$ (ii): Supongamos que $\sim_L$ tiene índice finito. Debemos construir un autómata finito que acepte el lenguaje L. Para cada $x \in \Sigma^*$, sea

$$[x] = \{y \in \Sigma^* \colon y \sim_L x\}$$

la clase de equivalencia de $\sim_L$ que contiene a x. Entonces, por la hipótesis, el conjunto $Q = \{[x] \colon x \in \Sigma^*\}$ es finito y será el conjunto de estados del autómata. Sea $\delta \colon Q \times \Sigma \to Q$ la relación dada por $\delta([x], a) = [xa]$ para $a \in \Sigma$. Veamos que es una función bien definida. Para eso, supongamos que $[x] = [y]$, entonces $x \sim_L y$ y luego,

$x(az) \in L$ exactamente cuando $y(az) \in L$ para todo $z \in \Sigma^*$. Por lo tanto, $[xa] = [ya]$. Ahora,

$$\delta([x], a) = [xa] = [ya] = \delta([y], a).$$

Esto prueba que δ está bien definida sobre las clases de Q. Tomemos $q_0 = [e]$ y $F = \{[x] \in Q \colon x \in L\}$. Tenemos entonces el autómata finito $M = (Q, \Sigma, \delta, q_0, F)$ que acepta al lenguaje L. En efecto, $\hat{\delta}([e], x) = [x]$ para todo $x \in \Sigma^*$. En particular, si $x \in L$ entonces $\hat{\delta}([e], x) \in F$.

$\underline{(ii) \Rightarrow (i)}$: Supongamos que el lenguaje L es aceptado por el autómata finito $M = (Q, \Sigma, \delta, q_0, F)$. Definimos $\sim_M$ la relación de equivalencia dada por $x \sim_M y$ si y sólo si $\hat{\delta}(q_0, x) = \hat{\delta}(q_0, y)$. Entonces, $\sim_M$ tiene índice finito puesto que hay un conjunto finito de estados en Q. Notemos que

$$L = \{x \in \Sigma^* \colon \hat{\delta}(q_0, x) \in F\},$$

y entonces L es una unión de algunas de las clases de equivalencia bajo la relación $\sim_M$. Supongamos ahora que $x \sim_M y$. Entonces, $\hat{\delta}(q_0, x) = \hat{\delta}(q_0, y)$ y luego, $\hat{\delta}(q_0, xz) = \hat{\delta}(q_0, yz)$ para todo $z \in \Sigma^*$. En consecuencia, $xz \in L$ si y sólo si $yz \in L$ para todo $z \in \Sigma^*$, es decir, $x \sim_L y$. Esto dice que el índice de $\sim_L$ es menor o igual que el índice de $\sim_M$ pues cada clase de $\sim_L$ es una unión de clases de $\sim_M$. $\square$

Vamos a ver varios ejemplos para calcular la cantidad de clases de equivalencia bajo $\sim_L$ para ver si determinados lenguajes L son o no aceptados por autómatas finitos.

Ejemplo 2.2.6. Sea L el vocabulario del idioma español que consiste en palabras formadas a partir del alfabeto $\Sigma = \{a, b, c, \ldots, z\}$. Asumimos que L es un conjunto finito; luego, existe una palabra $x \in L$ de longitud máxima d. Ahora, cualesquiera dos palabras $x, y \in \Sigma^*$ de longitud $> d$ son equivalentes pues, para toda palabra $z \in \Sigma^*$, tanto xz como yz no pertenecen a L. Luego, $\sim_L$ admite a lo sumo $|L| + 2$ clases de equivalencia (contando una clase por cada palabra incluyendo la palabra vacía y otra por todas las palabras fuera de L). Por el Teorema de Myhill–Nerode, el idioma español es aceptado por un autómata finito.

Ejemplo 2.2.7. Sea $L \subseteq \{a, b\}^*$ definido como

$$L = \{xay \colon x, y \in \{a, b\}^*\}.$$

Ahora, $y \sim_L e$ si y sólo si $yz \in L$ exactamente cuando $z \in L, \forall z \in \{a, b\}^*$. Luego, $[e] = \{y \colon y \notin L\}$. Esto lo podemos ver separando casos en z. Si $z \in L$, entonces yz también, pues seguro que contiene una letra a pues z ya la tiene. Si $z \notin L$, entonces yz sólo va a estar en L si $y \in L$.

Por otro lado, $y \sim_L a$ si y sólo si $yz \in L$ exactamente cuando $az \in L, \forall z$. Como az siempre está en L, necesito que yz también. Pero esto sólo sucede si $y \in L$. Luego, $[a] = \{y \colon y \in L\}$. Obviamente, $[e] \neq [a]$. Entonces, el conjunto de clases bajo $\sim_L$ es $\{[e], [a]\}$ con $L = [a]$. Por el Teorema de Myhill–Nerode, el lenguaje L es aceptado por el autómata finito de la Figura 2.4.

Notemos que se trata del mismo diagrama de la Figura 2.3 reetiquetando los nodos.

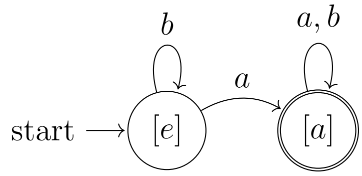

Figura 2.4: Diagrama del Ejemplo 2.2.7

Ejemplo 2.2.8. Sea $\Sigma = \{a, b\}$ y sea L el lenguaje formado por las palabras en $\{a, b\}^*$ que no tengan dos letras b consecutivas. Se tiene que $y \sim_L e$ si y sólo si $yz \in L$ exactamente cuando $z \in L$. En consecuencia, la clase $[e]$ está formada por todas las palabras $y \in L$ que terminan en a o bien $y = e$. Por otro lado, $y \sim_L b$ si y sólo si $yz \in L$ exactamente cuando $bz \in L$. Luego, $[b]$ está formada por todas las palabras que terminan en b pero no en bb. Finalmente, $y \sim_L bb$ si y sólo si $yz \in L$ exactamente cuando $bbz \in L$. Entonces, $[bb]$ es el conjunto de palabras $y \notin L$. El Teorema de Myhill–Nerode nos permite construir el autómata de la Figura 2.5 que acepta al lenguaje L.

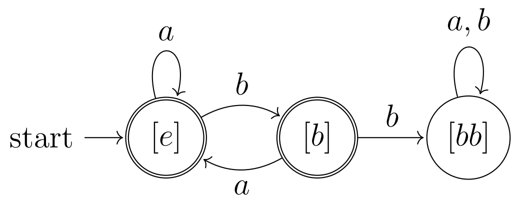

Figura 2.5: Diagrama del Ejemplo 2.2.8

Ejemplo 2.2.9. Tomemos $\Sigma = \{a, b\}$ y $L = \{a^n b^n : n \geq 0\}$, es decir,

$$L = \{e, ab, aabb, aaabbb, aaaabbbb, \dots\}.$$

El conjunto de clases bajo $\sim_L$ es

$$\{L \setminus \{e\}, [b], [e], [a], [aa], [aaa], [aaaa], \dots\}$$

con $L = L \setminus \{e\} \cup [e]$. Es fácil ver que las clases son distintas. Estudiando casos, se puede probar que son todas. Luego $\sim_L$ tiene índice infinito, y entonces no existe autómata finito que acepte el lenguaje L.

Fijemos un poco de notación para el resto de la sección. Sea K un cuerpo y S un monoide. Notamos por H a KS la biálgebra del monoide como en el Ejemplo 2.1.2 con dual lineal $H^* = KS^*$. Recordemos la estructura de H-módulo a derecha en H^* definida como

$$(p \leftharpoonup x)(y) = p(xy)$$

para todo $x, y \in H, p \in H^*$. El elemento $p \leftharpoonup x$ es el traslado a derecha de p por x. Además, $p \leftharpoonup H = \{p \leftharpoonup x \colon x \in H\}$ es un subespacio de H^*. Vamos a considerar el monoide $S = \Sigma^*$ de las palabras sobre el alfabeto finito Σ y $L \subseteq S$ un lenguaje. Sea $\rho \colon S \to K$ la **función característica** de L definida como

$$\rho(x) = \begin{cases} 1 & \text{si} \quad x \in L \\ 0 & \text{si} \quad x \notin L \end{cases}$$

Entonces, ρ se extiende por linealidad a un elemento $p \in H^*$. En efecto,

$$p\left(\sum_{x \in S} a_x x\right) = \sum_{x \in S} a_x \rho(x).$$

La siguiente proposición es fundamental en lo sucesivo.

Proposición 2.2.10. *Sea $L \subseteq S$ un lenguaje y sea p el elemento de $H^* = KS^*$ definido arriba. Entonces $\sim_L$ tiene índice finito si y sólo si el conjunto de traslados a derecha $\{p \leftharpoonup x \colon x \in S\}$ es finito.*

Demostración. Sea $[x]$ la clase de equivalencia de x por la relación $\sim_L$. Definimos una relación de equivalencia $\sim_p$ sobre S como sigue: $x \sim_p y$ si y sólo si $p(xz) = p(yz)$ para todo $z \in S$. Entonces, $\sim_L = \sim_p$ por la definición de p. Notemos por $[x]_p$ la clase de equivalencia de x bajo $\sim_p$. Luego, $\{[x] \colon x \in S\} = \{[x]_p \colon x \in S\}$. Definimos la relación

$$\phi \colon \{[x]_p \colon x \in S\} \to \{p \leftharpoonup x \colon x \in S\}$$

por la regla $\phi([x]_p) = p \leftharpoonup x$. Supongamos que $[x]_p = [y]_p$, entonces

$$\phi([x]_p) = p \leftharpoonup x = p \leftharpoonup y = \phi([y]_p).$$

Luego, ϕ está bien definida sobre las clases de equivalencia bajo $\sim_p$. La aplicación es claramente sobreyectiva. Veamos que es inyectiva. Para ello, supongamos que $\phi([x]_p) = \phi([y]_p)$. Entonces, $p \leftharpoonup x = p \leftharpoonup y$, de donde $[x]_p = [y]_p$. Tenemos entonces una biyección entre las clases de equivalencia bajo $\sim_L$ y $\{p \leftharpoonup x \colon x \in S\}$ de lo cual se sigue el resultado buscado. □

La Proposición 2.2.10 es el punto de partida para generalizar el teorema de Myhill–Nerode a un monoide S arbitrario. La condición "$\sim_L$ tiene índice finito" se reemplaza por la condición de finitud sobre el conjunto $\{p \leftharpoonup x \colon x \in S\}$. Una cierta biálgebra jugará el papel del autómata finito que acepta el lenguaje.

Proposición 2.2.11. *Sea S un monoide y sea $H = KS$ la biálgebra del monoide. Sea $p \in H^*$. Son equivalentes:*

(i) El conjunto $\{p \leftharpoonup x \colon x \in S\}$ de traslados a derecha es finito;

(ii) Existe una biálgebra B de dimensión finita, un morfismo de biálgebras $\Psi \colon H \to B$ y un elemento $f \in B^*$ tal que $p(h) = f(\Psi(h))$ para todo $h \in H$.

Demostración. (i) $\Rightarrow$ (ii): Sea $Q = \{p \leftharpoonup x \colon x \in S\}$ el conjunto finito de traslados a derecha. Para cada $u \in S$, definimos el operador a derecha $r_u \colon Q \to Q$ como

$$(p \leftharpoonup x)r_u = (p \leftharpoonup x) \leftharpoonup u = p \leftharpoonup xu.$$

El conjunto $\{r_u \colon u \in S\}$ es finito por la cota

$$|\{r_u \colon u \in S\}| \leq |Q|^{|Q|}.$$

Dotamos al conjunto $\{r_u \colon u \in S\}$ de la operación binaria dada por la "composición de operadores" definida como: para $r_u, r_v \in \{r_u \colon u \in S\}, p \leftharpoonup x \in Q$,

$$(p \leftharpoonup x)(r_u r_v) = (p \leftharpoonup xu)r_v = p \leftharpoonup xuv = (p \leftharpoonup x)r_{uv}.$$

Luego, $r_u r_v = r_{uv}$ para todo $u, v \in S$. Entonces, el conjunto $\{r_u \colon u \in S\}$ con la composición de operadores es un monoide con unidad r_1. Notemos por B la biálgebra del monoide $\{r_u \colon u \in S\}$ sobre K. Sea $\Psi \colon H \to B$ la transformación K-lineal definida por $\Psi(u) = r_u$. Entonces,

$$\Psi(uv) = r_{uv} = r_u r_v = \Psi(u)\Psi(v).$$

Además,

$$\Delta_B(\Psi(u)) = \Delta_B(r_u) = r_u \otimes r_u = \Psi(u) \otimes \Psi(u) = (\Psi \otimes \Psi)(u \otimes u) = (\Psi \otimes \Psi)\Delta_H(u),$$

y

$$\epsilon_B(\Psi(u)) = \epsilon_B(r_u) = \epsilon_H(u).$$

Entonces, Ψ es morfismo de biálgebras. Sea $f \in B^*$ definido como

$$f(r_u) = ((p \leftharpoonup 1)r_u)(1) = (p \leftharpoonup u)(1) = p(u).$$

Entonces $p(h) = f(\Psi(h))$ para todo $h \in H$ como se pide.

(ii) $\Rightarrow$ (i): Supongamos que existe una biálgebra de dimensión finita B, un morfismo de biálgebras $\Psi \colon H \to B$ y un elemento $f \in B^*$ tal que $p(h) = f(\Psi(h))$ para todo $h \in H$. Definimos una acción $\cdot$ de H en B, que resulta en una estructura de H-módulo a derecha, como

$$b \cdot h = b\Psi(h)$$

para todo $b \in B, h \in H$. Entonces, para $b \in B, x \in S$,

$$\begin{aligned}
\Delta_B(b \cdot x) = \Delta_B(b\Psi(x)) = \Delta_B(b)\Delta_B(\Psi(x)) &= \left(\sum_{(b)} b_{(1)} \otimes b_{(2)}\right)(\Psi \otimes \Psi)\Delta_H(x) \\
&= \left(\sum_{(b)} b_{(1)} \otimes b_{(2)}\right)(\Psi(x) \otimes \Psi(x)) = \sum_{(b)} b_{(1)}\Psi(x) \otimes b_{(2)}\Psi(x) \\
&= \sum_{(b)} b_{(1)} \cdot x \otimes b_{(2)} \cdot x
\end{aligned}$$

y

$$\epsilon_B(b \cdot x) = \epsilon_B(b\Psi(x)) = \epsilon_B(b)\epsilon_B(\Psi(x)) = \epsilon_B(b)\epsilon_H(x).$$

Luego, B es H-módulo coálgebra a derecha. Ahora, sea Q el conjunto de los elementos de tipo grupo de B. Por la Proposición 1.2.24, Q es un subconjunto linealmente independiente de B. Como B es de dimensión finita, Q es finito. Como B es H-módulo coálgebra a derecha con acción $\cdot$, tenemos

$$\Delta_B(q \cdot x) = q \cdot x \otimes q \cdot x$$

para $q \in Q, x \in S$. Luego, $\cdot$ se restringe a una acción de S en Q. Ahora, para $x, y \in S$,

$$\begin{aligned}(p \leftharpoonup x)(y) &= p(xy) = f(\Psi(xy)) = f(\Psi(x)\Psi(y)) \\ &= f((1_B\Psi(x))\Psi(y)) = f((1_B \cdot x) \cdot y).\end{aligned} \tag{2.4}$$

Sea

$$T = \{q \in Q \colon q = 1_B \cdot x, \text{ para cierto } x \in S\}$$

Por (2.4), existe una función sobreyectiva

$$\varrho \colon T \to \{p \leftharpoonup x \colon x \in S\}$$

definida como

$$\varrho(1_B \cdot x)(y) = f((1_B \cdot x) \cdot y) = (p \leftharpoonup x)(y).$$

Como T es finito, $\{p \leftharpoonup x \colon x \in S\}$ es finito. □

Las biálgebras construidas en la Proposición 2.2.11(ii) se llaman **biálgebras de Myhill–Nerode**. La forma más sencilla de construir una biálgebra de Myhill–Nerode es comenzar con un lenguaje $L \subseteq S$ para el cual $\sim_L$ es de índice finito. Luego, por la Proposición 2.2.10, el conjunto de traslados a derecha $\{p \leftharpoonup x \colon x \in S\}$ es finito, y entonces, por la implicación $(i) \Rightarrow (ii)$ de la Proposición 2.2.11, existe una biálgebra de Myhill–Nerode B, un morfismo de biálgebras $\Psi \colon KS \to B$ y un elemento $f \in B^*$ tal que $p(h) = f(\Psi(h))$, para todo $h \in KS$. Veamos algunos ejemplos.

Ejemplo 2.2.12. Sea $L \subseteq S = \Sigma^* = \{a, b\}^*$ el lenguaje del Ejemplo 2.2.7. En este caso, las clases de quivalencia bajo $\sim_L$ son $[e]$ y $[a]$, con $L = [a]$. La función característica $\rho \colon S \to K$ se extiende a una función $p \in KS^*$ definida como $p(\sum_{x \in S} a_x x) = \sum_{x \in S} a_x \rho(x)$. Hay exactamente dos traslados a derecha de p:

$$\{p \leftharpoonup 1, p \leftharpoonup a\}.$$

El conjunto de operadores a derecha es $\{r_1, r_a\}$ y quedan definidos por la tabla

$p \leftharpoonup x$	$(p \leftharpoonup x)r_1$	$(p \leftharpoonup x)r_a$
$p \leftharpoonup 1$	$p \leftharpoonup 1$	$p \leftharpoonup a$
$p \leftharpoonup a$	$p \leftharpoonup a$	$p \leftharpoonup a$

El monoide $T = \{r_1, r_a\}$ tiene la operación dada por

	r_1	r_a
r_1	r_1	r_a
r_a	r_a	r_a

La biálgebra del monoide KT es la biálgebra de Myhill–Nerode. Más aún, el morfismo de biálgebras $\Psi\colon KS \to KT$ está dado por $\Psi(x) = r_x$. Sea $\{e_{r_1}, e_{r_a}\}$ la base de KT^* dual a la base $\{r_1, r_a\}$ de KT. Considero $h = \sum_{x\in S} a_x x$. Entonces, el elemento $e_{r_a} \in KT^*$ es tal que

$$\begin{aligned} p(h) = p\left(\sum_{x\in S} a_x x\right) &= \sum_{x\in S} a_x \rho(x) = \sum_{x\in S} a_x \delta_{[a],[x]} = \sum_{x\in S} a_x e_{r_a}(r_x) \\ &= e_{r_a}\left(\sum_{x\in S} a_x r_x\right) = e_{r_a}\left(\Psi\left(\sum_{x\in S} a_x x\right)\right) = e_{r_a}(\Psi(h)). \end{aligned}$$

Es decir, e_{r_a} es el elemento f de la Proposición 2.2.11. Además, en este caso KT^* es una K-biálgebra con $KT^* \cong K \times K$ como K-álgebras mediante la asignación $e_1 \mapsto (1,0), e_a \mapsto (0,1)$ y con estructura de coálgebra definida como

$$\begin{aligned} \Delta_{KT^*}(e_{r_1}) &= e_{r_1} \otimes e_{r_1}, \\ \Delta_{KT^*}(e_{r_a}) &= e_{r_1} \otimes e_{r_a} + e_{r_a} \otimes e_{r_1} + e_{r_a} \otimes e_{r_a}, \\ \epsilon_{KT^*}(e_{r_1}) &= e_{r_1}(r_1) = 1, \\ \epsilon_{KT^*}(e_{r_a}) &= e_{r_a}(r_1) = 0. \end{aligned}$$

Ejemplo 2.2.13. Consideremos ahora el lenguaje L del Ejemplo 2.2.8. Las clases de equivalencia bajo $\sim_L$ son $[e], [b], [bb]$ con $L = [e] \cup [b]$. Si $p \in KS^*$ denota a la extensión de la función característica de L como antes, el conjunto de traslados a derecha es $Q = \{p \leftharpoonup 1, p \leftharpoonup b, p \leftharpoonup bb\}$. El conjunto de operadores a derecha es $\{r_1, r_b, r_{bb}, r_a, r_{ab}, r_{ba}\}$. Los operadores están definidos por la siguiente tabla

$p \leftharpoonup x$	$(p \leftharpoonup x)r_1$	$(p \leftharpoonup x)r_b$	$(p \leftharpoonup x)r_{bb}$	$(p \leftharpoonup x)r_a$	$(p \leftharpoonup x)r_{ab}$	$(p \leftharpoonup x)r_{ba}$
$p \leftharpoonup 1$	$p \leftharpoonup 1$	$p \leftharpoonup b$	$p \leftharpoonup bb$	$p \leftharpoonup 1$	$p \leftharpoonup b$	$p \leftharpoonup 1$
$p \leftharpoonup b$	$p \leftharpoonup b$	$p \leftharpoonup bb$	$p \leftharpoonup bb$	$p \leftharpoonup 1$	$p \leftharpoonup b$	$p \leftharpoonup bb$
$p \leftharpoonup bb$	$p \leftharpoonup bb$	$p \leftharpoonup bb$	$p \leftharpoonup bb$	$p \leftharpoonup bb$	$p \leftharpoonup bb$	$p \leftharpoonup bb$

El monoide $T = \{r_1, r_b, r_{bb}, r_a, r_{ab}, r_{ba}\}$ tiene la operación definida por

	r_1	r_b	r_{bb}	r_a	r_{ab}	r_{ba}
r_1	r_1	r_b	r_{bb}	r_a	r_{ab}	r_{ba}
r_b	r_b	r_{bb}	r_{bb}	r_{ba}	r_b	r_{bb}
r_{bb}	r_{bb}	r_{bb}	r_{bb}	r_{bb}	r_{bb}	r_{bb}
r_a	r_a	r_{ab}	r_{bb}	r_a	r_{ab}	r_a
r_{ab}	r_{ab}	r_{bb}	r_{bb}	r_a	r_{ab}	r_{bb}
r_{ba}	r_{ba}	r_b	r_{bb}	r_{ba}	r_b	r_{ba}

La biálgebra del monoide KT es la biálgebra de Myhill–Nerode y el morfismo de biálgebras $\Psi\colon KS \to KT$ está dado por $\Psi(x) = r_x$. Sea $\{e_{r_1}, e_{r_b}, e_{r_{bb}}, e_{r_a}, e_{r_{ab}}, e_{r_{ba}}\}$ la base de KT^* dual a la base T de KT. Sea $h = \sum_{x\in S} a_x x$. Entonces el elemento f de la Proposición 2.2.11 es $1 - e_{r_{bb}}$; en efecto

$$\begin{aligned}
p(h) &= p\left(\sum_{x\in S} a_x x\right) = \sum_{x\in S} a_x \rho(x) \\
&= \sum_{x\in S} a_x \sum_{\substack{r_y\in T,\\ r_y\neq r_{bb}}} \delta_{[y],[x]} = \sum_{x\in S} a_x \sum_{\substack{r_y\in T,\\ r_y\neq r_{bb}}} e_{r_y}(r_x) \\
&= \sum_{x\in S} a_x (1 - e_{r_{bb}})(r_x) = (1 - e_{r_{bb}})\left(\sum_{x\in S} a_x r_x\right) \\
&= (1 - e_{r_{bb}})\left(\Psi\left(\sum_{x\in S} a_x x\right)\right) = (1 - e_{r_{bb}})(\Psi(h)).
\end{aligned}$$

Ejemplo 2.2.14. Sea $\Sigma = \{a\}$, para cada entero $i \geq 0$, notemos $L_i = \{a^i\} \subseteq S = \Sigma^*$, con función característica $\rho_i\colon S \to K$. Sea $H = KS$ y sea $p_i \in H^* = KS^*$ la extensión de ρ_i. El conjunto finito de traslados a derecha de $p_i \in H^*$ es

$$Q_i = \{p_i \leftharpoonup 1, p_i \leftharpoonup a, p_i \leftharpoonup a^2, \ldots, p_i \leftharpoonup a^i, p_i \leftharpoonup a^{i+1}.\}$$

El conjunto de operadores a derecha sobre Q_i es el monoide $T_i = \{r_1, r_a, r_{a^2}, \ldots, r_{a^i}, r_{a^{i+1}}\}$. Tenemos, para cada $0 \leq m, n \leq i + 1$,

$$r_{a^m} r_{a^n} = \begin{cases} r_{a^{m+n}} & \text{si} \quad 0 \leq m + n \leq i + 1 \\ r_{a^{i+1}} & \text{si} \quad m + n > i + 1 \end{cases}$$

$B_i = KT_i$ es la biálgebra de Myhill–Nerode con morfismo de biálgebras $\Psi_i\colon H \to B_i$ definido como $x \mapsto r_x$. El elemento $e_{r_{a^i}} \in B_i^*$ es tal que

$$p_i(h) = e_{r_{a^i}}(\Psi_i(h)),$$

para todo $h \in KS$.

A continuación, vamos a ver cómo una biálgebra de Myhill–Nerode determina un autómata finito. Sea B una biálgebra de Myhill–Nerode construida a partir de un lenguaje L con $\sim_L$ de índice finito (como en los Ejemplos 2.2.12, 2.2.13 y 2.2.14).

Proposición 2.2.15. *La biálgebra de Myhill–Nerode B determina un autómata finito $(Q, \Sigma, \delta, q_o, F)$ que acepta el lenguaje L.*

Demostración. Como conjunto de estados del autómata tomamos Q el conjunto finito de elementos de tipo grupo de B; se trata precisamente del conjunto finito de operadores a derecha $Q = \{r_x : x \in S\}$. Como alfabeto de entrada elegimos Σ. Como hemos visto, la estructura de H-módulo a derecha de B se restringe a una acción "$\cdot$" de S en Q. Definimos, entonces, la función de transición $\delta \colon Q \times \Sigma \to Q$ como

$$\delta(r_x, y) = r_x \Psi(y) = r_x r_y = r_{xy},$$

para $r_x \in Q, y \in S$. El estado inicial es $q_0 = 1_B$ y el conjunto de estados aceptables F es el subconjunto de Q de los elementos de la forma $1_B \cdot x, x \in S$ para los cuales

$$p(x) = f(\Psi(x)) = f(1_B \Psi(x)) = f(1_B \cdot x) = 1$$

Por construcción, el autómata finito $(Q, \Sigma, \delta, 1_B, F)$ acepta el lenguaje L. $\square$

Ejemplo 2.2.16. Sea B la biálgebra de Myhill–Nerode construida en el Ejemplo 2.2.12. El autómata finito está dado por $Q = \{r_1, r_a\}$, $F = \{r_a\}$, con función de transición δ dada por la tabla

	a	b
r_1	r_a	r_1
r_a	r_a	r_a

El diagrama correspondiente al autómata está dado por la Figura 2.6. Este autómata acepta el lenguaje L del Ejemplo 2.2.12.

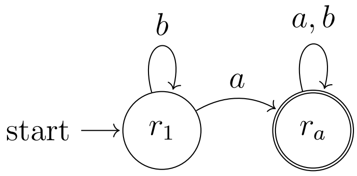

Figura 2.6: Diagrama de transición de estados para el autómata del Ejemplo 2.2.16.

Ejemplo 2.2.17. Sea B la biálgebra de Myhill–Nerode construida en el Ejemplo 2.2.13. El autómata finito está dado por $Q = \{r_1, r_b, r_{bb}, r_a, r_{ab}, r_{ba}\}$, $F = \{r_1, r_b, r_a, r_{ab}, r_{ba}\}$ con función de transición δ dada por la tabla

	a	b
r_1	r_a	r_b
r_b	r_{ba}	r_{bb}
r_{bb}	r_{bb}	r_{bb}
r_a	r_a	r_{ab}
r_{ab}	r_a	r_{bb}
r_{ba}	r_{ba}	r_b

El autómata asociado está dado por la Figura 2.7. Este autómata acepta el lenguaje L del Ejemplo 2.2.13. Notemos que no es el mismo autómata de la Figura correspondiente a dicho ejemplo.

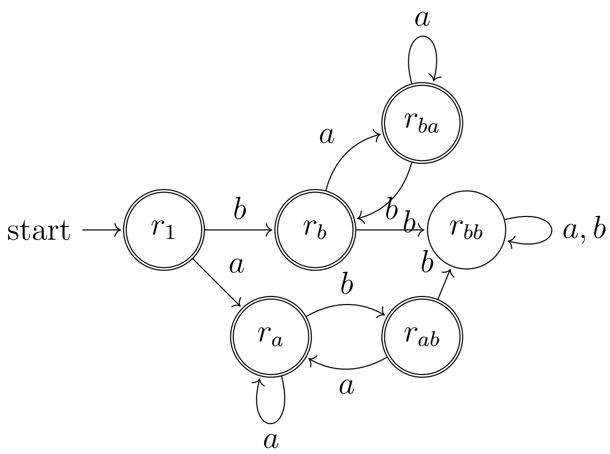

Figura 2.7: Diagrama de transición de estados para el autómata del Ejemplo 2.2.17.

Ejemplo 2.2.18. Para $i \geq 0$, sea B_i la biálgebra de Myhill–Nerode construida en el Ejemplo 2.2.14. El autómata finito está dado por $(Q_i, \Sigma, \delta_i, 1_{B_i}, F_i)$ con $Q_i = \{r_1, r_a, r_{a^2}, \ldots, r_{a^i}, r_{a^{i+1}}\}$, $F = \{r_{a^i}\}$ con función de transición δ_i dada por la tabla

	a
r_1	r_a
r_a	r_{a^2}
r_{a^2}	r_{a^3}
$\vdots$	$\vdots$
r_{a^i}	$r_{a^{i+1}}$
$r_{a^{i+1}}$	$r_{a^{i+1}}$

El diagrama de estados está dado por la Figura 2.8. Este autómata acepta el lenguaje L del Ejemplo 2.2.14.

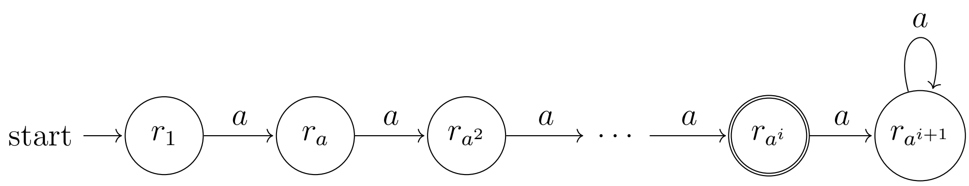

Figura 2.8: Diagrama de transición de estados para el autómata del Ejemplo 2.2.18.

2.3. Sucesiones regulares

En esta última sección presentamos el concepto de sucesión regular que generaliza las sucesiones recursivas lineales sobre cuerpos finitos.

Sea S un monoide numerable como conjunto. Luego, los elementos de S se pueden listar como

$$x_0, x_1, x_2, x_3, \dots$$

Sea K un cuerpo y consideremos $H = KS$ la biálgebra del monoide. Sea $p \in H^*$. Definimos una sucesión $\{s_n\}$ en K por la regla $s_n = p(x_n)$ para $n \geq 0$. Entonces, decimos que $\{s_n\}$ es una **sucesión regular** si el conjunto de traslados a derecha $\{p \leftharpoonup x \colon x \in S\}$ es finito. Recordemos que para $x \in S$, el traslado $p \leftharpoonup x \in H^*$ se define como $(p \leftharpoonup x)(y) = p(xy), \forall y \in S$.

Ejemplo 2.3.1. Sean $S = \{a, b\}^*$ y L el lenguaje que consiste de todas las palabras que no tienen dos letras b consecutivas (ver Ejemplo 2.2.8). Las clases de equivalencia bajo $\sim_L$ son $[e], [b], [bb]$, y $L = [e] \cup [b]$. El conjunto S es numerable y sus elementos se pueden listar como

$$e, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa, aaab, \dots$$

Estamos listando por longitud primero y luego por orden lexicográfico. Aquí, $x_0 = e, x_1 = a, x_2 = b$, etc. Sea $\rho \colon S \to K$ la función característica de L que se extiende a una función $p = \sum_{n=0}^{\infty} \rho(x_n) e_n \in H^*$ con $e_n(x_m) = \delta_{n,m}$. La sucesión $s_n = p(x_n)$ en K es

$$1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, \dots$$

El índice de $\sim_L$ es 3, entonces por la Proposición 2.2.10, el conjunto de traslados a derecha $\{p \leftharpoonup x \colon x \in S\}$ es finito. Luego, $\{s_n\}$ es una sucesión regular.

Veamos un lema, [NU11, Lema 4.1], que será necesario para caracterizar a las sucesiones regulares.

Lema 2.3.2. *Sea W un conjunto, K un cuerpo y $Map(W, K)$ el álgebra de funciones de W en K Si A es un subespacio de $Map(W, K)$ de dimensión finita $n > 0$, existen elementos $w_1, w_2, \dots, w_n \in W$ y una base $\{g_1, g_2, \dots, g_n\}$ de A tal que $g_i(w_j) = \delta_{ij}$ para todo $1 \leq i, j \leq n$.*

Demostración. Procederemos por inducción en n. Para el caso $n = 1$ tomamos $\{f\}$ base de A. Como f es no nulo, existe un elemento $w \in W$ tal que $f(w) \neq 0$. Sea $g = f(w)^{-1}f$. Entonces $\{g\}$ es base de A y cumple que $g(w) = 1$.

Asumamos que $n > 1$ y que existen elementos $w_1, \dots, w_{n-1} \in W$ y funciones $g'_1, \dots, g'_{n-1} \in \mathrm{Map}(W, K)$ que cumplen $g'_i(w_j) = \delta_{ij}$ para $1 \leq i, j \leq n-1$ y $\mathrm{span}\{g'_1, \dots, g'_{n-1}\} = \mathrm{span}\{f_1, \dots, f_{n-1}\}$. Como $f_n \notin \mathrm{span}\{g'_1, \dots, g'_{n-1}\}$, la función $h = f_n - f_n(w_1)g'_1 - \cdots - f_n(w_{n-1})g'_{n-1}$ es no nula. En consecuencia, existe un elemento $w_n \in W$ tal que $h(w_n) \neq 0$. Sea $g_n = h(w_n)^{-1}h$. Entonces, $g_n(w_i) = 0$ para $1 \leq i \leq n-1$ y $g_n(w_n) = 1$. Para cada $1 \leq i \leq n-1$, sea $g_i = g'_i - g'_i(w_n)g_n$. Entonces, $g_i(w_n) = 0$. Más aún, $g_i(w_j) = \delta_{ij}$. Además, $\mathrm{span}\{g_1, \dots, g_n\} = \mathrm{span}\{f_1, \dots, f_n\}$ y entonces la base buscada es $\{g_1, \dots, g_n\}$. □

Proposición 2.3.3. *Asumiendo la notación anterior, $\{s_n\}$ es una sucesión regular si y sólo si dim$(p \leftharpoonup H) < \infty$ y la imagen $p(S) = \{p(x) \colon x \in S\}$ es finita.*

Demostración. Si $\{s_n\}$ es una sucesión regular, entonces el conjunto de traslados $\{p \leftharpoonup x \colon x \in S\}$ es finito. Como $\{p \leftharpoonup x \colon x \in S\}$ genera $p \leftharpoonup H$, entonces $p \leftharpoonup H$ es finitamente generado. En particular, $\dim(p \leftharpoonup H) < \infty$. Más aún, para todo $x \in S$, $(p \leftharpoonup x)(1) = p(x)$ y entonces $\{p(x) \colon x \in S\}$ es finito.
Recíprocamente, supongamos que $\dim(p \leftharpoonup H) = n < \infty$ y $p(S) = \{p(x) \colon x \in S\}$ es finito. Luego, $p \leftharpoonup H$ es un subespacio de dimensión finita del K-espacio vectorial $\mathrm{Map}(S, K)$ y entonces, por el Lema 2.3.2, existen elementos $y_1, y_2, \dots, y_n \in S$ y una base $\{f_1, f_2, \dots f_n\}$ de $p \leftharpoonup H$ tal que $f_i(y_j) = \delta_{i,j}$. Sea $x \in S$. Entonces, existen elementos $r_1, r_2, \dots, r_n \in K$ para los cuales $p \leftharpoonup x = r_1 f_1 + r_2 f_2 + \cdots + r_n f_n$. Evaluando en y_j obtenemos $r_j = p(xy_j) \in p(S)$ para $1 \leq j \leq n$. Como $p(S)$ es finito, sólo hay una cantidad finita de combinaciones lineales de los f_i que representan a los traslados a derecha de p. Luego, la cantidad de traslados es finita y entonces $\{s_n\}$ es regular. □

Como consecuencia de la Proposición 2.3.3 la noción de sucesión regular no depende del orden en que listamos los elementos de S.

Proposición 2.3.4. *Sea $K = GF(p^m)$ el cuerpo finito de p^m elementos. Sea $\{s_n\}$ una sucesión recursiva lineal de orden k en K. Entonces, $\{s_n\}$ es regular.*

Demostración. Sea $\Sigma = \{x\}$ el alfabeto formado por una sola letra. Entonces, $S = \Sigma^* = \{1, x, x^2, \dots\}$ y $K[x]$ con la estructura de biálgebra del Ejemplo 2.1.3 es la biálgebra del monoide $H = KS$. Por la Proposición 1.3.13, la sucesión $\{s_n\}$ se corresponde con un elemento $p = \sum_{n=0}^{\infty} s_n e_n \in H^\circ$ con $e_n(x^m) = \delta_{n,m}$. Claramente, $s_n = p(x^n)$ para todo $n \geq 0$. Ahora, por el Lema 2.1.10 $\dim(p \leftharpoonup H) < \infty$. Además, como $p(S) \subseteq GF(p^m)$, se sigue que es un conjunto finito. Luego, por la Proposición 2.3.3, $\{s_n\}$ es regular. □

Ejemplo 2.3.5. Sea $K = GF(2)$. Consideremos $\{s_n\}$ la sucesión recursiva lineal de orden 3 sobre K con polinomio característico $f(x) = x^3 + x + 1$, relación de recurrencia

$$s_{n+3} = s_{n+1} + s_n, n \geq 0,$$

y vector inicial $s_0 = 101$. La sucesión $\{s_n\}$ es periódica de período 7. De hecho, la sucesión es

$$1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, \ldots$$

que es regular por la Proposición 2.3.4.

Sea $\{s_n\}$ la sucesión regular en $K = GF(2)$ del Ejemplo 2.3.5 con $p = \sum_{n=0}^{\infty} s_n e_n \in K[x]^{\circ}$. El conjunto finito de traslados a derecha es

$$\{p \leftharpoondown 1, p \leftharpoondown x, p \leftharpoondown x^2, p \leftharpoondown x^3, p \leftharpoondown x^4, p \leftharpoondown x^5, p \leftharpoondown x^6\}.$$

En consecuencia, la Proposición 2.2.11 nos permite construir una biálgebra de Myhill–Nerode B, un morfismo de biálgebras $\Psi\colon K[x] \to B$ y un elemento $f \in B^*$ tal que $p(h) = f(\Psi(h))$ para todo $h \in K[x]$. Construimos B de la siguiente manera. El conjunto de operadores a derecha es

$$T = \{r_1, r_x, r_{x^2}, r_{x^3}, r_{x^4}, r_{x^5}, r_{x^6}\}$$

con la operación dada por la tabla de abajo.

	r_1	r_x	r_{x^2}	r_{x^3}	r_{x^4}	r_{x^5}	r_{x^6}
r_1	r_1	r_x	r_{x^2}	r_{x^3}	r_{x^4}	r_{x^5}	r_{x^6}
r_x	r_x	r_{x^2}	r_{x^3}	r_{x^4}	r_{x^5}	r_{x^6}	r_1
r_{x^2}	r_{x^2}	r_{x^3}	r_{x^4}	r_{x^5}	r_{x^6}	r_1	r_x
r_{x^3}	r_{x^3}	r_{x^4}	r_{x^5}	r_{x^6}	r_1	r_x	r_{x^2}
r_{x^4}	r_{x^4}	r_{x^5}	r_{x^6}	r_1	r_x	r_{x^2}	r_{x^3}
r_{x^5}	r_{x^5}	r_{x^6}	r_1	r_x	r_{x^2}	r_{x^3}	r_{x^4}
r_{x^6}	r_{x^6}	r_1	r_x	r_{x^2}	r_{x^3}	r_{x^4}	r_{x^5}

La biálgebra de Myhill–Nerode B es $KT \cong KC_7$. Notemos que KT^* tiene como base

$$\{e_{r_1}, e_{r_x}, e_{r_{x^2}}, e_{r_{x^3}}, e_{r_{x^4}}, e_{r_{x^5}}, e_{r_{x^6}}\}$$

con $e_{r_{x^m}}(r_{x^n}) = \delta_{m,n}$. Existe un morfismo de biálgebras $\Psi\colon K[x] \to KT$ definido como $\Psi(x) = r_x$. Sea

$$f = e_{r_1} + e_{r_{x^2}} + e_{r_{x^3}} + e_{r_{x^4}}.$$

Entonces, $p(h) = f(\Psi(h)), \forall h \in K[x]$. Adicionalmente, la sucesión $\{s_n\}$ determina el lenguaje $L \subseteq \{x\}^*$ definido de la siguiente manera: para $n \geq 0$, $x^n \in L$ si y sólo si $s_n = 1$. El lenguaje L es aceptado por el autómata finito de la Figura 2.9.

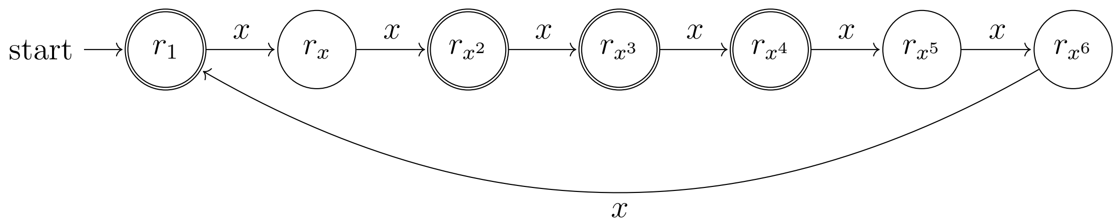

Figura 2.9: Diagrama del autómata finito que acepta el lenguaje L.

Capítulo 3

Álgebras de Hopf

En este capítulo vamos a introducir la noción de álgebra de Hopf sobre un cuerpo K como una biálgebra con un morfismo adicional conocido como antípoda que satisface una cierta propiedad. Damos algunos ejemplos básicos incluyendo el anillo del grupo KG. En este ejemplo, la antípoda tiene orden 2 y nos preguntamos entonces bajo qué condiciones es cierto este hecho. Damos una respuesta completa a esta pregunta y como corolario, probamos que las álgebras de Hopf conmutativas o coconmutativas tienen antípodas necesariamente de orden 2.

3.1. Definiciones y ejemplos básicos

Definición 3.1.1. Una *K-álgebra de Hopf* es una K-biálgebra $(H, m_H, \lambda_H, \Delta_H, \epsilon_H)$ junto con una transformación K-lineal $\sigma_H \colon H \to H$ que satisface

$$m_H(I_H \otimes \sigma_H)\Delta_H(h) = \epsilon_H(h)1_H = m_H(\sigma_H \otimes I_H)\Delta_H(h) \tag{3.1}$$

para todo $h \in H$. La función σ se conoce como *antípoda*. La Condición (3.1) es la *propiedad de la antípoda*.

Observación. En notación de Sweedler, la condición se traduce en

$$\sum_{(h)} h_{(1)}\sigma_H(h_{(2)}) = \epsilon_H(h)1_H = \sum_{(h)} \sigma_H(h_{(1)})h_{(2)} \tag{3.2}$$

para todo $h \in H$.

Definición 3.1.2. Sean H y H' dos K-álgebras de Hopf. Un *morfismo de álgebras de Hopf* es un morfismo de biálgebras $\phi \colon H \to H'$ que satisface la propiedad

$$\phi(\sigma_H(a)) = \sigma_{H'}(\phi(a))$$

para todo $a \in H$. Un morfismo de álgebras de Hopf es *isomorfismo* si ϕ es una biyección.

El cuerpo K es una K-álgebra de Hopf tomando $\sigma_K = I_K$. Se llama **K-álgebra de Hopf trivial**. Veamos algunos ejemplos más.

Ejemplo 3.1.3. Sea G un grupo finito y KG la biálgebra del monoide como en el Ejemplo 2.1.2. Definimos la antípoda como $\sigma_{KG} \colon KG \to KG$

$$\sigma_{KG}(\tau) = \tau^{-1}$$

para $\tau \in G$. Entonces KG es una K-álgebra de Hopf.

Ejemplo 3.1.4. Sea $K[x]$ la biálgebra de polinomios con x primitivo (ver Ejemplo 2.1.4). Definimos la antípoda $\sigma_{K[x]} \colon K[x] \to K[x]$ como

$$\sigma_{K[x]}(x^i) = (-x)^i$$

para $i \geq 0$. Entonces $K[x]$ es K-álgebra de Hopf. Veámoslo: sea $i > 0$,

$$\begin{aligned}
m_{K[x]}(I_{K[x]} \otimes \sigma_{K[x]})\Delta_{K[x]}(x^i) &= m_{K[x]}(I_{K[x]} \otimes \sigma_{K[x]}) \left(\sum_{k=0}^{i} \binom{i}{k} x^k \otimes x^{i-k} \right) \\
&= m_{K[x]} \left(\sum_{k=0}^{i} \binom{i}{k} x^k \otimes \sigma_{K[x]}(x^{i-k}) \right) = m_{K[x]} \left(\sum_{k=0}^{i} \binom{i}{k} x^k \otimes (-x)^{i-k} \right) \\
&= \sum_{k=0}^{i} \binom{i}{k} (-1)^{i-k} x^i = \left(\sum_{k=0}^{i} \binom{i}{k} (-1)^{i-k} \right) x^i = 0 = \epsilon_{K[x]}(x^i) 1_{K[x]}.
\end{aligned}$$

Si $i = 0$, tenemos

$$m_{K[x]}(I_{K[x]} \otimes \sigma_{K[x]})\Delta_{K[x]}(1) = m_{K[x]}(I_{K[x]} \otimes \sigma_{K[x]})(1 \otimes 1) = \sigma_{K[x]}(1) = 1 = \epsilon_{K[x]}(1)$$

Análogamente,

$$m_{K[x]}(\sigma_{K[x]} \otimes I_{K[x]})\Delta_{K[x]}(x^i) = \epsilon_{K[x]}(x^i).$$

Ejemplo 3.1.5. Si consideramos la biálgebra de polinomios con x de tipo grupo (ver Ejemplo 2.1.3), no podemos dotarla de una estructura de K-álgebra de Hopf. En efecto, la condición (3.1) nos dice que

$$\begin{aligned}
m_{K[x]}(I_{K[x]} \otimes \sigma_{K[x]})\Delta_{K[x]}(x) &= m_{K[x]}(I_{K[x]} \otimes \sigma_{K[x]})(x \otimes x) \\
&= m_{K[x]}(x \otimes \sigma_{K[x]}(x)) = x\sigma_{K[x]}(x) = \epsilon_{K[x]}(x) = 1.
\end{aligned}$$

En particular, necesitamos que $x\sigma_{K[x]}(x) = 1$. De la misma forma, desarrollando la otra mitad de la condición tenemos $\sigma_{K[x]}(x)x = 1$. Esto implica que $\sigma_{K[x]}$ debería ser el inverso de x en $K[x]$, algo que no es posible.

Sin embargo, podemos modificar esta biálgebra para poder definir una estructura de álgebra de Hopf.

Ejemplo 3.1.6. Sea $K[x, y]/(xy - 1)$ el cociente de K-álgebras. Entonces

$$K[x, y]/(xy - 1) \cong K[x, x^{-1}].$$

Definimos la comultiplicación $\Delta_{K[x,x^{-1}]}$ tomando tanto x como x^{-1} como elementos de tipo grupo. Definimos la counidad $\epsilon_{K[x,x^{-1}]}$ como $x \mapsto 1, x^{-1} \mapsto 1$. Consideramos como antípoda la aplicación dada por

$$x \mapsto x^{-1}, \quad x^{-1} \mapsto x \tag{3.3}$$

Entonces, $K[x,x^{-1}]$ es K-álgebra de Hopf.

El siguiente ejemplo está tomado de [Swe69, pp. 89-90] con la notación adaptada de [Mon93, Ejemplo 1.5.6].

Ejemplo 3.1.7 (Álgebra de Hopf de Sweedler)**.** Sea K un cuerpo de característica distinta de 2. Sea H la K-álgebra generada por $\{1, g, x, gx\}$ con las relaciones

$$g^2 = 1, \quad x^2 = 0, \quad , xg = -gx.$$

Definimos la comultiplicación $\Delta_H \colon H \to H \otimes_K H$ como

$$g \mapsto g \otimes g, \quad x \mapsto x \otimes 1 + g \otimes x,$$

y la counidad $\epsilon_H \colon H \to K$ por

$$g \mapsto 1, \quad x \mapsto 0.$$

Tomamos como antípoda $\sigma_H \colon H \to H$ la función dada por $g \mapsto g, x \mapsto -gx$. Veamos que H es K-álgebra de Hopf. Para ello debemos ver que se respetan las relaciones. Es decir, debemos verificar que $\Delta_H(x^2) = \Delta_H(0)$, $\Delta_H(g^2) = \Delta_H(1)$ y $\Delta_H(xg) = \Delta_H(-gx)$. Lo mismo para ϵ_H. Verifiquemos algunas de estas cuentas:

$$\begin{aligned}\Delta_H(x^2) &= \Delta_H(x)\Delta_H(x) = (x \otimes 1 + g \otimes x)^2 \\ &= x^2 \otimes 1 + xg \otimes x + gx \otimes x + g^2 \otimes x^2 = 0\end{aligned}$$

$$\begin{aligned}\Delta_H(xg) &= \Delta_H(x)\Delta_H(g) = xg \otimes g + g^2 \otimes xg \\ &= -(gx \otimes g + g^2 \otimes gx) = -\Delta_H(g)\Delta_H(x) = \Delta_H(-gx)\end{aligned}$$

Además debemos ver que se cumple la propiedad de la antípoda. Basta con verificarla sobre los generadores.

$$m_H(I_H \otimes \sigma_H)\Delta_H(g) = g\sigma_H(g) = gg = 1 = \sigma_H(g)g = m_H(\sigma_H \otimes I_H)\Delta_H(g)$$

$$\begin{aligned}m_H(I_H \otimes \sigma_H)\Delta_H(x) &= x\sigma_H(1) + g\sigma_H(x) = x - g^2x = 0 \\ &= -gx + gx = \sigma_H(x) + \sigma_H(g)x = m_H(\sigma_H \otimes I_H)\Delta_H(x)\end{aligned}$$

$$\begin{aligned}m_H(I_H \otimes \sigma_H)\Delta_H(xg) &= xg\sigma_H(g) + 1\sigma_H(xg) = x + \sigma_H(xg) \\ &= x + \sigma_H(g)\sigma_H(x) = x - g^2x = 0 \\ &= \epsilon_H(xg)\end{aligned}$$

$$m_H(\sigma_H \otimes I_H)\Delta_H(xg) = \sigma_H(xg)g + xg = (x + \sigma_H(xg))g = 0 = \epsilon_H(xg)$$

Una K-álgebra de Hopf H se dice **conmutativa** si es un álgebra conmutativa; de forma similar, decimos que H es **coconmutativa** si es una coálgebra coconmutativa. El álgebra de grupo KG del Ejemplo 3.1.3 es coconmutativa; es conmutativa si y sólo si G es un grupo abeliano.

Las álgebras de Hopf de los Ejemplos 3.1.4 y 3.1.6 son conmutativas y coconmutativas. Por otro lado, el álgebra de Hopf de Sweedler del Ejemplo 3.1.7 no es ni conmutativa ni coconmutativa. Una K-álgebra de Hopf de este tipo se dice **grupo cuántico**.

Veamos qué ocurre con la antípoda del Ejemplo 3.1.3. Tenemos

$$\sigma_{KG} \circ \sigma_{KG}(\tau) = \sigma_{KG}(\tau^{-1}) = (\tau^{-1})^{-1} = I_{KG}(\tau).$$

En consecuencia, tiene orden 2. Podemos preguntarnos si es cierto que las antípodas son de orden 2. En general, la respuesta es que no. Si consideramos el álgebra de Hopf de Sweedler del Ejemplo 3.1.7, tenemos

$$\begin{aligned}(\sigma_H \circ \sigma_H)(x) &= \sigma_H(\sigma_H(x)) = \sigma_H(-gx) = \sigma_H(xg)\\ &= \sigma_H(g)\sigma_H(x) = g(-gx) = -g^2x = -x.\end{aligned}$$

En el cálculo usamos que σ_H es un antimorfismo como veremos en breve en la Proposición 3.2.3 y la relación $-gx = xg$. Luego, σ_H no tiene orden 2 en este caso. De hecho, aplicando σ_H cuatro veces sobre x obtenemos x nuevamente. Como sobre g es la identidad y sobre gx sólo depende de lo que ocurra con x, tenemos que el orden es un divisor de 4. La cuenta anterior nos muestra que no puede ser 2, luego la antípoda es de orden 4.

Más adelante, daremos condiciones sobre el álgebra de Hopf que nos permitan afirmar que su antípoda es de orden 2.

3.2. Propiedades básicas

Consideremos una K-coálgebra C y una K-álgebra A. Notemos por $\mathrm{Hom}_K(C, A)$ la colección de transformaciones lineales $\phi\colon C \to A$. Sobre $\mathrm{Hom}_K(C, A)$ podemos definir una multiplicación del siguiente modo. Para $f, g \in \mathrm{Hom}_K(C, A)$, $a \in C$,

$$(f * g)(a) = m_A(f \otimes g)\Delta_C(a) = \sum_{(a)} f(a_{(1)})g(a_{(2)}).$$

Esta multiplicación se llama **convolución** de f y g.

Proposición 3.2.1. *Sea C una K-coálgebra y A una K-álgebra. Entonces, $Hom_K(C, A)$ junto con la convolución $*$ es un monoide.*

Demostración. Veamos que se cumplen los axiomas de monoide. Primero verifiquemos la asociatividad de $*$. Para $f, g \in \mathrm{Hom}_K(C, A)$ tenemos

$$
\begin{aligned}
(f * (g * h))(a) = m_A(f \otimes (g * h))\Delta_C(a) &= \sum_{(a)} f(a_{(1)})(g * h)(a_{(2)}) \\
&= \sum_{(a)} f(a_{(1)}) \sum_{(a_{(2)})} g(a_{(2)_{(1)}})h(a_{(2)_{(2)}}),
\end{aligned}
$$

que en notación de Sweedler es $\sum_{(a)} f(a_{(1)})g(a_{(2)})h(a_{(3)})$. Ahora, por la coasociatividad de Δ_C,

$$
\begin{aligned}
\sum_{(a)} f(a_{(1)})g(a_{(2)})h(a_{(3)}) &= \sum_{(a)} \sum_{(a_{(1)})} f(a_{(1)_{(1)}})g(a_{(1)_{(2)}})h(a_{(2)}) = \sum_{(a)} (f * g)(a_{(1)})h(a_{(2)}) \\
&= m_A((f * g) \otimes h)\Delta_C(a) = ((f * g) * h)(a).
\end{aligned}
$$

Luego, $*$ es asociativa. Ahora, debemos darle una unidad. Para ello, veamos que $\lambda_A \epsilon_C$ sirve a tal efecto. Para $\phi \in \mathrm{Hom}_K(C, A)$, $a \in C$,

$$
\begin{aligned}
(\lambda_A \epsilon_C * \phi)(a) = m_A(\lambda_A \epsilon_C \otimes \phi)\Delta_C(a) &= m_A \left(\sum_{(a)} \lambda_A(\epsilon_C(a_{(1)})) \otimes \phi(a_{(2)}) \right) \\
&= \sum_{(a)} \lambda_A(\epsilon_C(a_{(1)}))\phi(a_{(2)}) = \sum_{(a)} \epsilon_C(a_{(1)})\lambda_A(1_K)\phi(a_{(2)}) \\
&= \sum_{(a)} \epsilon_C(a_{(1)})1_A\phi(a_{(2)}) = \sum_{(a)} \phi(\epsilon_C(a_{(1)})a_{(2)}) = \phi(a).
\end{aligned}
$$

Luego, $\lambda_A \epsilon_C * \phi = \phi$. En forma totalmente análoga obtenemos $\phi * \lambda_A \epsilon_C = \phi$. Entonces, $\mathrm{Hom}_K(C, A)$ es monoide con la convolución. $\square$

Proposición 3.2.2. *Sea H una K-álgebra y sea $\mathrm{Hom}_K(C, A)$ el monoide de la Proposición 3.2.1. Entonces,*

$$\sigma_H * I_H = \lambda_H \epsilon_H = I_H * \sigma_H.$$

En otras palabras, σ_H es inverso a izquierda y a derecha de I_H bajo la operación $*$.

Demostración. Tomamos $a \in H$. Usando la notación de Sweedler

$$(\sigma_H * I_H)(a) = \sum_{(a)} \sigma_H(a_{(1)})a_{(2)}.$$

Esto último es igual, por un lado, a $\epsilon_H(a)1_H$ por la Condición (3.2). Pero además $\epsilon_H(a)1_H = \epsilon_H(a)\lambda_H(1_K) = \lambda_H(\epsilon_H(a)) = (\lambda_H \epsilon_H)(a)$. Por otro lado, por la misma ecuación tenemos que

$$\sum_{(a)} \sigma_H(a_{(1)})a_{(2)} = \sum_{(a)} a_{(1)}\sigma_H(a_{(2)})$$

que podemos escribir como $(I_H * \sigma_H)(a)$. Esto concluye la demostración. $\square$

La convolución se puede usar para mostrar que la antípoda $\sigma_H \colon H \to H$ es un antimorfismo de álgebras en un sentido que será precisado en la siguiente proposición.

Proposición 3.2.3. *Sea H una K-álgebra de Hopf con antípoda σ_H. Entonces, se verifican las siguientes propiedades:*

(i) $\sigma_H(ab) = \sigma_H(b)\sigma_H(a)$ *para todo $a, b \in H$, esto es, σ_H es antimorfismo de álgebras;*

(ii) $\sigma_H(1_H) = 1_H$.

Demostración. (i): Consideramos la K-coálgebra $H \otimes H$ y la colección de transformaciones lineales $\mathrm{Hom}_K(H\otimes H, H)$. Tenemos que $m_H \in \mathrm{Hom}_K(H\otimes H, H)$. Vamos a definir dos elementos más en $\mathrm{Hom}_K(H\otimes H, H)$ de la siguiente manera. Sean $a, b \in H$,

$$\sigma_H m_H \colon H \otimes H \to H, \quad a \otimes b \mapsto \sigma_H(ab),$$
$$\phi = m_H(\sigma_H \otimes \sigma_H)\tau \colon H \otimes H \to H, \quad a \otimes b \mapsto \sigma_H(b)\sigma_H(a).$$

Como vimos en la página 22, $H \otimes H$ es coálgebra con comultiplicación dada por $\Delta_{H\otimes H}(a \otimes b) = \sum_{(a,b)} a_{(1)} \otimes b_{(1)} \otimes a_{(2)} \otimes b_{(2)}$ y counidad $\epsilon_{H\otimes H}(a \otimes b) = \epsilon_H(a)\epsilon_H(b)$. Para probar ($i$) primero vamos a ver que

$$m_H * \phi = \lambda_H \epsilon_{H\otimes H} = \phi * m_H, \tag{3.4}$$

y después, que

$$m_H * \sigma_H m_H = \lambda_H \epsilon_{H\otimes H} = \sigma_H m_H * m_H. \tag{3.5}$$

Veamos primero (3.4). Para $a, b \in H$,

$$\begin{aligned}
(m_H * \phi)(a \otimes b) &= (m_H * m_H(\sigma_H \otimes \sigma_H)\tau)(a \otimes b) \\
&= m_H(m_H \otimes m_H(\sigma_H \otimes \sigma_H)\tau)\Delta_H(a \otimes b) \\
&= m_H \left(\sum_{(a,b)} m_H(a_{(1)} \otimes b_{(1)}) \otimes m_H(\sigma_H \otimes \sigma_H)\tau(a_{(2)} \otimes b_{(2)}) \right) \\
&= \sum_{(a,b)} a_{(1)} b_{(1)} \sigma_H(b_{(2)}) \sigma_H(a_{(2)}) = \sum_{(a)} a_{(1)} \epsilon_H(b) \sigma_H(a_{(2)}) \\
&= \sum_{(a)} \epsilon_H(b) a_{(1)} \sigma_H(a_{(2)}) = \epsilon_H(b)\epsilon_H(a) 1_H = \lambda_H \epsilon_{H\otimes H}(a \otimes b).
\end{aligned}$$

En las líneas 3 y 4 hemos usado la propiedad de la antípoda. Luego $m_H * \phi = \lambda_H \epsilon_{H\otimes H}$. Por un cálculo similar, tenemos $\phi * m_H = \lambda_H \epsilon_{H\otimes H}$. Veamos ahora (3.5).

Sean $a, b \in H$,

$$\begin{aligned}(m_H * \sigma_H m_H)(a \otimes b) &= m_H(m_H \otimes \sigma_H m_H)\Delta_{H\otimes H}(a \otimes b)\\ &= m_H\left(\sum_{(a,b)} m_H(a_{(1)} \otimes b_{(1)}) \otimes \sigma_H m_H(a_{(2)} \otimes b_{(2)})\right)\\ &= \sum_{(a,b)} a_{(1)}b_{(1)}\sigma_H(a_{(2)}b_{(2)}) = m_H(I_H \otimes \sigma_H)\Delta_H(ab)\\ &= \epsilon_H(ab)1_H = \epsilon_H(a)\epsilon_H(b)1_H = \lambda_H\epsilon_{H\otimes H},\end{aligned}$$

luego, $m_H * \sigma_H m_H = \lambda_H \epsilon_{H\otimes H}$. De forma similar, tenemos que $\sigma_H m_H * m_H = \lambda_H\epsilon_{H\otimes H}$. Ahora, juntando (3.4) y (3.5), tenemos

$$m_H * \phi = m_H * \sigma_H m_H,$$

luego,

$$\begin{aligned}(\phi * m_H) * \phi &= (\phi * m_H) * \sigma_H m_H\\ \lambda_H\epsilon_{H\otimes H} * \phi &= \lambda_H\epsilon_{H\otimes H} * \sigma_H m_H\\ \phi &= \sigma_H m_H \qquad \text{por la Proposición 3.2.1}\end{aligned}$$

Esto concluye la prueba de (i).

(ii): Observemos que

$$\begin{aligned}1_H = 1_K 1_H = \epsilon_H(1_H)1_K &= m_H(I_H \otimes \sigma_H)\Delta_H(1_H)\\ &= m_H(I_H \otimes \sigma_H)\Delta_H(1_H \otimes 1_H) = \sigma_H(1_H).\end{aligned}$$

□

Observación. Notemos que si H es conmutativa, σ_H es morfismo de álgebras.

3.2.1. Antípodas de orden 2

Podemos probar ahora una proposición que nos permite determinar bajo qué condiciones la antípoda de un álgebra de Hopf tiene orden 2.

Proposición 3.2.4. *[Swe69, Proposición 4.0.1] Sea H un álgebra de Hopf. Son equivalentes:*

(i) $\sum_{(h)} h_{(2)}\sigma_H(h_{(1)}) = \lambda_H\epsilon_H(h)$ *para todo* $h \in H$,

(ii) $\sum_{(h)} \sigma_H(h_{(2)})h_{(1)} = \lambda_H\epsilon_H(h)$ *para todo* $h \in H$,

(iii) $\sigma_H\sigma_H = I_H$.

Demostración. $\underline{(i) \Rightarrow (iii)}$: Basta ver que $\sigma_H\sigma_H$ es inversa a derecha de σ_H pues I_H es inversa de σ_H y la inversa es única. Sea $h \in H$,

$$
\begin{aligned}
\sigma_H * (\sigma_H\sigma_H)(h) &= \sum_{(h)} \sigma_H(h_{(1)})\sigma_H\sigma_H(h_{(2)}) \\
&= \sigma_H\left(\sum_{(h)} \sigma_H(h_{(2)})h_{(1)}\right) && \text{por Proposición 3.2.3(i)} \\
&= \sigma_H(\lambda_H\epsilon_H(h)) && \text{por hipótesis} \\
&= \epsilon_H(h)\sigma_H(\lambda_H(1_K)) = \epsilon_H(h)\sigma_H(1_H) \\
&= \epsilon_H 1_H && \text{por Proposición 3.2.3(ii)} \\
&= \lambda_H\epsilon_H(h).
\end{aligned}
$$

como queríamos ver.

$\underline{(iii) \Rightarrow (ii)}$: Notemos que

$$
\begin{aligned}
\lambda_H\epsilon_H(h) &= I_H * \sigma_H(h) && \text{por definición de antípoda} \\
&= \sum_{(h)} h_{(1)}\sigma_H(h_{(2)}) = \sum_{(h)} \sigma_H\sigma_H(h_{(1)})\sigma_H(h_{(2)}) && \text{por hipótesis} \\
&= \sigma_H\left(\sum_{(h)} h_{(2)}\sigma_H(h_{(1)})\right).
\end{aligned}
$$

Aplicando σ_H a ambos lados de la igualdad obtenida y usando la hipótesis tenemos

$$\sigma_H(\lambda_H\epsilon_H(h)) = \sigma_H\sigma_H\left(\sum_{(h)} h_{(2)}\sigma_H(h_{(1)})\right) = \sum_{(h)} h_{(2)}\sigma_H(h_{(1)}.$$

Como vimos en la implicación anterior, tenemos que $\sigma_H(\lambda_H\epsilon_H) = \lambda_H\epsilon_H$. Entonces,

$$\lambda_H\epsilon_H(h) = \sum_{(h)} h_{(2)}\sigma_H(h_{(1)})$$

como queríamos ver.

$\underline{(ii) \Rightarrow (iii)}$: En forma análoga a la primera implicación, basta ver que $\sigma_H\sigma_H$ es inversa a izquierda de σ_H.

Sea $h \in H$,

$$
\begin{aligned}
(\sigma_H\sigma_H) * \sigma_H(h) &= \sum_{(h)} \sigma_H\sigma_H(h_{(1)})\sigma_H(h_{(2)}) = \sigma_H\left(\sum_{(h)} h_{(2)}\sigma_H(h_{(1)})\right) \\
&= \sigma_H(\lambda_H\epsilon_H)(h) = \lambda_H\epsilon_H(h)
\end{aligned}
$$

como queríamos ver.

(*iii*) $\Rightarrow$ (*i*): En forma análoga a la segunda implicación, notemos que:

$$\begin{aligned}\lambda_H\epsilon_H(h) = \sigma_H * I_H(h) &= \sum_{(h)} \sigma_H(h_{(1)})h_{(2)} \\ &= \sum_{(h)} \sigma_H(h_{(1)})\sigma_H\sigma_H(h_{(2)}) = \sigma_H\left(\sum_{(h)} \sigma_H(h_{(2)})h_{(1)}\right).\end{aligned}$$

Aplicando σ_H a ambos términos de la igualdad obtenida y usando la hipótesis, tenemos

$$\sigma_H(\lambda_H\epsilon_H(h)) = \sigma_H\sigma_H\left(\sum_{(h)} \sigma_H(h_{(2)})h_{(1)}\right) = \sum_{(h)} \sigma_H(h_{(2)})h_{(1)}$$

y entonces

$$\lambda_H\epsilon_H(h) = \sum_{(h)} \sigma_H(h_{(2)})h_{(1)}$$

como queríamos. □

Corolario 3.2.5. *Si H es conmutativa o coconmutativa, entonces $\sigma_H\sigma_H = I_H$.*

Demostración. Si H es conmutativa, tenemos

$$\begin{aligned}\lambda_H\epsilon_H(h) &= \sum_{(h)} \sigma_H(h_{(1)})h_{(2)} && \text{por definición de antípoda} \\ &= \sum_{(h)} h_{(2)}\sigma_H(h_{(1)}) && \text{pues } H \text{ es conmutativa.}\end{aligned}$$

Entonces, por la Proposición 3.2.4(*ii*) $\Rightarrow$ (*iii*), tenemos lo pedido.

Por otro lado, si H es coconmutativa, se tiene

$$\begin{aligned}\lambda_H\epsilon_H(h) &= \sum_{(h)} h_{(1)}\sigma_H(h_{(2)}) && \text{por definición de antípoda} \\ &= \sum_{(h)} h_{(2)}\sigma_H(h_{(1)}) && \text{pues } H \text{ es coconmutativa.}\end{aligned}$$

Luego, por la Proposición 3.2.4(*ii*) $\Rightarrow$ (*iii*) nuevamente, tenemos lo pedido. □

Vamos a ver ahora que σ_H es antimorfismo de coálgebras (en un sentido que precisamos a continuación).

Proposición 3.2.6. *Sea H una K-álgebra de Hopf con antípoda σ_H. Entonces se satisfacen las siguientes propiedades:*

(*i*) $\tau(\sigma_H \otimes \sigma_H)\Delta_H = \Delta_H\sigma_H$, *(ii)* $\epsilon_H \sigma_H = \epsilon_H$.

Demostración. Consideramos $\mathrm{Hom}_K(H, H \otimes H)$ el conjunto de transformaciones lineales de H en $H \otimes H$. Notemos que $\Delta_H \in \mathrm{Hom}_K(H, H \otimes H)$. Definimos dos elementos más:

$$\psi = \tau(\sigma_H \otimes \sigma_H)\Delta_H \colon H \to H \otimes H, \quad a \mapsto \sum_{(a)} \sigma_H(a_{(2)}) \otimes \sigma_H(a_{(1)}),$$

$$\Delta_H \sigma_H \colon H \to H \otimes H, \quad a \mapsto \sum_{(\sigma_H(a))} \sigma_H(a)_{(1)} \otimes \sigma_H(a)_{(2)},$$

para todo $a \in H$.

En la página 10, vimos cómo darle a $H \otimes H$ estructura de K-álgebra. Recordemos que la multiplicación está dada por $(a \otimes b) \otimes (c \otimes d) \mapsto ac \otimes bd$ y la unidad por $r \mapsto \lambda_H(r) \otimes 1_H = r1_H \otimes 1_H$ para todo $a, b, c, d \in H, r \in K$. Adoptaremos una estrategia similar a la de la Proposición 3.2.3 para probar que los elementos definidos arriba son iguales. Más precisamente, veremos que

$$\Delta_H * \psi = \lambda_{H \otimes H} \epsilon_H = \psi * \Delta_H \tag{3.6}$$

y

$$\Delta_H * \Delta_H \sigma_H = \lambda_{H \otimes H} \epsilon_H = \Delta_H \sigma_H * \Delta_H. \tag{3.7}$$

Para probar (3.6), sea $a \in H$,

$$\begin{aligned}
(\Delta_H * \psi)(a) &= m_{H \otimes H}(\Delta_H \otimes \psi)\Delta_H(a) = m_{H \otimes H}(\Delta_H \otimes \psi)\left(\sum_{(a)} a_{(1)} \otimes a_{(2)}\right) \\
&= m_{H \otimes H}\left(\sum_{(a)} \Delta_H(a_{(1)}) \otimes \psi(a_{(2)})\right) \\
&= m_{H \otimes H}\left(\sum_{(a)} a_{(1)} \otimes a_{(2)} \otimes \sigma_H(a_{(4)}) \otimes \sigma_H(a_{(3)})\right) \\
&= \sum_{(a)} a_{(1)}\sigma_H(a_{(4)}) \otimes a_{(2)}\sigma_H(a_{(3)}) \\
&= \sum_{(a)} a_{(1)}\sigma_H(a_{(3)}) \otimes \epsilon_H(a_{(2)})1_H \qquad \text{por la propiedad de la antípoda} \\
&= \sum_{(a)} \epsilon_H(a_{(2)})a_{(1)}\sigma_H(a_{(3)}) \otimes 1_H \\
&= \sum_{(a)} a_{(1)}\sigma_H(a_{(2)}) \otimes 1_H \qquad \text{por la propiedad de la counidad} \\
&= \epsilon_H(a)1_H \otimes 1_H \qquad \text{por la propiedad de la antípoda} \\
&= (\lambda_{H \otimes H}\epsilon_H)(a).
\end{aligned}$$

Esto prueba que $\Delta_H * \psi = \lambda_{H\otimes H}\epsilon_H$. De forma similar, obtenemos $\psi * \Delta_H = \lambda_{H\otimes H}\epsilon_H$. Entonces, vale (3.6).

De forma directa, se demuestra (3.7). Se sigue que

$$\begin{aligned} \psi * (\Delta_H * \psi) &= \psi * (\Delta_H * \Delta_H \sigma_H) \\ (\psi * \Delta_H) * \psi &= (\psi * \Delta_H) * \Delta_H \sigma_H \\ \lambda_{H\otimes H}\epsilon_H * \psi &= \lambda_{H\otimes H}\epsilon_H * \Delta_H \sigma_H \\ \psi &= \Delta_H \sigma_H. \end{aligned}$$

Esto concluye (i).

Para ver (ii), notemos que para todo $a \in H$,

$$\begin{aligned} \epsilon_H(a) &= \epsilon_H(a)\epsilon_H(1_H) = \epsilon_H(\epsilon_H(a)1_H) \\ &= \epsilon_H\left(\sum_{(a)} a_{(1)}\sigma_H(a_{(2)})\right) \qquad \text{por la propiedad de la antípoda} \\ &= \sum_{(a)} \epsilon_H(a_{(1)})\epsilon_H(\sigma_H(a_{(2)})) = \sum_{(a)} \epsilon_H(\sigma_H(\epsilon_H(a_{(1)})a_{(2)})) \\ &= \epsilon_H(\sigma_H(a)) \qquad \text{por la propiedad de la counidad.} \end{aligned}$$

□

Observación. De forma similar a lo que mencionamos anteriormente, σ_H es un morfismo de coálgebras si H es coconmutativa.

3.3. Biideales, cocientes y duales

Definición 3.3.1. Sea H una K-álgebra de Hopf. Un *ideal de Hopf* I es un biideal (viendo a H como K-biálgebra) tal que $\sigma_H(I) \subseteq I$.

Proposición 3.3.2. *Sea $I \subseteq H$ un ideal de Hopf de H. Entonces, H/I es una K-álgebra de Hopf.*

Demostración. Por la Proposición 2.1.6, H/I es K-biálgebra. Además, como $\sigma_H(I) \subseteq I$, entonces σ_H induce una transformación K-lineal $\sigma_{H/I}\colon H/I \to H/I$ definida como $a + I \mapsto \sigma_H(a) + I$. Tenemos entonces

$$\begin{aligned} m_{H/I}(I_{H/I} \otimes \sigma_{H/I})\Delta_{H/I}(a+I) &= m_{H/I}(I_{H/I} \otimes \sigma_{H/I})\left(\sum_{(a)} a_{(1)} + I \otimes a_{(2)} + I\right) \\ &= \sum_{(a)} a_{(1)}\sigma_H(a_{(2)}) + I = \epsilon_H(a)1_H + I \\ &= \epsilon_{H/I}(a+I)1_{H/I}. \end{aligned}$$

En forma análoga obtenemos

$$m_{H/I}(\sigma_{H/I} \otimes I_{H/I})\Delta_{H/I}(a+I) = \epsilon_{H/I}(a+I)1_{H/I}.$$

Luego, H/I es K-álgebra de Hopf, como queríamos ver. □

Proposición 3.3.3. *Sea H un K-espacio vectorial de dimensión finita. Entonces, H es K-álgebra de Hopf si y sólo si H^* es K-álgebra de Hopf.*

Demostración. Supongamos que H es K-álgebra de Hopf. Por la Proposición 2.1.13, H^* es una biálgebra. Sea $\sigma_H^* \colon H^* \to H^*$ la traspuesta de σ_H. Entonces, para $f \in H^*, a \in H$,

$$\begin{aligned}(m_{H^*}(I_{H^*} \otimes \sigma_{H^*})\Delta_{H^*}(f))(a) &= m_{H^*}((I_{H^*} \otimes \sigma_{H^*})\Delta_{H^*}(f))(a)\\ &= ((I_{H^*} \otimes \sigma_{H^*})\Delta_{H^*}(f))\Delta_H(a) = \Delta_{H^*}(f)(I_H \otimes \sigma_H)\Delta_H(a)\\ &= f(m_H(I_H \otimes \sigma_H)\Delta_H(a)) = f(\epsilon_H(a)1_H)\\ &= \epsilon_H(a)f(1_H) = \epsilon_{H^*}(f)\epsilon_H(a)\\ &= \epsilon_{H^*}(f)1_{H^*}(a).\end{aligned}$$

En forma similar, obtenemos

$$m_{H^*}(\sigma_{H^*} \otimes I_{H^*})\Delta_{H^*}(f) = \epsilon_{H^*}(f)1_{H^*}.$$

En consecuencia, $\sigma_{H^*} = \sigma_H^*$ satisface la propiedad de la antípoda y H^* es K-álgebra de Hopf.

Recíprocamente, si H^* es K-álgebra de Hopf, entonces $H^{**} \cong H$ es K-álgebra de Hopf. □

Ejemplo 3.3.4. Sea G un grupo finito. Entonces KG es K-álgebra de Hopf (ver Ejemplo 3.1.3). Entonces, KG^* es K-álgebra de Hopf. El subconjunto $\{p_\upsilon\}_{\upsilon \in G}$ con $p_\upsilon(\tau) = \delta_{\upsilon,\tau}$ es una base para KG^*. La multiplicación en KG^* se define como $(p_\upsilon p_\tau)(\omega) = p_\upsilon(\omega)p_\tau(\omega)$, luego $p_\upsilon p_\tau = \delta_{\upsilon,\tau}p_\upsilon$. La unidad es

$$\lambda_{KG^*} \colon K \to KG^*, \quad r \mapsto r\epsilon_{KG}.$$

La comultiplicación de KG^* está dada por

$$\Delta_{KG^*}(p_\upsilon) = \sum_{\upsilon=\tau\omega} p_\tau \otimes p_\omega,$$

(recordar la Proposición 1.3.11), y la counidad ϵ_{KG^*} está dada por $p_\upsilon \mapsto p_\upsilon(1)$. Por último, la antípoda $\sigma_{KG^*} \colon KG^* \to KG^*$ está definida como $p_\upsilon \mapsto p_{\upsilon^{-1}}$.

Capítulo 4

Aplicaciones

En este capítulo vamos a ver tres aplicaciones de las álgebras de Hopf. En primer lugar, vamos a estudiar las biálgebras casi coconmutativas y las estructuras cuasitriangulares sobre biálgebras. Mostraremos que toda biálgebra cuasitriangular determina una solución de la ecuación cuántica de Yang-Baxter y trataremos especialmente dos ejemplos de dimensión dos para hallar todas sus estructuras cuasitriangulares. Veremos que las álgebras de Hopf casi coconmutativas permiten generalizar nuestra respuesta al problema de cuándo una antípoda tiene orden 2. Específicamente, probaremos que las antípodas al cuadrado dan una conjugación.

Como segunda aplicación, definiremos el grupo de trenzas en tres cuerdas y mostraremos que las estructuras cuasitriangulares determinan representaciones de este grupo.

Por último, la tercera aplicación relaciona variedades afines con álgebras de Hopf. Más precisamente, veremos qué estructura algebraica podemos asociarle a una variedad afín Λ a partir de la identificación con el conjunto de morfismos de K-álgebras de su anillo de coordenadas $K[\Lambda]$ al cuerpo K. Veremos que si $K[\Lambda]$ es una biálgebra o un álgebra de Hopf, entonces podemos darle a Λ estructura de monoide o grupo, respectivamente.

4.1. Estructuras cuasitriangulares y QYBE

En esta sección introducimos los conceptos de biálgebra casi coconmutativa y biálgebra cuasitriangular. Veremos que las biálgebras cuasitriangulares determinan soluciones a la ecuación cuántica de Yang-Baxter y veremos cómo calcular las estructuras cuasitriangulares de una biálgebra y un álgebra de Hopf de dimensión 2. Por último, veremos que las álgebras de Hopf cuasitriangulares generalizan a las álgebras de Hopf con antípoda de orden 2.

Sea K un cuerpo. Sea B una K-biálgebra y $B \otimes B$ el producto tensorial de K-*álgebras*. Sea $U(B \times B)$ el grupo de unidades de $B \otimes B$ y $R \in U(B \otimes B)$.

Definición 4.1.1. El par (B, R) se dice *casi coconmutativo* si el elemento R satisface

$$\tau(\Delta_B(b)) = R\Delta_B(b)R^{-1} \tag{4.1}$$

para todo $b \in B$.

Si la biálgebra B es coconmutativa, entonces el par $(B, 1 \otimes 1)$ es casi coconmutativo. Además, si B es conmutativa pero no coconmutativa, entonces (B, R) no puede ser casi coconmutativo para ningún $R \in U(B \otimes B)$ pues la condición (4.1) se reduce a la condición de coconmutatividad.

Escribamos $R = \sum_{i=1}^{n} a_i \otimes b_i \in U(B \otimes B)$. Notaremos

$$R^{12} = \sum_{i=1}^{n} a_i \otimes b_i \otimes 1 \in B^{\otimes 3},$$
$$R^{13} = \sum_{i=1}^{n} a_i \otimes 1 \otimes b_i \in B^{\otimes 3},$$
$$R^{23} = \sum_{i=1}^{n} 1 \otimes a_i \otimes b_i \in B^{\otimes 3}.$$

Definición 4.1.2. El par (B, R) se dice *cuasitriangular* si (B, R) es casi coconmutativo y además se cumplen las condiciones:

$$(\Delta_B \otimes I_B)R = R^{13}R^{23}, \tag{4.2}$$
$$(I_B \otimes \Delta_B)R = R^{13}R^{12}. \tag{4.3}$$

Claramente, si B es coconmutativa, entonces $(B, 1 \otimes 1)$ es cuasitriangular. Una **estructura cuasitriangular** es un elemento $R \in U(B \otimes B)$ tal que (B, R) es cuasitriangular. Dos biálgebras cuasitriangulares (B, R) y (B', R') se dicen **isomorfas como biálgebras cuasitriangulares** si existe un isomorfismo de biálgebras $\phi\colon B \to B'$ tal que $R' = (\phi \otimes \phi)(R)$. Lo notamos $(B, R) \cong (B', R')$. Dos estructuras cuasitriangulares R, R' sobre B son equivalentes si $(B, R) \cong (B, R')$ como biálgebras cuasitriangulares.

Ejemplo 4.1.3. Supongamos que B es una biálgebra conmutativa y no coconmutativa (por ejemplo podemos tomar $B = KG^*$ con G un grupo finito no abeliano). Entonces (B, R) no puede ser cuasitriangular para ningún $R \in U(B \otimes B)$ puesto que vimos que no puede ser casi coconmutaivo; es decir, B no tiene estructuras cuasitriangulares.

Presentaremos ahora unos ejemplos en forma parcial que serán tratados con más detalle en lo sucesivo.

Ejemplo 4.1.4. Sea $T = \{1, a\}$ el monoide con multiplicación dada por la tabla

	1	a
1	1	a
a	a	a

Sea KT la biálgebra del monoide. Hemos visto esta biálgebra con anterioridad: es isomorfa a la biálgebra de Myhill-Nerode del Ejemplo 2.2.12. Veremos que sólo tiene estructura cuasitriangular trivial $R = 1 \otimes 1$.

Ejemplo 4.1.5. Sea K un cuerpo de característica $\neq 2$, sea C_2 el grupo cíclico de orden 2 generado por el elemento g y sea KC_2 la biálgebra del grupo. Entonces, existen exactamente dos estructuras cuasitriangulares no equivalentes sobre KC_2, que llamaremos $R_0 = 1 \otimes 1$ y

$$R_1 = \frac{1}{2}(1 \otimes 1 + 1 \otimes g + g \otimes 1 - g \otimes g).$$

Mostramos el siguiente ejemplo para ilustrar un caso en que se pueden definir infinitas estructuras cuasitriangulares no equivalentes sobre una misma álgebra de Hopf. Se encuentra tratado con mayor detalle en [Rad93, §2].

Ejemplo 4.1.6. Sea H el álgebra de Hopf de Sweedler del Ejemplo 3.1.7 definida sobre el cuerpo $K = \mathbb{Q}$. Para $a \in K$, sea

$$\begin{aligned} R^{(a)} = \frac{1}{2}&(1 \otimes 1 + 1 \otimes g + g \otimes 1 - g \otimes g) \\ &+ \frac{a}{2}(x \otimes x - x \otimes gx + gx \otimes x + gx \otimes gx). \end{aligned}$$

Luego, $R^{(a)}$ es estructura cuasitriangular sobre H. Más aún, existe un número infinito de estructuras cuasitriangulares no equivalentes de la forma $R^{(a)}$.

Nuestra intención es clasificar las estructuras cuasitriangulares de los Ejemplos 4.1.4 y 4.1.5. Pero antes vamos a mostrar por qué es importante el estudio de las biálgebras cuasitriangulares.

Proposición 4.1.7 (Drinfeld, 1990)**.** *Supongamos que (B, R) es una biálgebra cuasitriangular. Entonces*

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}. \tag{4.4}$$

Demostración. Por un lado tenemos

$$\begin{aligned} R^{12}R^{13}R^{23} &= R^{12}(\Delta_B \otimes I_B)(R) && \text{por (4.2)} \\ &= (R \otimes 1)\left(\sum_{i=1}^{n} \Delta_B(a_i) \otimes b_i\right) \\ &= \sum_{i=1}^{n} R\Delta_B(a_i) \otimes b_i = \sum_{i=1}^{n} \tau\Delta_B(a_i)R \otimes b_i && \text{por (4.1)} \\ &= \left(\sum_{i=1}^{n} \tau\Delta_B(a_i) \otimes b_i\right)(R \otimes 1) \\ &= (\tau\Delta_B \otimes I_B)\left(\sum_{i=1}^{n} a_i \otimes b_i\right)(R \otimes 1). \end{aligned}$$

Continuando el cálculo, tenemos

$$\begin{aligned}(\tau\Delta_B \otimes I_B)\left(\sum_{i=1}^{n} a_i \otimes b_i\right)(R\otimes 1) &= (\tau\Delta_B \otimes I_B)(R)R^{12}\\ &= (\tau \otimes I_B)(\Delta_B \otimes I_B)(R)R^{12}\\ &= (\tau \otimes I_B)(R^{13}R^{23})R^{12} \qquad \text{por (4.2)}\\ &= R^{23}R^{13}R^{12}.\end{aligned}$$

Y esto concluye la prueba. □

La ecuación (4.4) se conoce como **ecuación cuántica de Yang-Baxter** (**QYBE**, por sus siglas en inglés). La Proposición 4.1.7 nos dice que las biálgebras cuasitriangulares determinan soluciones para la QYBE. Más adelante veremos que las soluciones de la QYBE nos dan representaciones del grupo de trenzas $\mathbb{B}_3$. Por el momento, continuamos con el problema de construir estructuras cuasitriangulares para la biálgebra de monoide KT y la biálgebra de grupo KC_2.

La siguiente proposición nos permite extender isomorfismos entre biálgebras a isomorfismos de biálgebras cuasitriangulares.

Proposición 4.1.8. *Supongamos que (B,R) es cuasitriangular y que $\phi\colon B\to B'$ es un isomorfismo de K-biálgebras. Sea $R' = (\phi\otimes\phi)(R)$. Entonces, (B',R') es cuasitriangular.*

Demostración. Notemos primero que $(\phi\otimes\phi(R^{-1})) = ((\phi\otimes\phi)(R))^{-1}$. Sea $b'\in B'$, luego existe $b\in B$ tal que $\phi(b)=b'$. Ahora,

$$\begin{aligned}\tau\Delta_{B'}(b') = \tau\Delta_{B'}(\phi(b)) &= \tau(\phi\otimes\phi)\Delta_B(b) \qquad \text{pues } \phi \text{ es morfismo de biálgebras}\\ &= (\phi\otimes\phi)\tau\Delta_B(b)\\ &= (\phi\otimes\phi)(R\Delta_B(b)R^{-1}) \qquad \text{pues } (B,R) \text{ es cuasitriangular.}\end{aligned}$$

Si continuamos el cálculo usando que $\phi\otimes\phi$ es morfismo de álgebras $B\otimes B\to B'\otimes B'$,

$$\begin{aligned}(\phi\otimes\phi)(R\Delta_B(b)R^{-1}) &= (\phi\otimes\phi)(R)(\phi\otimes\phi)\Delta_B(b)(\phi\otimes\phi)(R^{-1})\\ &= (\phi\otimes\phi)(R)(\phi\otimes\phi)\Delta_B(b)((\phi\otimes\phi)(R))^{-1}\\ &= R'\Delta_{B'}(b')(R')^{-1}\end{aligned}$$

y entonces (B',R') es casi coconmutativa. Veamos ahora que se verifica la Condición (4.2):

$$\begin{aligned}(\Delta_{B'}\otimes I_{B'})(R') = (\Delta_{B'}\otimes I_{B'})(\phi\otimes\phi)(R) &= (\Delta_{B'}\otimes I_{B'})\left(\sum_{i=1}^{n}\phi(a_i)\otimes\phi(b_i)\right)\\ &= \sum_{i=1}^{n}\Delta_{B'}(\phi(a_i))\otimes\phi(b_i) = \sum_{i=1}^{n}(\phi\otimes\phi)\Delta_B(a_i)\otimes\phi(b_i)\\ &= (\phi\otimes\phi\otimes\phi)\left(\sum_{i=1}^{n}\Delta_B(a_i)\otimes b_i\right) = (\phi\otimes\phi\otimes\phi)(\Delta_B\otimes I_B)(R).\end{aligned}$$

Continuando con la misma cuenta,

$$\begin{aligned}(\phi\otimes\phi\otimes\phi)(\Delta_B\otimes I_B)(R) &= (\phi\otimes\phi\otimes\phi)(R^{13}R^{23}) \qquad \text{pues } (B,R) \text{ es cuasitriangular}\\ &= (\phi\otimes\phi\otimes\phi)\left(\left(\sum_{i=1}^{n} a_i\otimes 1\otimes b_i\right)\left(\sum_{i=1}^{n} 1\otimes a_i\otimes b_i\right)\right)\\ &= \left(\sum_{i=1}^{n}\phi(a_i)\otimes 1\otimes\phi(b_i)\right)\left(\sum_{i=1}^{n} 1\otimes\phi(a_i)\otimes\phi(b_i)\right)\\ &= ((\phi\otimes\phi)(R))^{13}((\phi\otimes\phi)(R))^{23}\\ &= (R')^{13}(R')^{23}.\end{aligned}$$

Luego, se verifica la Condición (4.2). De forma análoga verificamos la condición (4.3). Y entonces (B',R') es cuasitriangular. $\square$

Necesitaremos las siguientes proposiciones para encontrar estructuras cuasitriangulares. Recordemos las transformaciones $s_1\colon K\otimes B\to B, s_2\colon B\otimes K\to B$ que están definidas como $r\otimes b\mapsto rb, b\otimes r\mapsto rb$, respectivamente.

Proposición 4.1.9. *Supongamos que* (B,R) *es cuasitriangular. Entonces*

(i) $s_1(\epsilon_B\otimes I_B)(R)=1$,

(ii) $s_2(I_B\otimes\epsilon_B)(R)=1$.

Demostración. Para probar (i), observamos que

$$\begin{aligned}(s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)(\Delta_B\otimes I_B)(R) &= (s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)\left(\sum_{i=1}^{n}\Delta_B(a_i)\otimes b_i\right)\\ &= (s_1\otimes I_B)\left(\sum_{i=1}^{n}(\epsilon_B\otimes I_B)\Delta_B(a_i)\otimes b_i\right)\\ &= \sum_{i=1}^{n} s_1(\epsilon_B\otimes I_B)\Delta_B(a_i)\otimes b_i = \sum_{i=1}^{n} a_i\otimes b_i = R.\end{aligned}$$

Entonces, tenemos

$$\begin{aligned}&R = (s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)(\Delta_B\otimes I_B)(R)\\ &= (s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)(R^{13}R^{23}) \qquad \text{por (4.2)}\\ &= (s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)(R^{13})(s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)(R^{23})\\ &= (s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)\left(\sum_{i=1}^{n} a_i\otimes 1\otimes b_i\right)(s_1\otimes I_B)(\epsilon_B\otimes I_B\otimes I_B)\left(\sum_{i=1}^{n} 1\otimes a_i\otimes b_i\right)\\ &= \left(\sum_{i=1}^{n}\epsilon_B(a_i)1\otimes b_i\right)\left(\sum_{i=1}^{n} a_i\otimes b_i\right) = \left(\sum_{i=1}^{n} 1\otimes\epsilon_B(a_i)b_i\right)R.\end{aligned}$$

Entonces,

$$\sum_{i=1}^{n} 1 \otimes \epsilon_B(a_i)b_i = 1 \otimes 1$$

y, en consecuencia,

$$1 = s_1\left(\sum_{i=1}^{n} \epsilon_B(a_i) \otimes b_i\right) = s_1(\epsilon_B \otimes I_B)(R).$$

De forma análoga, se prueba (ii). □

Ahora estamos en condiciones de probar que la biálgebra del monoide $B = KT$ del Ejemplo 4.1.4 tiene una única estructura cuasitriangular y es la trivial. Antes observemos que el dual KT^* es una K-biálgebra con base $\{e_1, e_a\}$ donde $e_x(y) = \delta_{x,y}$. La estructura de álgebra en KT^* está dada por $e_x e_y = \delta_{x,y}e_x$. Por la Proposición 1.3.11, la comultiplicación está dada por

$$\Delta_{KT^*}(e_1) = e_1 \otimes e_1 \qquad \Delta_{KT^*}(e_a) = e_1 \otimes e_a + e_a \otimes e_1 + e_a \otimes e_a.$$

La counidad viene dada por

$$\epsilon_{KT^*}(e_1) = 1 \qquad \epsilon_{KT^*}(e_a) = 0.$$

Tenemos un isomorfismo de biálgebras $\phi\colon KT \to KT^*$ definido como $\phi(1) = e_1 + e_a$ y $\phi(a) = e_1$.

Proposición 4.1.10. *Sea KT la K-biálgebra del Ejemplo 4.1.4. Entonces existe una única estructura cuasitriangular en KT tomando $R = 1 \otimes 1$.*

Demostración. Claramente, $1 \otimes 1$ es estructura cuasitriagular de KT. Debemos ver que no puede haber otra.

Si (KT, R) es cuasitriangular, entonces (KT^*, R') con $R' = (\phi \otimes \phi)(R)$ es cuasitriangular por la Proposición 4.1.8. Veamos entonces cómo son las estructuras cuasitriangulares en el dual.

Supongamos pues que (KT^*, R') es cuasitriangular para cierto $R' \in U(KT^* \otimes KT^*)$. Dado que $\{e_1 \otimes e_1, e_1 \otimes e_a, e_a \otimes e_1, e_a \otimes e_a\}$ es base para $KT^* \otimes KT^*$, podemos escribir

$$R' = w(e_1 \otimes e_1) + x(e_1 \otimes e_a) + y(e_a \otimes e_1) + z(e_a \otimes e_a)$$

para $w, x, y, z \in K$. Para simplificar los cálculos adoptaremos la notación $1 = 1_{KT^*}$, $I = I_{KT^*}$, $\epsilon = \epsilon_{KT^*}$ y $\Delta = \Delta_{KT^*}$. Por la parte (i) de la Proposición 4.1.9,

$$\begin{aligned} 1 &= e_1 + e_a \\ &= s_1(\epsilon \otimes I)(w(e_1 \otimes e_1) + x(e_1 \otimes e_a) + y(e_a \otimes e_1) + z(e_a \otimes e_a)) \\ &= we_1 + xe_a. \end{aligned}$$

y entonces $w = x = 1$. De forma similar, aplicando la parte (ii) de la Proposición 4.1.9 tenemos $y = 1$. Entonces,

$$R' = e_1 \otimes e_1 + e_1 \otimes e_a + e_a \otimes e_1 + z(e_a \otimes e_a)$$

para $z \in K$. Necesitamos hallar todos los valores de z tales que (KT^*, R') es cuasitriangular. Necesariamente, debe valer

$$(\Delta \otimes I)(R') = (R')^{13}(R')^{23}.$$

Ahora,

$$\begin{aligned}
(\Delta \otimes I)(R') =&(\Delta \otimes I)(e_1 \otimes e_1 + e_1 \otimes e_a + e_a \otimes e_1 + z(e_a \otimes e_a))\\
=&(e_1 \otimes e_1) \otimes e_1 + (e_1 \otimes e_1) \otimes e_a + (e_1 \otimes e_a + e_a \otimes e_1 + e_a \otimes e_a) \otimes e_1 +\\
&z((e_1 \otimes e_a + e_a \otimes e_1 + e_a \otimes e_a) \otimes e_a)\\
=&e_1 \otimes e_1 \otimes e_1 + e_1 \otimes e_1 \otimes e_a + e_1 \otimes e_a \otimes e_1 + e_a \otimes e_1 \otimes e_1\\
&+ e_a \otimes e_a \otimes e_1 \otimes e_1 + z(e_1 \otimes e_a \otimes e_a) + z(e_a \otimes e_1 \otimes e_a)\\
&+ z(e_a \otimes e_a \otimes e_a)
\end{aligned} \tag{4.5}$$

Más aún,

$$\begin{aligned}
(R')^{13}(R')^{23} =&(e_1 \otimes (e_1 + e_a) \otimes e_1 + e_1 \otimes (e_1 + e_a) \otimes e_a + e_a \otimes (e_1 + e_a) \otimes e_1\\
&+ z(e_a \otimes (e_a + e_a) \otimes e_a))((e_a + e_a) \otimes e_1 \otimes e_1 + (e_1 + e_a) \otimes e_1 \otimes e_a\\
&+ (e_1 + e_a) \otimes e_a \otimes e_1 + z((e_1 + e_a) \otimes e_a \otimes e_a))\\
=&(e_1 \otimes e_1 \otimes e_1 + e_1 \otimes e_a \otimes e_1 + e_1 \otimes e_1 \otimes e_a + e_1 \otimes e_a \otimes e_a\\
&+ e_a \otimes e_1 \otimes e_1 + e_a \otimes e_a \otimes e_1 + z(e_a \otimes e_1 \otimes e_a)\\
&z(e_a \otimes e_a \otimes e_a))(e_1 \otimes e_1 \otimes e_1 + e_a \otimes e_1 \otimes e_1 + e_1 \otimes e_1 \otimes e_a\\
&e_a \otimes e_a \otimes e_1 + e_1 \otimes e_a \otimes e_1 + e_a \otimes e_a \otimes e_1 + z(e_1 \otimes e_a \otimes e_a)\\
&+ z(e_a \otimes e_a \otimes e_a))\\
=&e_1 \otimes e_1 \otimes e_1 + e_1 \otimes e_a \otimes e_1 + e_1 \otimes e_1 \otimes e_a + z(e_1 \otimes e_a \otimes e_a)\\
&+ e_a \otimes e_1 \otimes e_1 + e_a \otimes e_a \otimes e_1 + z(e_a \otimes e_1 \otimes e_a)\\
&z^2(e_a \otimes e_a \otimes e_a).
\end{aligned} \tag{4.6}$$

Luego, si (KT^*, R') es cuasitriangular, comparando las Ecuaciones (4.5) y (4.6) tenemos

$$\begin{aligned}
&e_1 \otimes e_1 \otimes e_1 + e_1 \otimes e_1 \otimes e_a + e_1 \otimes e_a \otimes e_1 + e_a \otimes e_1 \otimes e_1\\
&+ e_a \otimes e_a \otimes e_1 + z(e_1 \otimes e_a \otimes e_a) + z(e_a \otimes e_1 \otimes e_a)\\
&z(e_a \otimes e_a \otimes e_a)\\
=&e_1 \otimes e_1 \otimes e_1 + e_1 \otimes e_a \otimes e_1 + e_1 \otimes e_1 \otimes e_a + z(e_1 \otimes e_a \otimes e_a)\\
&+ e_a \otimes e_1 \otimes e_1 + e_a \otimes e_a \otimes e_1 + z(e_a \otimes e_1 \otimes e_a)\\
&z^2(e_a \otimes e_a \otimes e_a)
\end{aligned}$$

y entonces $z^2 = z$. Tenemos dos posibilidades: $z = 0$ o bien $z = 1$. Si $z = 0$, entonces R' no es una unidad en $KT^* \otimes KT^*$ pues, por ejemplo, $R'(a \otimes a) = 0$. Luego,

$$R' = e_1 \otimes e_1 + e_1 \otimes e_a + e_a \otimes e_1 + e_a \otimes e_a = 1 \otimes 1$$

es la única estructura cuasitriangular para KT^*. En consecuencia, si (KT, R) es cuasitriangular, entonces

$$(\phi \otimes \phi)(R) = 1 \otimes 1.$$

Se sigue que $R = 1 \otimes 1$ es la única estructura cuasitriangular en KT. □

Sea H una K-álgebra de Hopf y $R = \sum_{i=1}^{n} a_i \otimes b_i \in U(H \otimes H)$.

Definición 4.1.11. El par (H, R) es un *álgebra de Hopf cuasitriangular* si (H, R) es cuasitriangular como K-biálgebra y la antípoda σ_H es una biyección.

Observación. Notemos que si H es una K-álgebra de Hopf de dimensión finita, su antípoda es necesariamente una biyección. Este hecho se deduce del Teorema Fundamental de los módulos de Hopf y de la teoría de integrales de las álgebras de Hopf que no hemos tratado en esta tesis. Para una demostración de este hecho, puede consultarse, por ejemplo [Mon93, Teorema 2.1.3]. Luego, si buscamos álgebras de Hopf que eran cuasitriangulares como biálgebras pero que no tengan antípodas biyectivas, no podemos buscar entre las álgebras de Hopf de dimensión finita.

Una **estructura cuasitriangular** es un elemento $R \in U(H \otimes H)$ tal que (H, R) es cuasitriangular. De la misma forma que antes, decimos que dos álgebras de Hopf cuasitriangulares (H, R) y (H', R') son **isomorfas como álgebras de Hopf cuasitriangulares** si existe un isomorfismo de álgebras de Hopf $\phi \colon H \to H'$ tal que $(\phi \otimes \phi)(R) = R'$. Dos estructuras R y R' sobre una misma álgebra de Hopf son **equivalentes** si $(H, R) \cong (H, R')$.

Nuestro objetivo ahora es calcular todas las estructuras cuasitriangulares del álgebra de Hopf KC_2 del Ejemplo 4.1.5. Necesitamos una proposición.

Proposición 4.1.12. *Supongamos que (H, R) es cuasitriangular. Entonces se cumple que $(\sigma_H \otimes I_H)(R) = R^{-1}$.*

Demostración. Tenemos

$$\begin{aligned}
R(\sigma_H \otimes I_H)(R) &= \left(\sum_{i=1}^{n} a_i \otimes b_i\right) (\sigma_H \otimes I_H) \left(\sum_{j=1}^{n} a_j \otimes b_j\right) \\
&= \left(\sum_{i=1}^{n} a_i \otimes b_i\right) \left(\sum_{j=1}^{n} \sigma_H(a_j) \otimes b_j\right) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i \sigma_H(a_j) \otimes b_i b_j \\
&= (m_H \otimes I_H)(I_H \otimes \sigma_H \otimes I_H) \left(\sum_{i=1}^{n} \sum_{j=1}^{n} a_i \otimes a_j \otimes b_i b_j\right) \\
&= (m_H \otimes I_H)(I_H \otimes \sigma_H \otimes I_H)(R^{13} R^{23}).
\end{aligned}$$

Continuando con el cálculo,

$$
\begin{aligned}
&(m_H \otimes I_H)(I_H \otimes \sigma_H \otimes I_H)(R^{13}R^{23}) \\
&\qquad = (m_H \otimes I_H)(I_H \otimes \sigma_H \otimes I_H)(\Delta_H \otimes I_H)(R) && \text{por (4.2)} \\
&\qquad = \sum_{i=1}^{n} \epsilon_H(a_i)1_H \otimes b_i && \text{por la propiedad de la antípoda} \\
&\qquad = 1_H \otimes 1_H && \text{por la Proposición 4.1.9}(i).
\end{aligned}
$$

Luego, $(\sigma_H \otimes I_H)(R) = R^{-1}$ como queríamos ver. □

Proposición 4.1.13. *Sea KC_2 el álgebra de Hopf del Ejemplo 4.1.5. Existen exactamente dos estructuras cuasitriangulares en KC_2. Son:*

$$R_0 = 1 \otimes 1 \qquad \text{y} \qquad R_1 = \frac{1+g}{2} \otimes 1 + \frac{1-g}{2} \otimes g.$$

Demostración. Obviamente, R_0 es una estructura cuasitriangular para KC_2.

Sea $\{p_1, p_g\}$ la base de KC_2^* dual a la base $\{1, g\}$ de KC_2. El dual KC_2^* es un álgebra de Hopf con comultiplicación dada por

$$\Delta_{KC_2^*}(p_1) = p_1 \otimes p_1 + p_g \otimes p_g, \qquad \Delta_{KC_2^*}(p_g) = p_1 \otimes p_g + p_g \otimes p_1,$$

counidad dada por

$$\epsilon_{KC_2^*}(p_1) = 1 \quad \epsilon_{KC_2^*}(p_g) = 0$$

y antípoda $\sigma_{KC_2^*}(p_x) = p_x$ para $x \in \{1, g\}$.

Notemos que $\phi\colon KC_2 \to KC_2^*$ definida como $\phi(1) = p_1 + p_g$, $\phi(g) = p_1 - p_g$ es un isomorfismo de álgebras de Hopf. Si (KC_2, R) es cuasitriangular, entonces (KC_2^*, R') con $R' = (\phi \otimes \phi)(R)$ es cuasitriangular por la Proposición 4.1.8. Luego, siguienda una idea similar a la de la Proposición 4.1.10, calcularemos primero todas las estructuras cuasitriangulares en KC_2^*. Supongamos entonces que (KC_2^*, R') es cuasitriangular para algún elemento $R' \in U(KC_2^* \otimes KC_2^*)$. Escribimos

$$R' = w(p_1 \otimes p_1) + x(p_1 \otimes p_g) + y(p_g \otimes p_1) + z(p_g \otimes p_g)$$

para $w, x, y, z \in K$. Por la parte (i) de la Proposición 4.1.9, $1 = wp_1 + xp_g$, entonces $w = x = 1$. Por la parte (ii) de la misma proposición, tenemos además $y = 1$. Luego,

$$R' = p_1 \otimes p_1 + p_1 \otimes p_g + p_g \otimes p_1 + z(p_g \otimes p_g),$$

para $z \in K$. Por la Proposición 4.1.12

$$(\sigma_{KC_2^*} \otimes I_{KC_2^*})(R') = R' = (R')^{-1},$$

y entonces $z^2 = 1$. Si $z = 1$ tenemos la etructura R_0 y si $z = -1$, tenemos

$$R' = p_1 \otimes p_1 + p_1 \otimes p_g + p_g \otimes p_1 - 1(p_g \otimes p_g).$$

Como se puede ver, (KC_2^*, R') es cuasitriangular. En consecuencia,

$$\phi^{-1}(R') = R_1 = \frac{1+g}{2} \otimes 1 + \frac{1-g}{2} \otimes g$$

es una estructura cuasitriangular para KC_2. □

Sea H una K-álgebra de Hopf. Hemos visto que si H es coconmutativa, entonces el par $(H, 1\otimes 1)$ es casi coconmutativo. Por la Proposición 3.2.5, la coconmutatividad de H implica que $\sigma_H^2(h) = h$ para todo $h \in H$. Esta propiedad puede generalizarse para pares casi coconmutativos.

Proposición 4.1.14 (Drinfeld, 1990)**.** *Sea (H, R) un par casi coconmutativo con $R = \sum_{i=1}^n a_i \otimes b_i \in U(H \otimes H)$. Sea $u = \sum_{i=1}^n \sigma_H(b_i)a_i$. Entonces $u \in U(H \otimes H)$ y además*

$$\sigma_H^2(h) = uhu^{-1},$$

para todo $h \in H$.

Demostración. Sea $h \in H$. Como (H, R) es casi coconmutativo, la expresión

$$R\Delta_H(h) = \left(\sum_{i=1}^n a_i \otimes b_i\right)\left(\sum_{(h)} h_{(1)} \otimes h_{(2)}\right) = \sum_{(h)}\sum_{i=1}^n a_i h_{(1)} \otimes b_i h_{(2)}$$

es igual a

$$\begin{aligned}\tau\Delta_H(h)R = \tau\left(\sum_{(h)} h_{(1)} \otimes h_{(2)}\right)\left(\sum_{i=1}^n a_i \otimes b_i\right) &= \left(\sum_{(h)} h_{(2)} \otimes h_{(1)}\right)\left(\sum_{i=1}^n a_i \otimes b_i\right)\\ &= \sum_{(h)}\sum_{i=1}^n h_{(2)}a_i \otimes h_{(1)}b_i.\end{aligned}$$

En consecuencia,

$$\sum_{(h)}\sum_{i=1}^n a_i h_{(1)} \otimes b_i h_{(2)} \otimes h_{(3)} = \sum_{(h)}\sum_{i=1}^n h_{(2)}a_i \otimes h_{(1)}b_i \otimes h_{(3)}, \tag{4.7}$$

donde $h_{(3)}$ es tal que

$$(I_H \otimes \Delta_H)\Delta_H(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} \otimes h_{(3)}.$$

De la Ecuación 4.7, obtenemos

$$\sum_{(h)}\sum_{i=1}^n \sigma_H(\sigma_H(h_{(3)}))\sigma_H(b_i h_{(2)})a_i h_{(1)} = \sum_{(h)}\sum_{i=1}^n \sigma_H(\sigma_H(h_{(3)}))\sigma_H(h_{(1)}b_i)h_{(2)}a_i. \tag{4.8}$$

Ahora,

$$\begin{aligned}
&\sum_{(h)}\sum_{i=1}^{n}\sigma_H(\sigma_H(h_{(3)}))\sigma_H(b_ih_{(2)})a_ih_{(1)}\\
&\quad=\sum_{(h)}\sum_{i=1}^{n}\sigma_H(\sigma_H(h_{(3)}))\sigma_H(h_{(2)})\sigma_H(b_i)a_ih_{(1)} \qquad \text{pues } \sigma_H \text{ es antimorfismo}\\
&\quad=\sum_{(h)}\sum_{i=1}^{n}\sigma_H(h_{(2)}\sigma_H(h_{(3)}))\sigma_H(b_i)a_ih_{(1)} \qquad \text{pues } \sigma_H \text{ es antimorfismo}\\
&\quad=\sum_{(h)}\sum_{i=1}^{n}\sigma_H(\epsilon_H(h_{(2)})1_H)\sigma_H(b_i)a_ih_{(1)} \qquad \text{por la propiedad de la antípoda}\\
&\quad=\sum_{i=1}^{n}\sigma_H(b_i)a_ih \qquad \text{por la propiedad de la counidad}\\
&\quad=uh.
\end{aligned}$$

Por otro lado,

$$\begin{aligned}
&\sum_{(h)}\sum_{i=1}^{n}\sigma_H(\sigma_H(h_{(3)}))\sigma_H(h_{(1)}b_i)h_{(2)}a_i\\
&=\sum_{(h)}\sum_{i=1}^{n}\sigma_H(\sigma_H(h_{(3)}))\sigma_H(b_i)\sigma_H(h_{(1)})h_{(2)}a_i, \qquad \text{pues } \sigma_H \text{ es antimorfismo}\\
&=\sum_{(h)}\sum_{i=1}^{n}\sigma_H(\sigma_H(h_{(2)}))\sigma_H(b_i)\epsilon_H(h_{(1)})a_i \qquad \text{por la propiedad de la antípoda}\\
&=\sum_{i=1}^{n}\sigma_H(\sigma_H(h))\sigma_H(b_i)a_i \qquad \text{por la propiedad de la counidad}\\
&=\sigma_H^2(h)u.
\end{aligned}$$

Entonces, la Ecuación (4.8) nos da

$$uh=\sigma_H^2(h)u, \tag{4.9}$$

para todo $h \in H$.

Nos falta ver que u es una unidad en H. Para ello, notemos $R^{-1}=\sum_{j=1}^{m}c_j\otimes d_j$ y sea $v=\sum_{j=1}^{m}\sigma_H^{-1}(d_j)c_j$ (recordemos que σ_H es una biyección).

Ahora,

$$\begin{aligned}
uv &= u\sum_{j=1}^{m}\sigma_H^{-1}(d_j)c_j = \sum_{j=1}^{m}(u\sigma_H^{-1}(d_j))c_j = \sum_{j=1}^{m}(\sigma_H^{2}(\sigma_H^{-1}(d_j))u)c_j \qquad \text{por } (4.9)\\
&= \sum_{j=1}^{m}\sigma_H(d_j)uc_j = \sum_{j=1}^{m}\sigma_H(d_j)\sum_{i=1}^{n}\sigma_H(b_i)a_ic_j\\
&= \sum_{j=1}^{m}\sum_{i=1}^{n}\sigma_H(b_id_j)a_ic_j \qquad \text{pues } \sigma_H \text{ es antimorfismo.}
\end{aligned}$$

Más aún,

$$\begin{aligned}
\sum_{j=1}^{m}\sum_{i=1}^{n}\sigma_H(b_id_j)a_ic_j &= m_H(\sigma_H\otimes I_H)\left(\sum_{i=1}^{n}\sum_{j=1}^{m}b_id_j\otimes a_ic_j\right)\\
&= m_H(\sigma_H\otimes I_H)(1_H\otimes 1_H) \qquad \text{pues } RR^{-1}=1_H\otimes 1_H\\
&= \sigma_H(1_H) = 1_H \qquad \text{por la Proposición 3.2.3}(ii).
\end{aligned}$$

En consecuencia, $uv = 1_H$. Ahora,

$$1_H = uv = \sigma_H^2(v)u$$

por (4.9) y entonces $v = \sigma_H^2(v)$ por la unicidad del inverso. Luego, v es tal que

$$uv = 1_H = vu$$

y se tiene que u es una unidad de H. Podemos reescribir ahora (4.9) como

$$\sigma_H^2(h) = uhu^{-1},$$

para todo $h \in H$ como queríamos. □

4.2. Representaciones del grupo de trenzas

En esta sección vamos a aplicar las propiedades de la sección anterior para mostrar cómo encontrar representaciones $\rho\colon \mathbb{B}_3 \to Gl_{n^3}(K)$ del grupo de trenzas a partir de una K-álgebra de Hopf cuasitriangular de dimensión n. Probaremos que la solución que dimos de la QYBE satisface la relación del grupo de trenzas y eso nos dará la representación buscada. Damos ejemplos específicos de representaciones a partir del ejemplo KC_2 estudiado en la sección previa.

Recordemos el grupo de trenzas sólo para fijar notación. Vamos a centrarnos en el **grupo de trenzas de tres cuerdas** que notaremos por $\mathbb{B}_3$. Pensaremos al grupo presentado mediante dos generadores que notaremos B_1 y B_2 sujetos a la relación $B_1B_2B_1 = B_2B_1B_2$. Sabemos que se trata de un grupo infinito.

Sea (H,R) una K-álgebra de Hopf cuasitriangular de dimensión n y $\{c_1,c_2,\ldots,c_n\}$ una base para H. Entonces, $\{c_i\otimes c_j\otimes c_k\}$ con $1\le i,j,k\le n$ es base para el álgebra producto $H\otimes H\otimes H=H^{\otimes 3}$ de dimensión n^3. Las matrices en $GL_{n^3}(K)$ se coresponden con la colección de transformaciones lineales inversibles $H^{\otimes 3}\to H^{\otimes 3}$. Algunas de las matrices en $GL_{n^3}(K)$ provienen de los elementos $R^{12}=\sum_i a_i\otimes b_i\otimes 1$, $R^{13}=\sum_i a_i\otimes 1\otimes b_i$ y $R^{23}=\sum_i 1\otimes a_i\otimes b_i$ construidos a partir del elemento $R=\sum_i a_i\otimes b_i\in U(H\otimes H)$. Veamos de qué forma. Para cada par $ij=12,13,23$, sea

$$R^{ij}\colon H^{\otimes 3}\to H^{\otimes 3},$$

la transformación definida por multiplicación a izquierda por el elemento R^{ij}. Además, sean μ_{ij} las trasposiciones

$$\begin{aligned}
\mu_{12}\colon H^{\otimes 3}\to H^{\otimes 3},&\quad x\otimes y\otimes z\mapsto y\otimes x\otimes z,\\
\mu_{13}\colon H^{\otimes 3}\to H^{\otimes 3},&\quad x\otimes y\otimes z\mapsto z\otimes y\otimes x,\\
\mu_{23}\colon H^{\otimes 3}\to H^{\otimes 3},&\quad x\otimes y\otimes z\mapsto x\otimes z\otimes y.
\end{aligned}$$

Ahora, definimos $R_{ij}\colon H^{\otimes 3}\to H^{\otimes 3}$ como la composición $R_{ij}=\mu_{ij}R^{ij}$. notemos que, en particular R_{12} y R_{23} son transformaciones lineales inversibles sobre $H^{\otimes 3}$ que se corresponden con matrices en $GL_{n^3}(K)$ tomando coordenadas en la base $\{c_1,c_2,\ldots,c_n\}$.

Proposición 4.2.1. *Sea K un cuerpo y (H,R) una K-álgebra de Hopf cuasitriangular de dimensión n. Entonces las matrices R_{12} y R_{23} en $GL_{n^3}(K)$ satisfacen*

$$R_{12}R_{23}R_{12}=R_{23}R_{12}R_{23}.$$

Demostración. Para $x\otimes y\otimes z\in H^{\otimes 3}$ tenemos

$$\begin{aligned}
(\mu_{13}\mu_{23}R_{23}\mu_{13}\mu_{12})(x\otimes y\otimes z)&=(\mu_{13}\mu_{23}R_{23}\mu_{13})(y\otimes x\otimes z)\\
&=(\mu_{13}\mu_{23}R_{23})(z\otimes x\otimes y)\\
&=(\mu_{13}\mu_{23})\left(\sum_i z\otimes b_iy\otimes a_ix\right)\\
&=\mu_{13}\left(\sum_i z\otimes a_ix\otimes b_iy\right)\\
&=\sum_i b_iy\otimes a_ix\otimes z=R_{12}(x\otimes y\otimes z),
\end{aligned}$$

y entonces

$$\mu_{13}\mu_{23}R_{23}\mu_{13}\mu_{12}=R_{12}. \tag{4.10}$$

Por otro lado,

$$\begin{aligned}
(\mu_{12}R_{13}\mu_{12})(x\otimes y\otimes z)=(\mu_{12}R_{13})(y\otimes x\otimes z)&=\mu_{12}\left(\sum_i b_iz\otimes x\otimes a_iy\right)\\
&=\sum_i x\otimes b_iz\otimes a_iy=R_{23}(x\otimes y\otimes z),
\end{aligned}$$

y entonces
$$\mu_{12}R_{13}\mu_{12} = R_{23}. \tag{4.11}$$
En consecuencia,
$$\begin{aligned} R_{12}R_{23}R_{12} &= (\mu_{13}\mu_{23}R_{23}\mu_{13}\mu_{12})(\mu_{12}R_{13}\mu_{12})R_{12} \qquad \text{por (4.10) y (4.11)} \\ &= \mu_{13}(\mu_{23}R_{23})(\mu_{13}\mu_{12}\mu_{12}R_{13})(\mu_{12}R_{12}) \\ &= \mu_{13}(R^{23}R^{13}R^{12}) \\ &= \mu_{13}(R^{12}R^{13}R^{23}) \qquad \text{por la Proposición 4.1.7.} \end{aligned} \tag{4.12}$$
Pensando ahora en el otro término de la igualdad del enunciado, tenemos
$$\begin{aligned} (\mu_{13}\mu_{12}R_{12}\mu_{13}\mu_{23})(x\otimes y\otimes z) &= (\mu_{13}\mu_{12}R_{12}\mu_{13})(x\otimes z\otimes y) \\ &= (\mu_{13}\mu_{12}R_{12})(y\otimes z\otimes x) \\ &= (\mu_{13}\mu_{12})\left(\sum_i b_i z\otimes a_i y\otimes x\right) \\ &= \mu_{13}\left(\sum_i a_i y\otimes b_i z\otimes x\right) \\ &= \sum_i x\otimes b_i z\otimes a_i y \\ &= R_{23}(x\otimes y\otimes z), \end{aligned}$$
y entonces,
$$\mu_{13}\mu_{12}R_{12}\mu_{13}\mu_{23} = R_{23}. \tag{4.13}$$
Más aún,
$$\begin{aligned} (\mu_{23}R_{13}\mu_{23})(x\otimes y\otimes z) = (\mu_{23}R_{13})(x\otimes z\otimes y) &= \mu_{23}\left(\sum_i b_i y\otimes z\otimes a_i x\right) \\ = \sum_i b_i y\otimes a_i x\otimes z &= R_{12}(x\otimes y\otimes z), \end{aligned}$$
y entonces
$$\mu_{23}R_{13}\mu_{23} = R_{12}. \tag{4.14}$$
En consecuencia, tenemos
$$\begin{aligned} R_{23}R_{12}R_{23} &= (\mu_{13}\mu_{12}R_{12}\mu_{13}\mu_{23})(\mu_{23}R_{13}\mu_{23})R_{23} \qquad \text{por (4.13) y (4.14)} \\ &= \mu_{13}R^{12}R^{13}R^{23} = R_{12}R_{23}R_{12} \qquad \text{por (4.12).} \end{aligned}$$
Que es lo que queríamos probar. □

Vamos a ver ahora cómo construir representaciones de $\mathbb{B}_3$.

Proposición 4.2.2. *Sea (H, R) una K-álgebra de Hopf cuasitriangular de dimensión n. Entonces existe una representación lineal de dimensión n^3 del grupo de trenzas $\mathbb{B}_3$*

$$\rho\colon \mathbb{B}_3 \to GL_{n^3}(K)$$

definida como:

$$\rho(B_1) = R_{12}, \qquad \rho(B_2) = R_{23}, \qquad \rho(B_{-1}) = R_{12}^{-1}, \qquad \rho(B_{-2}) = R_{23}^{-1},$$

y para una trenza cualquiera $B = B_{i_1}B_{i_2}\dots B_{i_k}$ donde $i_1, i_2, \dots, i_k$ una sucesión finita en $\{-2, -1, 1, 2\}$,

$$\rho(B) = \rho(B_{i_1}B_{i_2}\dots B_{i_k}) = \rho(B_{i_1})\rho(B_{i_2})\dots\rho(B_{i_k}).$$

Demostración. Sólo debemos ver que ρ respeta la relación del grupo de trenzas: $B_1B_2B_1 = B_2B_1B_2$. Pero esto es fácil de ver, pues

$$\begin{aligned}\rho(B_1B_2B_1) &= \rho(B_1)\rho(B_2)\rho(B_1) = R_{12}R_{23}R_{12} \\ &= R_{23}R_{12}R_{23} && \text{por la Proposición 4.2.1} \\ &= \rho(B_2)\rho(B_1)\rho(B_2) = \rho(B_2B_1B_2).\end{aligned}$$

□

Ejemplo 4.2.3. Recordemos que por la Proposición 4.1.13, tenemos dos estructuras cuasitriangulares en KC_2: $R_0 = 1\otimes 1$ y $R_1 = \frac{1}{2}(1\otimes 1)+\frac{1}{2}(1\otimes g)+\frac{1}{2}(g\otimes 1)-\frac{1}{2}(g\otimes g)$. Ahora, $(KC_2)^{\otimes 3}$ es un K-espacio vectorial de dimensión 8. Tomemos la base

$$\{1\otimes 1\otimes 1, 1\otimes 1\otimes g, 1\otimes g\otimes 1, 1\otimes g\otimes g, g\otimes 1\otimes 1, g\otimes 1\otimes g, g\otimes g\otimes 1, g\otimes g\otimes g\}$$

para $(KC_2)^{\otimes 3}$. Por la Proposición 4.2.2 tenemos dos representaciones lineales de dimensión 8 para $\mathbb{B}_3$. La primera está dada por el álgebra de Hopf cuasitriangular (KC_2, R_0) y es de la forma

$$\rho_0\colon \mathbb{B}_3 \to GL_8(K),$$

con

$$\rho_0(B_1) = R_{12} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix},$$

y

$$\rho_0(B_2) = R_{23} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix}.$$

La segunda está dada por (KC_2, R_1) y es de la forma

$$\rho_1 \colon \mathbb{B}_3 \to GL_8(K),$$

con

$$\rho_1(B_1) = R_{12} = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix},$$

y

$$\rho_1(B_2) = R_{23} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Como se puede verificar,

$$\rho_0(\mathbb{B}_3) \cong \rho_1(\mathbb{B}_3) \cong S_3.$$

De hecho, considerando la presentación

$$\langle a, b | a^2 = b^2 = 1, aba = bab \rangle$$

de S_3 podemos ver que el morfismo que asigna $R_{12} \mapsto a$, $R_{23} \mapsto b$ es un isomorfismo de grupos en ambos casos.

4.3. Álgebras de Hopf y variedades afines

En esta sección veremos la relación entre las K-álgebras de Hopf y las variedades afines Λ sobre K. Veremos de qué manera podemos identificar el anillo de coordenadas $K[\Lambda]$ con la colección de morfismos de K-álgebras $K[\Lambda] \to K$. Esto nos permitirá pensar en el objeto geométrico Λ desde un punto de vista algebraico. Veremos que si $K[\Lambda]$ es biálgebra, entonces Λ es un monoide y que si $K[\Lambda]$ es álgebra de Hopf, entonces Λ es un grupo.

Sea $n \geq 1$ un entero y K un cuerpo infinito que contiene a $\mathbb{Q}$. Notemos como es usual $K^n = \underbrace{K \times K \times \cdots \times K}_{n}$ el producto cartesiano de n copias de K. Sean $x_1, x_2, \ldots, x_n$ indeterminadas y notemos por $K[x_1, x_2, \ldots, x_n]$ al anillo de polinomios sobre K.

Definición 4.3.1. Una *variedad afín* Λ sobre K es un subconjunto Λ de K^n formado por los ceros comunes $a = (a_1, a_2, \ldots, a_n)$ sobre K de un conjunto finito $F = \{f_1, f_2, \ldots, f_m\}$ de polinomios en $K[x_1, x_2, \ldots, x_n]$, es decir,

$$\Lambda = \{a = (a_1, a_2, \ldots, a_n) \in K^n \colon f(a) = 0, \forall f \in F\}.$$

Observación. La variedad afín $\Lambda \subseteq K^n$ es el conjunto de soluciones simultáneas del conjunto de ecuaciones $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ si y sólo si $g(\Lambda) = 0$ para todo g en el ideal $N = (f_1, f_2, \ldots, f_m)$ generado por $f_1, f_2, \ldots, f_m$.

Ejemplo 4.3.2. $\Lambda = \{0, 1\} \subseteq K^1$ es variedad afín por ser el conjunto de ceros del polinomio $f(x) = x^2 - x \in K[x]$.

Ejemplo 4.3.3. $\Lambda = \{-1, 2\} \subseteq K^1$ es el conjunto de ceros comunes de $\{x^2 - x - 2, x^3 - 4x^2 + x + 6\} \subseteq K[x]$.

Ejemplo 4.3.4. $\Lambda = \{(a, a^{-1}) \colon a \in K^\times\} \subseteq K^2$ es variedad afín por ser el conjunto de ceros del polinomio $f(x_1, x_2) = x_1x_2 - 1 \in K[x_1, x_2]$.

Ejemplo 4.3.5 (Generalización del Ejemplo 4.3.4)**.**

$$\Lambda = \{(a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}, b^{-1}) \colon a_{i,j} \in K, b = a_{1,1}a_{2,2} - a_{1,2}a_{2,1} \in K^\times\} \subseteq K^5$$

es una variedad afín por ser el conjunto de ceros sobre K del polinomio

$$f(x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, y) = (x_{1,1}x_{2,2} - x_{1,2}x_{2,1})y - 1$$

en $K[x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, y]$.

Ejemplo 4.3.6. $\Lambda = K^n$ es variedad afín por ser los ceros de $f(x_1, x_2, \ldots, x_n) = 0$.

Sea $\Lambda \subseteq K^n$ una variedad afín. El conjunto de polinomios

$$N_\Lambda = \{f \in K[x_1, x_2, \ldots, x_n] \colon f(a) = 0, \forall a \in \Lambda\},$$

es un ideal de $K[x_1, x_2, \ldots, x_n]$ que llamamos **ideal de** Λ. Por ejemplo, si Λ es la variedad afín del Ejemplo 4.3.4, entonces $N_\Lambda = (x_1x_2 - 1)$ y si $\Lambda = K^n$, entonces $N_\Lambda = 0$.

Si Λ es la variedad afín que proviene de los ceros comunes del conjunto de polinomios $\{f_1, f_2, \ldots, f_m\}$ en $K[x_1, x_2, \ldots, x_n]$, entonces $(f_1, f_2, \ldots, f_m) \subseteq N_\Lambda$. La inclusión puede ser propia. Por ejemplo, tomemos $K = \mathbb{Q}$; luego, $x^3 - 1$ define la variedad afín $\Lambda = \{1\}$ y se cumple $(x^3 - 1) \subsetneq N_\Lambda = (x - 1)$.

Por el Teorema de la Base de Hilbert, $K[x_1, x_2, \ldots, x_n]$ es un anillo noetheriano. Luego, $N_\Lambda = (g_1, g_2, \ldots, g_l)$ para ciertos polinomios $g_1, g_2, \ldots, g_l \in K[x_1, x_2, \ldots, x_n]$.

Proposición 4.3.7. *Sea $\Lambda \subseteq K^n$ una variedad afín con ideal $N_\Lambda = (g_1, g_2, \ldots, g_l)$. Sea Λ' la variedad afín que se obtiene de todos los ceros comunes en K de la colección de polinomios $\{g_1, g_2, \ldots, g_l\}$. Entonces, $\Lambda = \Lambda'$.*

Demostración. Por la definición de N_Λ, tenemos $\Lambda \subseteq \Lambda'$. Como Λ es una variedad afín, está formada por puntos de K^n que son los ceros comunes de cierto conjunto de polinomios $\{f_1, f_2, \ldots, f_m\} \in K[x_1, x_2, \ldots x_n]$. Tenemos que $(f_1, f_2, \ldots, f_m) \subseteq N_\Lambda$. Sea ahora $b \in \Lambda'$; entonces b es cero común de todos los polinomios de N_Λ. Luego, en particular, b es un cero común de todos los polinomios $\{f_1, f_2, \ldots, f_m\}$ y se tiene $b \in \Lambda$. $\square$

Definición 4.3.8. Sea $\Lambda \subseteq K^n$ una variedad afín. Una función $\phi\colon \Lambda \to K$ se dice *regular* si existe un polinomio $f \in K[x_1, x_2, \ldots, x_n]$ tal que $\phi(a) = f(a)$ para todo $a \in \Lambda$. La colección de todas las funciones regulares sobre Λ es un anillo con las operaciones definidas punto a punto. Se llama *anillo de funciones regulares* $K[\Lambda]$ *sobre* Λ. El anillo $K[\Lambda]$ también se llama el *anillo de coordenadas* de Λ.

Veamos una descripción más precisa de $K[\Lambda]$.

Proposición 4.3.9. *Sea $\Lambda \subseteq K^n$ una variedad afín y sea N_Λ el ideal de Λ. Entonces $K[\Lambda] = K[x_1, x_2, \ldots, x_n]/N_\Lambda$.*

Demostración. Supongamos que $g, h \in K[x_1, x_2, \ldots, x_n]$ con $g - h \in N_\Lambda$. Entonces, para todo $a = (a_1, a_2, \ldots, a_n) \in \Lambda$,

$$0 = (g - h)(a) = g(a) - h(a),$$

y entonces $g(a) = h(a)$. Luego, g y h definen la misma función regular sobre Λ. $\square$

Por ejemplo, si Λ es la variedad afín del Ejemplo 4.3.4, entonces

$$K[\Lambda] = K[x_1, x_2]/(x_1x_2 - 1) = K[x, x^{-1}]$$

y si $\Lambda = K^n$, entonces $K[\Lambda] \cong K[x_1, x_2, \ldots, x_n]$.

En [Wat79, §1.2] se construye una biyección entre Λ y $\mathrm{Hom}_{K-\text{álg}}(K[\Lambda], K)$. Veamos cómo se hace esto. Sea $\mathcal{F}$ una familia de ecuaciones polinomiales sobre K que involucra n variables. Consideramos $K[x_1, x_2, \ldots, x_n]$ el anillo de polinomios con una indeterminada por cada variable involucrada en el sistema. Sea N_Λ el ideal en $K[x_1, x_2, \ldots, x_n]$ como antes. Por la Proposición 4.3.7, podemos suponer que los polinomios de la familia $\mathcal{F}$ son los generadores de N_Λ. Las imágenes de las indeterminadas sobre el anillo cociente $K[\Lambda]$ forman una solución del sistema que satisface formalmente sólo las ecuaciones dadas. Esta solución es la "más general posible" en el sentido que se precisará a continuación.

Supongamos dada una función $\phi \in \mathrm{Hom}_{K-\text{álg}}(K[\Lambda], K)$; la imagen de las indeterminadas por ϕ nos da una solución del sistema, es decir, un elemento de Λ pues las relaciones polinomiales están en el núcleo de ϕ. Como ϕ está determinada por la imagen de las clases de las indeterminadas, tenemos una inyección $\mathrm{Hom}_{K-\text{álg}}(K[\Lambda], K) \hookrightarrow \Lambda$. En realidad, se trata de una biyección y de aquí que se trate de la solución "más general posible". En efecto, dado a un elemento en Λ (es decir, una solución del sistema) consideramos la aplicación $\bar{\phi}\colon K[x_1, x_2, \ldots, x_n] \to K$

que asigna a cada indeterminada las coordenadas de la solución a. Como a es solución, las relaciones que definen N_Λ van a parar a 0 y entonces $\bar{\phi}$ se factoriza por $K[\Lambda]$ dando una $\phi \in \mathrm{Hom}_{K-\text{álg}}(K[\Lambda], K)$.

Para mayor claridad expositiva, dejemos el resultado en la siguiente proposición.

Proposición 4.3.10. *Sea $\Lambda \subseteq K^n$ una variedad afín con anillo de coordenadas $K[\Lambda]$. Entonces*

$$\Lambda = \mathrm{Hom}_{K-\text{álg}}(K[\Lambda], K),$$

mediante la identificación $a = (\phi \mapsto \phi(a))$ para todo $a \in \Lambda, \phi \in K[\Lambda]$.

Es natural pensar en una variedad afín $\Lambda \subseteq K^n$ en términos geométricos como una colección de puntos en el espacio K^n. También podemos pensarla en términos algebraicos aprovechando la estructura del anillo de coordenadas $K[\Lambda]$ usando la identificación de la Proposición 4.3.10.

En lo que resta, veremos cómo podemos darle estructura a la variedad afín estudiando esta relación.

Supongamos que el anillo de coordenadas $B = K[\Lambda]$ tiene estructura de K-biálgebra. Veremos que en este caso obtendremos una estructura de monoide sobre Λ.

Proposición 4.3.11. *Existe una operación binaria Θ en Hom$_{K-\text{álg}}(B, K)$*

$$\Theta\colon \mathrm{Hom}_{K-\text{álg}}(B, K) \times \mathrm{Hom}_{K-\text{álg}}(B, K) \to \mathrm{Hom}_{K-\text{álg}}(B, K)$$

definida como

$$\Theta(f, g)(a) = m_K(f \otimes g)\Delta_B(a) = \sum_{(a)} f(a_{(1)})g(a_{(2)}),$$

para $f, g \in \mathrm{Hom}_{K-\text{álg}}(B, K), a \in B$ y $\Delta_B(a) = \sum_{(a)} a_{(1)} \otimes a_{(2)}$.

Demostración. Debemos ver que la función $\Theta(f, g)\colon B \to K$ es un morfismo de K-álgebras. Para ello, sea $a, b \in B, r \in K$. Entonces,

$$\begin{aligned}
\Theta(f, g)(ra + b) &= m_K(f \otimes g)\Delta_B(ra + b) = m_K(f \otimes g)(r\Delta_B(a) + \Delta_B(b) \\
&= m_K(f \otimes g)\left(\left(\sum_{(a)} ra_{(1)} \otimes a_{(2)}\right) + \left(\sum_{(b)} b_{(1)} \otimes b_{(2)}\right)\right) \\
&= m_K\left(\left(\sum_{(a)} f(ra_{(1)}) \otimes g(a_{(2)})\right) + \left(\sum_{(b)} f(b_{(1)}) \otimes g(b_{(2)})\right)\right) \\
&= \left(\sum_{(a)} rf(a_{(1)})g(a_{(2)})\right) + \left(\sum_{(b)} f(b_{(1)})g(b_{(2)})\right) \\
&= r\Theta(f, g)(a) + \Theta(f, g)(b),
\end{aligned}$$

y entonces $\Theta(f,g)$ es K-lineal. Debemos ver ahora que respeta la multiplicación. Para ello:

$$\begin{aligned}\Theta(f,g)(ab) = m_K(f\otimes g)\Delta_B(ab) &= m_K(f\otimes g)\left(\sum_{(a,b)} a_{(1)}b_{(1)}\otimes a_{(2)}b_{(2)}\right)\\ &= \sum_{(a,b)} f(a_{(1)}b_{(1)})g(a_{(2)}b_{(2)}) = \sum_{(a,b)} f(a_{(1)})f(b_{(1)})g(a_{(2)})g(b_{(2)})\\ &= \sum_{(a,b)} f(a_{(1)})g(a_{(2)})f(b_{(1)})g(b_{(2)}) = \sum_{(a)} f(a_{(1)})g(a_{(2)})\sum_{(b)} f(b_{(1)})g(b_{(2)})\\ &= \Theta(f,g)(a)\Theta(f,g)(b).\end{aligned}$$

Y esto completa la prueba. □

La operación que definimos no es más que la operación de convolución sobre el conjunto $\mathrm{Hom}_K(B,K)$ que vimos en la página 68 restringida al subconjunto $\mathrm{Hom}_{K-\text{álg}}(B,K)\subseteq \mathrm{Hom}_K(B,K)$.

Proposición 4.3.12. *Sea Λ una variedad afín con anillo de coordenadas $K[\Lambda]$. Si $K[\Lambda]$ es una K-biálgebra, entonces $\Lambda =$Hom$_{K-\text{álg}}(B,K)$ con la convolución $*$ es un monoide.*

Demostración. Es igual a la Proposición 3.2.1. □

Supongamos ahora que el anillo de coordenadas $K[\Lambda]$ es una K-álgebra de Hopf H.

Proposición 4.3.13. *Hom$_{K-\text{álg}}(H,K)$ es un grupo con la operación $*$.*

Demostración. Por la Proposición 4.3.12, $\mathrm{Hom}_{K-\text{álg}}(H,K)$ con la convolución $*$ es un monoide con unidad $\lambda_K\epsilon_H$. Sólo debemos ver que cada $f\in \mathrm{Hom}_{K-\text{álg}}(H,K)$ tiene un inverso bajo $*$. Notemos que $f\sigma_H\in \mathrm{Hom}_{K-\text{álg}}(H,K)$. Ahora, para todo $a\in H$,

$$(f\sigma_H * f)(a) = \sum_{(a)} f(\sigma_H(a_{(1)}))f(a_{(2)}) = f\left(\sum_{(a)}\sigma_H(a_{(1)})a_{(2)}\right),$$

pues f es morfismo de álgebras. Continuando, tenemos

$$\begin{aligned}f\left(\sum_{(a)}\sigma_H(a_{(1)})a_{(2)}\right) &= f(\epsilon_H(a)1_H) \qquad \text{por la propiedad de la antípoda}\\ &= \epsilon_H(a)1_K = \lambda_K(\epsilon_H(a)) = (\lambda_K\epsilon_H)(a).\end{aligned}$$

De forma totalmente análoga, tenemos $f*f\sigma_H = \lambda_K\epsilon_H$ y esto concluye la prueba. □

La conclusión de la Proposición 4.3.13 es la siguiente: si una K-álgebra de Hopf H es el anillo de coordenadas de cierta variedad afín $\Lambda \subseteq K^n$ (necesariamente, H es conmutativa), entonces $\Lambda = \mathrm{Hom}_{K-\text{álg}}(H, K)$ es un grupo. Esto nos permite darle estructura de grupo a un objeto geométrico. Veamos los siguientes ejemplos.

Ejemplo 4.3.14. El anillo de polinomios $K[x]$ es una K-álgebra de Hopf con x un elemento primitivo. Se puede ver que es el anillo de coordenadas de la variedad afín K^1. En este caso para todo $a, b \in K^1$ tenemos $(a * b)(x) = a(x)b(1) + a(1)b(x) = a(x) + b(x) = (a + b)(x)$. Luego, $a * b = a + b$. Es el **grupo aditivo** de K.

Ejemplo 4.3.15. $K[x, x^{-1}]$ con x elemento de tipo grupo es una K-álgebra de Hopf y es el anillo de coordenadas de la variedad afín $\Lambda = \{(a, a^{-1}) \colon a \in K^\times\}$. En este caso, $a * b = ab$ pues $a * b(x) = a(x)b(x) = ab(x)$. Se trata entonces del **grupo multiplicativo** de los elementos no nulos de K.

Ejemplo 4.3.16. Consideramos Λ la variedad afín del Ejemplo 4.3.5. Su anillo de coordenadas es $K[x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, y]/((x_{1,1}x_{2,2} - x_{1,2}x_{2,1})y - 1)$. Un elemento $a \in \Lambda$ se puede ver como una matriz inversible

$$M = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}.$$

La convolución es el producto usual de matrices y $(\Lambda, *)$ es el grupo de matrices $GL_2(K)$.

Bibliografía

[CG93] William Chin and Jerry Goldman. Bialgebras of linearly recursive sequences. *Comm. Algebra*, 21(11):3935–3952, 1993.

[Kas95] Christian Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Mon93] Susan Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993.

[NU11] Warren D. Nichols and Robert G. Underwood. Algebraic Myhill–Nerode theorems. *Theoretical Computer Science*, 412(4):448–457, 2011.

[Rad93] David E Radford. Minimal quasitriangular Hopf algebras. *Journal of Algebra*, 157(2):285–315, 1993.

[Swe69] Moss E. Sweedler. *Hopf algebras*. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York, 1969.

[Und15] Robert G. Underwood. *Fundamentals of Hopf algebras*. Universitext. Springer, Cham, 2015.

[Wat79] William C Waterhouse. Introduction to Affine group schemes. In *Introduction to Affine Group Schemes*. Springer, 1979.

[ZM73] Neal Zierler and WH Mills. Products of linear recurring sequences. *Journal of Algebra*, 27(1):147–157, 1973.