MARGARITA MATHEMATICA EN MEMORIA DE
JOSÉ JAVIER (CHICHO) GUADALUPE HERNÁNDEZ
(Luis Español y Juan L. Varona, editores),
Servicio de Publicaciones, Universidad de La Rioja,
Logroño, Spain, 2001.

# ITERACIÓN DE LA COMPOSICIÓN DE SERIES FORMALES

LUIS M. NAVAS

ABSTRACT. This paper is a unified survey of the problem of finding compositional roots of formal power series, that is, finding power series whose $n$-fold iteration is a given series. We have set ourselves a twofold purpose: on the one hand, we collect various results dispersed throughout the literature, such as the theory of Schröder functions and continuous iteration of power series, and on the other, we generalize many of these results from the complex numbers to an arbitrary commutative ring, when possible, or to an integral domain or a field when this is more natural. In doing so we give new proofs using the method of successive $z$-adic approximations, which are valid in the general case. We also treat the case of power series with coefficients in a field of nonzero characteristic and torsion linear term. The paper is intended to serve as a convenient reference for all these results.

Es un honor poder participar en el homenaje que la Universidad de La Rioja ofrece con este libro al profesor Guadalupe Hernández, cuyo recuerdo sigue vivo en cuantos le conocieron. Tuve la suerte de ser invitado por él a dar dos conferencias en la Universidad de La Rioja y comprobar personalmente lo que me habían dicho: su cordialidad, su amabilidad, su exigencia académica y su eficacia organizadora. Sea este artículo mi testimonio de gratitud por un lado, y de admiración profesional por otro.

## 1. INTRODUCCIÓN

Nuestra intención al escribir este artículo es dar una visión unificada de varios problemas relacionados con la composición en anillos de series formales. El primer problema es el de la existencia y extracción de raíces «composicionales». Dada una serie formal $f$ y un entero positivo $n$, cuándo se puede asegurar la existencia de una serie $g$ tal que $g^{\circ n} = g \circ g \circ \cdots_{(n \text{ veces})} \circ g = f$? De esta pregunta derivan lógicamente otras, como cuántas raíces hay y cómo se construyen a partir de $f$.

Una solución elegante de este problema es mediante la extensión de la operación de potencia composicional (iteración) desde los enteros positivos a exponentes más generales. Por ejemplo, si se puede definir la exponenciación composicional $g = f^{\circ 1/2}$, ésta debe ser una raíz cuadrada composicional de $f$, es decir, $g \circ g = f$. En el caso de un anillo de series formales sobre un cuerpo, para un determinado tipo de serie se puede definir una iteración «continua» con exponentes en el cuerpo.

Otra manera de resolver los problemas de raíces composicionales es mediante la determinación de clases de representantes sencillas para las clases de conjugación de

2000 *Mathematics Subject Classification.* 13F25, 13J05, 26A18.
*Key words and phrases.* Formal power series, composition, iteration.

las series formales bajo la acción del grupo de series invertibles. Esta conjugación es la denominada conjugación topológica en sistemas dinámicos, y que aquí especificamos como conjugación topológica formal. Por ejemplo, si denotamos la serie identidad por $\imath$ y $f$ es una serie conjugada a $-\imath$, es decir, $f = \lambda^{-1} \circ (-\imath) \circ \lambda$, entonces $f \circ f = \lambda^{-1} \circ (-\imath) \circ (-\imath) \circ \lambda = \lambda^{-1} \circ \imath \circ \lambda = \imath$, dando así una raíz cuadrada composicional de la identidad.

El método de las clases de conjugación es el adoptado por ejemplo en [10], [9], y [7]. Nosotros utilizaremos el método de aproximaciones sucesivas, que proporciona además algoritmos computacionales directos para el cálculo de iteraciones.

Una serie $f$, «genérica» en un sentido que especificaremos, es conjugada a su parte lineal, y la función, debidamente normalizada, que realiza la conjugación, se denomina *función de Schröder* de $f$. Esta parte de la teoría es la más sencilla, por corresponder, en el caso de un cuerpo, a la ausencia de torsión en el término lineal, un hecho que se refleja en el estudio de sistemas dinámicos sobre los números complejos, en la clasificación de los puntos periódicos ([1], cap. 6).

En este trabajo, además de presentar resultados dispersos en la literatura, con el fin de proporcionar una referencia unificada, extendemos varios resultados de los complejos $\mathbb{C}$ a un anillo conmutativo en general cuando sea posible, y en otros casos, en interés de simplificar la exposición, a un anillo íntegro o a un cuerpo. Obtenemos resultados para cuerpos de característica arbitraria en § 6.

## 2. Preliminares

Sea $R$ un anillo conmutativo, y consideremos el anillo de series formales $R[[z]]$ sobre $R$. Denotaremos por $\mathfrak{m} = \mathfrak{m}(R)$ al ideal $(z)$, por $\mathfrak{m}^* = \mathfrak{m}^*(R)$ al grupo de series invertibles respecto a la composición, (aquellas series $f = \sum_{n=1}^{\infty} a_n z^n \in \mathfrak{m}$ con $a_1 \in R^*$) y por $\imath$ a la serie identidad. Damos a $R[[z]]$ la topología generada por este ideal, denominada $z$-ádica. Es equivalente a la topología producto en el espacio de sucesiones $R^{\mathbb{N}}$, con la topología discreta en $R$.

Para $a \in R$, sea $[a] = az$, y $[R] = \{[a] : a \in \mathbb{R}\}$. Entonces $([R], +, 0, \circ, \imath)$ es un anillo, y la aplicación $a \to [a]$ es un isomorfismo de anillos $R \to [R]$. $[R]$ es un submonoide de $(\mathfrak{m}, \circ, \imath)$. La estructura $(\mathfrak{m}, +, 0, \circ, \imath)$ no es un anillo, pues se cumple la ley distributiva $(f + g) \circ h = f \circ h + g \circ h$, pero no $f \circ (g + h) \neq f \circ g + f \circ h$. Esta propiedad es la única que falta para que $(\mathfrak{m}, +, 0, \circ, \imath)$ sea un anillo.

Denotamos por $D$ a la derivada formal. La aplicación $\delta f = Df(0) : \mathfrak{m} \to R$ es un epimorfismo de monoides entre $(\mathfrak{m}, \circ, \imath)$ y $(R, +, 0)$. Obviamente sobre $[R]$ es el isomorfismo inverso de $a \to [a]$. Llamamos *morfismo de linealización* a la composición

$$Lf = [Df(0)] : \mathfrak{m} \to [R]$$

ya que extrae de $f = \sum_{n=1}^{\infty} a_n z^n \in \mathfrak{m}$ su término lineal $a_1 z = [a_1]$. Es un endomorfismo del monoide $(\mathfrak{m}, \circ, \imath)$ que además es morfismo de los grupos aditivos. Se deduce que $L : \mathfrak{m}^* \to [R^*]$ es un morfismo de grupos, en particular $Lf^{-1} = (Lf)^{-1}$.

Como la imagen de $L$ es $[R]$, que es un anillo conmutativo bajo $+, \circ$, las relaciones $L(f+g) = Lf+Lg$ y $L(f\circ g) = Lf\circ Lg$, $L\imath = \imath$ implican que $L(f\circ g) = Lf\circ Lg = Lg\circ Lf = L(g\circ f)$ y $L(f\circ(g+h)) = Lf\circ L(g+h) = Lf\circ(Lg+Lh) = Lf\circ Lg+Lf\circ Lh$. Por tanto, aunque no sea $(\mathfrak{m}, +, 0, \circ, \imath)$ ni anillo ni conmutativo, $L$ tiene las propiedades de un morfismo de anillos conmutativos. Lo mismo se puede decir de $\delta : \mathfrak{m} \to R$, $\delta f = Df(0)$.

El conjunto $\imath + \mathfrak{m}^2 = \{f : f \equiv \imath \operatorname{mód} \mathfrak{m}^2\} = \{f : Lf = \imath\}$ es un subgrupo de $\mathfrak{m}^*$, normal al ser el núcleo de $L : \mathfrak{m}^* \to [R^*]$ y de $\delta : \mathfrak{m}^* \to R^*$. Se tiene la descomposición en producto directo

$$\mathfrak{m}^* = [R^*] \circ (\imath + \mathfrak{m}^2) = (\imath + \mathfrak{m}^2) \circ [R^*]$$

que corresponde a la normalización del término lineal: si $f \in \mathfrak{m}^*$, con $\delta f = a \in R^*$, entonces $L([a]^{-1} \circ f) = L(f \circ [a]^{-1}) = \imath$.

**Definición 2.1.** Dado $a \in R$, es útil considerar el conjunto

$$C_a = \{\lambda \in \mathfrak{m} : \lambda \circ [a] = [a] \circ \lambda\}, \qquad C_a^* = C_a \cap \mathfrak{m}^*,$$

de series que conmutan con $[a]$, es decir, tales que $\lambda(az) = a\lambda(z)$. Obviamente $[R] \subseteq C_a$ al ser $R$ conmutativo, y $C_0 = C_1 = \mathfrak{m}$. En general, $C_a$ caracteriza a los conjugados de $[a]$ : $\lambda^{-1} \circ [a] \circ \lambda = \mu^{-1} \circ [a] \circ \mu \iff \exists\, \gamma \in C_a : \mu = \gamma \circ \lambda$.

**Lema 2.1.** *Sea $R$ un anillo íntegro. Entonces*

$$C_a = \begin{cases} [R] & \text{si } a \text{ no es raíz de la unidad,} \\ zR[[z^m]] & \text{si } a \text{ es una raíz primitiva } m\text{-ésima de la unidad.} \end{cases}$$

*Sea $K$ el cuerpo de fracciones de $R$ y $m$ el orden de $a$ en el grupo multiplicativo $K^*$. El primer caso se puede considerar como un caso particular del segundo, poniendo $m = \infty$, ya que $z$-ádicamente se tiene $R[[z^\infty]] = R[[0]] = R$.*

*Demostración.* Sea $\lambda = \sum_{n=1}^\infty a_n z^n$. Entonces $\lambda \in C_a \iff \lambda(az) - a\lambda(z) = \sum_{n=1}^\infty (a_n a^n - a_n a)\, z^n = 0 \iff a_n(a^n - a) = 0 \quad \forall n \geq 2$ (para $n = 1$ es automático). Si $a$ no es raíz de la unidad, entonces $a^n \neq a$ para todo $n \geq 2$, y las condiciones se cumplen si y solo si $a_n = 0$ $\forall n \geq 2$, es decir, $\lambda = [a_1]$.

Si $a$ es una raíz primitiva $m$-ésima de la unidad, entonces $a^n = a \iff a^{n-1} = 1 \iff n \equiv 1 \operatorname{mód} m$, luego las condiciones son equivalentes a $a_n = 0$ $\forall n \not\equiv 1 \operatorname{mód} m \iff \lambda = \sum_{n \equiv 1 \operatorname{mód} m} a_n z^n \iff \lambda \in zR[[z^m]]$. □

*Ejemplo* 2.1. Si $a = -1$ y $\operatorname{car} R \neq 2$, entonces $m = 2$ y $C_{-1} = zR[[z^2]]$, las series pares.

*Nota* 2.1. Las condiciones $a_n(a^n - a) = 0, n \geq 2 \iff \lambda \in C_a$ son válidas en cualquier anillo. En general, si $e$ es idempotente, $e^2 = e$, entonces $C_e = \mathfrak{m}$. Si $R^0$ denota a los divisores de 0 en $R$, entonces $a, 1 - a^m \notin R^0$ $\forall m \geq 1 \implies C_a = [R]$.

**Lema 2.2.**

$$f \equiv g \operatorname{mód} z^m \implies f^n \equiv g^n \operatorname{mód} z^{m+n-1}, \quad f, g \in \mathfrak{m},\ m \geq 1.$$

*Demostración.* Basta observar lo siguiente:

$$f^n - g^n = (f - g)(f^{n-1} + f^{n-2}g + \cdots + fg^{n-2} + g^{n-1}) = O(z^m)\, O(z^{n-1}).$$

□

**Corolario 2.3.** $f \equiv az \operatorname{mód} z^2 \implies f^n \equiv a^n z^n \operatorname{mód} z^{n+1}$ *para* $n \geq 0$.

**Lema 2.4** (Desarrollos de Taylor). *Sea $f \in R[[z]]$. Si $\mathbb{Z} \subseteq R^*$, entonces en $R[[z,w]]$ se tiene*

$$f(z+w) = f(z) + Df(z)\,w + \frac{D^2 f(z)}{2!}\,w^2 + \cdots = \sum_{n=0}^{\infty} \frac{D^n f(z)}{n!}\,w^n.$$

*Demostración.* Para potencias $f(z) = z^p$ es simplemente el desarrollo del binomio, ya que $D^n z^p = n!\binom{p}{n} z^{p-n}$ para $n \leq p$ y $D^n z^p = 0$ para $n > p$. Entonces $\sum_{n=0}^{\infty} \frac{D^n z^p}{n!}\,w^n = \sum_{n=0}^{p} \binom{p}{n} z^{p-n}\,w^n = (z+w)^p$. Por linealidad la fórmula es válida para polinomios, y por continuidad $z, w$-ádica para cualquier serie. □

*Nota* 2.2. La fórmula truncada lineal $f(z+w) = f(z) + Df(z)\,w + O(w^2)$ es válida en cualquier anillo. En general si $1, 2, \ldots, p-1 \in R^*$, es válida hasta orden $p$.

**Corolario 2.5.**

$$f \circ (g+h) = \sum_{n=0}^{\infty} \frac{(D^n f) \circ g}{n!}\,h^n = (f \circ g) + (Df \circ g)\,h + O(h^2), \qquad g, h, \in \mathfrak{m}$$

*(la aproximación lineal es válida en cualquier anillo).*

**Lema 2.6.** *Para $m \geq 2$,*

$$f = a_1 z + a_m z^m + O(z^{m+1}) \implies f^n = a_1^n z^n + n a_1^{n-1} a_m z^{n+m-1} + O(z^{n+m}).$$

*Demostración.* Por el Lema 2.2, $f^n = (a_1 z + a_m z^m)^n + O(z^{m+1+n-1})$. Desarrollando el binomio, queda $\sum_{l=0}^{n} \binom{n}{l} (a_1 z)^{n-l} (a_m z^m)^l + O(z^{n+m})$, y separando los términos de grado $l = 0, 1$, queda $a_1^n z^n + n a_1^{n-1} a_m z^{n+m-1} + O(z^{n+2(m-1)}) + O(z^{n+m}) = a_1^n z^n + n a_1^{n-1} a_m z^{n+m-1} + O(z^{n+m})$. □

**Lema 2.7** (Fórmula de Composición Iterada). *Si $f = \varphi + b z^{m+1} + O(z^{m+2})$, con $m \geq 1$, y $f = \varphi = az + O(z^2)$, entonces para todo $n \geq 1$,*

$$f^{\circ n} = \varphi^{\circ n} + a^{n-1} b\,(1 + a^m + a^{2m} + \cdots + a^{(n-1)m})\,z^{m+1} + O(z^{m+2}).$$

*Demostración.* Por inducción en $n$. El caso $n = 1$ es trivial. Suponiendo cierta la fórmula para $n$, y usando la aproximación lineal de Taylor, se tiene

$$\begin{aligned}
f^{\circ(n+1)} = f^{\circ n} \circ f &= \varphi^{\circ n} \circ f + a^{n-1} b\,(1 + a^m + \cdots + a^{(n-1)m})\,f^{m+1} + O(f^{m+2}) \\
&= \varphi^{\circ n}(\varphi + b z^{m+1} + O(z^{m+2})) \\
&\quad + a^{n-1} b\,(1 + a^m + \cdots + a^{(n-1)m})\,(a^{m+1} z^{m+1} + O(z^{m+2})) \\
&\quad + O(z^{m+2}) \\
&= \varphi^{\circ n}(\varphi) + (D\varphi^{\circ n})(\varphi) \cdot (b z^{m+1} + O(z^{m+2})) + O(z^{2m+2}) \\
&\quad + a^{m+n} b\,(1 + a^m + \cdots + a^{(n-1)m})\,z^{m+1} + O(z^{m+2}) \\
&= \varphi^{\circ(n+1)} + (D\varphi^{\circ n})(\varphi) \cdot b z^{m+1} \\
&\quad + a^n b\,(a^m + a^{2m} + \cdots + a^{nm})\,z^{m+1} + O(z^{m+2})
\end{aligned}$$

y ahora

$$\varphi = az + O(z^2) \implies \varphi^{\circ n} = a^n z + O(z^2)$$

$$\begin{aligned}&\Longrightarrow D\varphi^{\circ n} = a^n + O(z)\\ &\Longrightarrow D\varphi^{\circ n}(\varphi) = a^n + O(\varphi) = a^n + O(z)\end{aligned}$$

de modo que

$$\begin{aligned}f^{\circ(n+1)} &= \varphi^{\circ(n+1)} + a^n b z^{m+1} + a^n b\left(a^m + a^{2m} + \cdots + a^{nm}\right) z^{m+1} + O(z^{m+2})\\ &= \varphi^{\circ(n+1)} + a^n b\left(1 + a^m + a^{2m} + \cdots + a^{nm}\right) z^{m+1} + O(z^{m+2})\end{aligned}$$

lo cual demuestra la fórmula para $n+1$. □

*Nota* 2.3. El lema es válido para cualquier anillo, ya que sólo usamos el desarrollo de Taylor lineal. Esta fórmula generaliza el Teorema 2.6.4 de [1].

**Corolario 2.8.** *Si* $f = \varphi + bz^{m+1} + O(z^{m+2}), f \equiv \varphi \equiv z$ mód $z^2$, *entonces* $f^{\circ n} = \varphi^{\circ n} + nbz^{m+1} + O(z^{m+2}),\ m \geq 1$.

## 3. Término lineal libre de torsión: Teoría de Schröder

**Teorema 3.1.** *Sea* $\alpha \in \mathfrak{m}^*, a \in R^*$ *con* $\alpha \equiv [a]$ mód $\mathfrak{m}^2$. *Si* $1 - a^m \in R^*$ *para todo* $m \geq 1$, *existe una única* $\lambda \equiv \imath$ mód $\mathfrak{m}^2$, *tal que* $\alpha = \lambda^{-1} \circ [a] \circ \lambda$.

*Demostración.* Empezamos con la unicidad. Si $\lambda, \mu \in \mathfrak{m}$, y $a, 1-a^m \in R^*$ para todo $m \geq 1$, entonces $\lambda^{-1}\circ[a]\circ\lambda = \mu^{-1}\circ[a]\circ\mu \iff \mu\circ\lambda^{-1} \in C_a = [R]$ (Lema 2.1) $\iff \exists c \in R : \mu = [c] \circ \lambda = c\lambda$, luego cuando normalizamos poniendo $\lambda \equiv \mu \equiv z$ mód $z^2$, obtenemos $c = 1$, por tanto $\mu = \lambda$.

La normalización es siempre posible, pues dado cualquier $\lambda \in \mathfrak{m}^*$ tal que $\alpha = \lambda^{-1}\circ[a]\circ\lambda$, para todo $c \in R^*$ tenemos $([c]\circ\lambda)^{-1}\circ[a]\circ([c]\circ\lambda) = \lambda^{-1}\circ[c]^{-1}\circ[a]\circ[c]\circ\lambda = \lambda^{-1}\circ[a]\circ\lambda = \alpha$ de modo que eligiendo $c = a^{-1}$ normaliza $\lambda$ y preserva la conjugación. Esto funciona porque al ser $R$ conmutativo, $[R] \subseteq C_a$.

Construimos $\lambda$ mediante aproximaciones sucesivas $\lambda_m = \sum_{n=1}^m \ell_n z^n$ tales que $\lambda_m \circ \alpha \equiv a\lambda_m$ mód $z^{m+1}$. Para $m = 1$ esto se reduce a la igualdad de los términos lineales: $\lambda_1 = \imath$ y $L(\lambda_1 \circ \alpha) = L\alpha = [a], L(a\lambda_1) = L([a]) = [a]$. Supongamos que hemos construido $\ell_1, \ldots, \ell_m$ tales que $\lambda_m \circ \alpha \equiv a\lambda_m$ mód $z^{m+1}$. Buscamos $\ell = \ell_{m+1}$ tal que $\lambda_{m+1} = \lambda_m + \ell z^{m+1}$ satisfaga $\lambda_{m+1} \circ \alpha \equiv a\lambda_{m+1}$ mód $z^{m+2}$. Sean $\mu, \tilde{\alpha} \in R[[z]]$ definidas por $\alpha = z\tilde{\alpha}$ y $\lambda_m \circ \alpha - a\lambda_m = z^{m+1}\mu$. Observar que $\tilde{\alpha}(0) = a$. Entonces

$$\begin{aligned}&\lambda_{m+1} \circ \alpha \equiv a\lambda_{m+1} \text{ mód } z^{m+2}\\ \iff &(\lambda_m + \ell z^{m+1}) \circ \alpha \equiv a\lambda_m + a\ell z^{m+1} \text{ mód } z^{m+2}\\ \iff &\lambda_m \circ \alpha + \ell\alpha^{m+1} \equiv a\lambda_m + a\ell z^{m+1} \text{ mód } z^{m+2}\\ \iff &\lambda_m \circ \alpha - a\lambda_m \equiv a\ell z^{m+1} - \ell\alpha^{m+1} \text{ mód } z^{m+2}\\ \iff &z^{m+1}\mu \equiv a\ell z^{m+1} - \ell z^{m+1}\tilde{\alpha}^{m+1} \text{ mód } z^{m+2}\\ \iff &\mu \equiv a\ell - \ell\tilde{\alpha}^{m+1} \text{ mód } z\\ \iff &\mu(0) = a\ell - \ell\tilde{\alpha}(0)^{m+1}\\ \iff &\mu(0) = a\ell - \ell a^{m+1}\\ \iff &\ell(a - a^{m+1}) = \mu(0)\end{aligned}$$

y como $a - a^{m+1} \in R^*$ para todo $m$, podemos resolver esta ecuación, quedando $\ell = \ell_{m+1} = (a - a^{m+1})^{-1}\,\mu(0)$. $\square$

El teorema dice que $\alpha$ es conjugada a su linealización $L\alpha$. Como sistemas dinámicos en la topología formal, $\alpha$ y $L\alpha$ son topológicamente conjugados. Escribiremos $\alpha \sim \beta$ si $\alpha, \beta$ son conjugados por un elemento $\lambda \in \mathfrak{m}^*$.

**Definición 3.1.** La función normalizada $\lambda$ que realiza la conjugación se llama *función de Schröder* de $\alpha$.

La «ecuación de Schröder» $\lambda(\alpha(z)) = a\lambda(z)$ fue introducida por E. Schröder en *Math. Annalen* **3** (1871), en el contexto del desarrollo asintótico del término general $x_n$ de una sucesión de iteraciones $x_{n+1} = f(x_n)$ de un punto $x_0$ por una función analítica $f$, en el caso de ser $|f'(0)| < 1$. El Teorema del Punto Fijo de Banach implica que $\lim_n x_n$ es un punto fijo atractor de $f$. Ver [3], cap. 8. Para los aspectos de eficiencia computacional, ver [4], p. 512–513 y [2]. El Teorema 3.1 es una generalización de la Proposición 4 de [9].

Obsérvese además que $Lf$ es la única serie lineal que puede ser conjugada a $f$, ya que $f = \lambda^{-1} \circ [a] \circ \lambda \implies Lf = L\lambda^{-1} \circ L[a] \circ L\lambda = (L\lambda)^{-1} \circ [a] \circ L\lambda = [a]$.

**Corolario 3.2.** *Si $R = K$ es un cuerpo, entonces $f \sim Lf$ si $\delta f \in K^*$ no es una raíz de la unidad, es decir, $\delta f \notin \operatorname{Tor} K^*$ (torsión multiplicativa).*

*Demostración.* Sea $a = \delta f$. Se tiene $a^m \neq 1$ para todo $m \geq 1$; por tanto $a, 1 - a^m \in K^*$. $\square$

**Corolario 3.3.** *Si $R$ es íntegro, con cuerpo de fracciones $K$, entonces $f \sim Lf$ en $K[[z]]$ si $\delta f \neq 0$ no es una raíz de la unidad.*

*Nota* 3.1. La función de Schröder existe, pero en $K[[z]]$, no necesariamente en $R[[z]]$. Por ejemplo, considerar el anillo de enteros $p$-ádicos $R = \mathbb{Z}_p$ y $a = q$ donde $q$ es un primo que satisface $q \equiv 1 \bmod p$. Ciertamente $q \in R^*$, $q$ no es una raíz de la unidad, pero ningún $1 - q^m$ es una unidad en $R$; por tanto estos términos introducen denominadores en la función de Schröder.

**Teorema 3.4** (Raíces composicionales I)**.** *Sea $\alpha \in \mathfrak{m}^*$ con $\alpha \equiv [a] \bmod \mathfrak{m}^2$, de modo que $a \in R^*$. Suponer que $1 - a^m \in R^*$ para todo $m \geq 1$. Para todo $p \geq 1$, hay una correspondencia biunívoca entre los $b \in R^*$ tales que $b^p = a$, y los $\beta \in \mathfrak{m}^*$ tales que $\beta^{\circ p} = \alpha$, dada por $\delta\beta = b$.*

*Demostración.* Sea $\lambda$ la función de Schröder de $\alpha$, o sea, $\alpha = \lambda^{-1} \circ [a] \circ \lambda$. Suponer que $\beta^{\circ p} = \alpha$, con $\delta\beta = b$. Como $\delta$ es un morfismo de monoides, $b^p = a$. Entonces $b \in R^*$ y como $1 - a^m = 1 - b^{pm} = (1 - b^m)(1 + b^m + \cdots + b^{(p-1)m}) \in R^*$, se tiene $1 - b^m \in R^*$ para todo $m \geq 1$; por tanto $\beta$ es conjugada a $L\beta = [b]$. Sea $\mu$ la función de Schröder de $\beta$, de modo que $\beta = \mu^{-1} \circ [b] \circ \mu$. Entonces $\alpha = \beta^{\circ p} = (\mu^{-1} \circ [b] \circ \mu)^{\circ p} = \mu^{-1} \circ [b]^{\circ p} \circ \mu = \mu^{-1} \circ [b^p] \circ \mu = \mu^{-1} \circ [a] \circ \mu$. Por unicidad de la función de Schröder, $\mu = \lambda$. Por tanto toda solución de $\beta^{\circ p} = \alpha$ debe ser de la forma $\beta = \lambda^{-1} \circ [b] \circ \lambda$, donde $b = \delta\beta$ satisface $b^p = a$. Recíprocamente, dada una tal $b$, $\beta = \lambda^{-1} \circ [b] \circ \lambda$ es una solución de $\beta^{\circ p} = \alpha$. Esto demuestra que $b \to \lambda^{-1} \circ [b] \circ \lambda$

es una correspondencia biunívoca entre las soluciones de $b^p = a$ y de $\beta^{\circ p} = \alpha$. La correspondencia inversa es $\beta \to \delta\beta$. □

Diremos que la serie $\beta$ *levanta* $b$ si $\delta\beta = b$, y que $\beta$ está *por encima* de $b$. Hemos demostrado que toda solución $b \in R^*$ de $b^p = a$ levanta de manera única a una solución de $\beta^{\circ p} = \alpha$, y todas las soluciones de $\beta^{\circ p} = \alpha$ se obtienen así.

**Corolario 3.5.** *Sea $K$ un cuerpo y $\alpha \in \mathfrak{m}^*(K)$ tal que $\delta\alpha = D\alpha(0)$ no es una raíz de la unidad. Entonces dado $p \geq 1$, para cada $b \in K^*$ tal que $b^p = a$, hay una única $\beta \in \mathfrak{m}^*$ tal que $\delta\beta = b$ y $\beta^{\circ p} = \alpha$, y todas las soluciones de $\beta^{\circ p} = \alpha$ se obtienen de esta manera. En particular, hay a lo sumo $p$ soluciones.*

**Corolario 3.6.** *Sea $K$ un cuerpo algebraicamente cerrado y $\alpha \in \mathfrak{m}^*(K)$ tal que $\delta\alpha = D\alpha(0)$ no es una raíz de la unidad. Si $p \geq 1$ es primo con la característica de $K$, entonces $\beta^{\circ p} = \alpha$ tiene exactamente $p$ soluciones, por encima de las $p$ soluciones de $b^p = a$ (la condición sobre $p$ implica que $x^p - a$ es separable).*

Los casos particulares del Teorema 3.4 y los corolarios para $R = \mathbb{C}$ son tratados en [8], donde se trata una forma alternativa de calcular las soluciones.

## 4. Raíces composicionales de la identidad

Si $R = K$ es un cuerpo, hemos visto que cualquier $f \in K[[z]]$ con $\delta f \notin \operatorname{Tor} K^*$ es conjugada a $Lf$. Si $\delta f = a \in \operatorname{Tor} K^*$, y $a^m = 1$, entonces $f = \lambda^{-1} \circ [a] \circ \lambda, \quad \lambda \in \mathfrak{m}^* \implies f^{\circ m} = \lambda^{-1} \circ [a]^{\circ m} \circ \lambda = \lambda^{-1} \circ [a^m] \circ \lambda = \lambda^{-1} \circ [1] \circ \lambda = \imath$, de modo que la única manera que $f$ puede ser conjugada a $Lf$ es si $f$ es una raíz composicional de $\imath$. Esto plantea la determinación de dichas raíces, y la cuestión de si son conjugadas a su parte lineal. Volvamos al caso de un anillo general. Para $h \in \mathfrak{m}$, sea $h^*$ el endomorfismo de $R$-algebras $h^*(f) = f \circ h$.

**Teorema 4.1.** *Si $\varphi^{\circ n} = \imath$ y $n \in R^*$, entonces $\varphi$ es conjugada a su parte lineal.*

*Demostración.* Sea $\omega = \delta\varphi$, de modo que $\omega^n = 1$. Queremos encontrar $\lambda \in \mathfrak{m}^*$ tal que $\lambda \circ \varphi = \omega\lambda$, equivalentemente, $\varphi^*(\lambda) = \omega\lambda$. Consideremos por tanto el endomorfismo de $R$-*módulos* $S = \varphi^* - \omega 1$. Si $\varphi^{\circ n} = \imath$, entonces $\varphi^{*n} = 1$; luego si

$$\Delta = \varphi^{*(n-1)} + \omega\varphi^{*(n-2)} + \cdots + \omega^{n-2}\varphi^* + \omega^{n-1}1$$

entonces $\Delta S = S\Delta = \varphi^{*n} - \omega^n = \varphi^{*n} - 1 = 0$. Poniendo $\lambda = \Delta\imath$ da un elemento obvio de $\ker S$, $\lambda = \Delta\imath = \varphi^{\circ(n-1)} + \omega\varphi^{\circ(n-2)} + \cdots + \omega^{n-2}\varphi + \omega^{n-1}\imath$, y además $\lambda \equiv n\omega^{n-1}\imath = n\omega^{-1}\imath \operatorname{mód} \mathfrak{m}^2$, luego si $n \in R^*$, $\lambda$ es invertible. □

El Lema 4 de [7], que se demuestra mediante el Teorema de Riemann para regiones simplemente conexas en $\mathbb{C}$, es una versión analítica del Teorema 4.1.

*Nota* 4.1. $\operatorname{img}\Delta \subseteq \ker S$ ya que $S\Delta = 0$. Si $n$ es invertible, entonces se da la igualdad: $S\lambda = 0 \iff \varphi^*\lambda = \omega\lambda \implies \Delta\lambda = n\omega^{n-1}\lambda \implies \lambda = \Delta\frac{\omega}{n}\lambda \in \operatorname{img}\Delta$. La función conjugante $\lambda$ está determinada salvo composición a la izquierda con una serie de $C^*_\omega : \lambda^{-1} \circ [\omega] \circ \lambda = \mu^{-1} \circ [\omega] \circ \mu \iff \exists\, \gamma \in C^*_\omega : \mu = \gamma \circ \lambda$. Si $d \mid n$ es el orden de $\omega$, recordar que $C_\omega = zR[[z^d]]$.

**Corolario 4.2.** *Si $n \in R^*$ y $\varphi^{\circ n} = \imath$, con $\varphi \equiv \imath \operatorname{mód} \mathfrak{m}^2$, entonces $\varphi = \imath$.*

*Demostración.* $\varphi \equiv \imath$ mód $\mathfrak{m}^2$ significa que $\delta\varphi = \omega = 1$, luego $\varphi$ es conjugada a $[1] = \imath$, por tanto $\varphi$ es igual a $\imath$. □

**Corolario 4.3.** *Si $\varphi^{\circ n} = [\omega]$ con $\omega^m = 1$ y $m, n \in R^*$, entonces $\varphi \sim L\varphi$, ya que $\varphi^{\circ nm} = [\omega]^{\circ m} = [\omega^m] = \imath$.*

**Lema 4.4.** *Supongamos que $\alpha$ satisface $\alpha \sim L\alpha$ y que toda raíz $n$-ésima composicional $\beta$ de $\alpha$ también satisface $\beta \sim L\beta$. Sea $\alpha = \lambda^{-1} \circ [a] \circ \lambda$. Entonces $\beta^{\circ n} = \alpha \iff \beta = \mu^{-1} \circ [b] \circ \mu$, donde $b^n = a$ y $\mu = \gamma \circ \lambda, \gamma \in C_a^*$.*

*Demostración.* Primero, veamos que tales elementos son de hecho raíces composicionales $n$-ésimas. Si $\beta = \mu^{-1} \circ [b] \circ \mu$, con $b^n = a$ y $\mu = \gamma \circ \lambda, \gamma \in C_a^*$, entonces $\beta^{\circ n} = \mu^{-1} \circ [b]^{\circ n} \circ \mu = \mu^{-1} \circ [b^n] \circ \mu = \mu^{-1} \circ [a] \circ \mu = \lambda^{-1} \circ [a] \circ \lambda = \alpha$.

Ahora supongamos que $\beta^{\circ n} = \alpha$ es cualquier raíz. Sea $b = \delta\beta$. Entonces $b^n = a$. Como $\beta \sim L\beta = [b]$, existe un $\mu \in \mathfrak{m}^*$ tal que $\beta = \mu^{-1} \circ [b] \circ \mu$. Entonces $\alpha = \beta^{\circ n} = \mu^{-1} \circ [b^n] \circ \mu = \mu^{-1} \circ [a] \circ \mu$; por tanto $\mu^{-1} \circ [a] \circ \mu = \lambda^{-1} \circ [a] \circ \lambda$, luego $\mu = \gamma \circ \lambda$ con $\gamma \in C_a^*$. □

**Teorema 4.5.** *Sean $m, n \in R^*$, y $a \in R$ tales que $a^m = 1$. Las soluciones de la ecuación $\beta^{\circ n} = [a]$ son los conjugados de $[b]$ por elementos de $C_a^*$, donde $b$ es una solución de la ecuación $b^n = a$ en $R$.*

*Demostración.* $\alpha = [a]$ satisface $\alpha \sim L\alpha$ trivialmente, con $\lambda = \imath$ como función conjugante. Si $\beta^{\circ n} = [a]$, entonces $\beta \sim L\beta$ ya que $\beta^{\circ nm} = \imath$. Por el lema, $\beta^{\circ n} = [a] \iff \beta = \mu^{-1} \circ [b] \circ \mu$, con $\mu = \gamma \in C_a^*$ y $b^n = a$. □

**Corolario 4.6.** *Si $n \in R^*$, las raíces composicionales $n$-ésimas de $\imath$ son los conjugados por $\mathfrak{m}^*$ de $[\omega]$, $\omega \in R$, $\omega^n = 1$.*

*Demostración.* Este es el caso $m = 1$, y el hecho que $C_1^* = \mathfrak{m}^*$. □

**Corolario 4.7.** *Si $2 \in R^*$, las series $f \in \mathfrak{m}$ tales que $f \circ f = \imath$ son $f = \lambda^{-1} \circ -\imath \circ \lambda$ donde $\lambda \in \mathfrak{m}^*$.*

*Demostración.* Este es el caso $n = 2$, $m = 1$. □

**Teorema 4.8.** *Sea $K$ un cuerpo de característica $0, a \in K^*$. Entonces para todo $n \in \mathbb{N}$, las soluciones de la ecuación $\beta^{\circ n} = [a]$ son los conjugados de $[b]$ por elementos de $C_a^*$, donde $b \in K$ es una solución de $b^n = a$.*

*Demostración.* Como $[a] = L[a], [a] \sim L[a]$ trivialmente por $\imath$. Sea $\beta^{\circ n} = [a]$, con $b = \delta\beta$. Si $a \in \mathrm{Tor}(K^*)$, entonces $\beta \sim L\beta$ porque es una raíz composicional de $\imath$. Si $a \notin \mathrm{Tor}(K^*)$, entonces como $b^n = a$, también $b \notin \mathrm{Tor}(K^*)$, y por tanto $\beta \sim L\beta$ por la teoría de funciones de Schröder. Así que cualquier $\alpha = [a]$ satisface las hipótesis del Lema 4.4, con $\lambda = \imath$, y el resultado se deduce de él. □

*Nota* 4.2. Si $a \notin \mathrm{Tor}(K^*)$, entonces $C_a = [K]$; por tanto cualquier $\gamma \in C_a^*$ tiene la forma $\gamma = [c]$, con $c \in K^*$, y $\gamma^{-1} \circ [b] \circ \gamma = [c^{-1}bc] = [b]$ para cualquier $b$. El teorema dice que en este caso las soluciones de $\beta^{\circ n} = [a]$ son precisamente los elementos $\beta = [b]$ para cada solución $b$ de $b^n = a$. Esto también se podía deducir usando funciones de Schröder: si $a \notin \mathrm{Tor}(K^*)$, la función de Schröder de $\alpha = [a]$

existe y está caracterizada por $\lambda \in \imath + \mathfrak{m}^2$ y $[a] = \lambda^{-1} \circ [a] \circ \lambda$. En otras palabras, $\lambda \in C_a^* = [K^*]$, y $\delta\lambda = 1$, por tanto de hecho $\lambda = \imath$. Hemos mostrado que las soluciones de $\beta^{\circ n} = [a]$ son los conjugados $\beta = \lambda^{-1} \circ [b] \circ \lambda$, donde $b^n = a$. Como $\lambda = \imath$ en este caso, $\beta = [b]$.

## 5. Raíces composicionales en $\imath + \mathfrak{m}^2$. Iteración continua

**Teorema 5.1.** *Sea $\alpha \equiv \imath \mod \mathfrak{m}^2$, $p \geq 1$. Si $p \in R^*$, hay una única serie $\beta \equiv \imath \mod \mathfrak{m}^2$ tal que $\beta^{\circ p} = \alpha$.*

*Demostración.* Sea $\alpha = \sum_{n=1}^{\infty} a_n z^n$, con $a_1 = 1$. Sea $\alpha_m = \sum_{n=1}^{m} a_n z^n$. Construimos por aproximaciones sucesivas una sucesión $b_n$ tal que $\beta_m = \sum_{n=1}^{m} b_n z^n$ satisface $\beta_m^{\circ p} \equiv \alpha_m \mod z^{m+1}$ para todo $m \geq 1$. Si $\beta = \sum_{n=1}^{\infty} b_n z^n$, tomando el límite queda $\beta^{\circ p} = \alpha$.

Definimos $b_1 = 1$. Entonces $\beta_1 = \imath$ satisface la condición con $m = 1$. Suponemos que hemos hallado $b_1, b_2, \ldots, b_m$ tales que $\beta_m^{\circ p} \equiv \alpha_m \mod z^{m+1}$. Sea $\alpha_m - \beta_m^{\circ p} = z^{m+1}\rho_m$, de modo que $\rho_m$ solo depende de $a_1, \ldots, a_m, b_1, \ldots, b_m$. Demostraremos que hay un único $b = b_{m+1}$ tal que $\beta_{m+1} = \beta_m + bz^{m+1}$ satisface $\beta_{m+1}^{\circ p} \equiv \alpha_{m+1} \mod z^{m+2}$. Recordando que $\beta_{m+1} = \beta_m + bz^{m+1} + O(z^{m+2})$, $\beta_{m+1} \equiv \beta_m \equiv z \mod z^2 \implies \beta_{m+1}^{\circ p} = \beta_m^{\circ p} + pbz^{m+1} + O(z^{m+2})$, tenemos

$$\begin{aligned}
\beta_{m+1}^{\circ p} \equiv \alpha_{m+1} \mod z^{m+2} &\iff \beta_m^{\circ p} + pbz^{m+1} \equiv \alpha_{m+1} \mod z^{m+2} \\
&\iff \beta_m^{\circ p} + pbz^{m+1} \equiv \alpha_m + a_{m+1} z^{m+1} \mod z^{m+2} \\
&\iff pbz^{m+1} \equiv (\alpha_m - \beta_m^{\circ p}) + a_{m+1} z^{m+1} \mod z^{m+2} \\
&\iff pbz^{m+1} \equiv \rho_m z^{m+1} + a_{m+1} z^{m+1} \mod z^{m+2} \\
&\iff pb \equiv \rho_m + a_{m+1} \mod z \\
&\iff pb = \rho_m(0) + a_{m+1}
\end{aligned}$$

luego si $p$ es invertible en $R$, esto equivale a

$$b_{m+1} = \frac{\rho_m(0) + a_{m+1}}{p}$$

lo cual expresa $b_{m+1}$ por recurrencia en términos de $a_1, \ldots, a_{m+1}, b_1, \ldots, b_m$. Por tanto una vez puesto $b_1 = 1$, los demás $b_m$ están determinados de manera única por las condiciones $\beta_m^{\circ p} \equiv \alpha_m \mod z^{m+1}$.

Como cualquier $\tilde{\beta} = \sum_{n=1}^{\infty} \tilde{b}_n z^n$ que satisface $\tilde{\beta}^{\circ p} = \alpha$ automáticamente satisface $\tilde{\beta}_m^{\circ p} \equiv \tilde{\beta}^{\circ p} = \alpha \equiv \alpha_m \mod z^{m+1}$, la construcción previa muestra que si $\tilde{b}_1 = 1$, entonces $\tilde{\beta} = \beta$. $\square$

No hemos encontrado una referencia explícita al resultado del Teorema 5.1 en la literatura consultada.

**Corolario 5.2.** *Si $R$ tiene característica 0, y $\mathbb{Q} \subseteq R$, entonces $(\imath + \mathfrak{m}^2, \circ, \imath)$ es un grupo divisible, con raíces únicas.*

También podemos usar el teorema para dar otra demostración del resultado:

**Corolario 5.3.** *Si $p \in R^*$ y $\varphi^{\circ p} = \imath$, con $\varphi \equiv \imath \mod \mathfrak{m}^2$, entonces $\varphi = \imath$.*

*Demostración.* $\imath$ satisface $\imath^{\circ p} = \imath$, y $\imath \equiv \imath$ mód $\mathfrak{m}^2$. Por la unicidad expresada en el teorema, $\varphi = \imath$. □

Procederemos ahora a esbozar la teoría de Brent y Traub, [2]. El propósito de su trabajo era dar métodos efectivos de cálculo para las potencias composicionales de una serie. Reformulamos su método algebraicamente para definir una potencia composicional en $\imath + \mathfrak{m}^2$ con exponentes en $R$ cuando $R$ es un cuerpo de característica 0.

**Definición 5.1.** Dados $\alpha \in \mathfrak{m}$, $\varphi \in R[[z]]$, definimos los conjuntos

$$\begin{aligned} M_\varphi &= \{f \in \mathfrak{m} : \varphi \circ f = \varphi D f\}, \\ M_\varphi^* &= M_\varphi \cap \mathfrak{m}^*, \\ M'_\alpha &= \{\varphi \in R[[z]] : \alpha \in M_\varphi\}. \end{aligned}$$

**Proposición 5.4.** *$M_\varphi$ es un submonoide de $(\mathfrak{m}, \circ, \imath)$. $M_\varphi^*$ es un subgrupo de $\mathfrak{m}^*$. $M'_\alpha$ es un $R$-submódulo de $R[[z]]$.*

*Demostración.* $M_\varphi$ es un submonoide de $\mathfrak{m}$ puesto que $\varphi \circ \imath = \varphi = \varphi D\imath$, luego $\imath \in M_\varphi$, y si $f, g \in M_\varphi$ entonces $\varphi \circ f = \varphi Df$, $\varphi \circ g = \varphi Dg \implies \varphi \circ f \circ g = (\varphi Df) \circ g = (\varphi \circ g)(Df \circ g) = \varphi Dg(Df \circ g) = \varphi D(f \circ g) \implies f \circ g \in M_\varphi$. $M_\varphi^*$ es un subgrupo de $\mathfrak{m}^*$ puesto que $f \in M_\varphi \cap \mathfrak{m}^* \implies \varphi \circ f = \varphi Df \implies \varphi = (\varphi \circ f^{-1})(Df \circ f^{-1}) \implies \varphi Df^{-1} = (\varphi \circ f^{-1})(Df \circ f^{-1})Df^{-1} = (\varphi \circ f^{-1})D(f \circ f^{-1}) = \varphi \circ f^{-1} \implies f^{-1} \in M_\varphi$. Finalmente, $M'_\alpha = \{\varphi : \varphi \circ \alpha = \varphi D\alpha\} = \{\varphi : (\alpha^* - D\alpha)\varphi = 0\} = \ker(\alpha^* - D\alpha)$, donde para $\beta \in R[[z]]$, denotamos también por $\beta$ al endomorfismo dado por la multiplicación por $\beta : f \to \beta f$. Esto demuestra que $M'_\alpha$ es un $R$-submódulo de $R[[z]]$. Por supuesto $\alpha \in M_\varphi \iff \varphi \in M'_\alpha$. □

*Nota* 5.1. Supongamos de ahora en adelante en esta sección que $R = K$ es un cuerpo de característica 0. El siguiente teorema reúne los resultados de [5], Lema 9.4 y su aplicación a la computación de iteraciones en [4], § 4.7.

**Teorema 5.5.**
*(1) Dada $\alpha \in \imath + \mathfrak{m}^2$ con $m = \operatorname{ord}(\alpha - \imath)$, hay una única $\varphi \in \imath^m + \mathfrak{m}^{m+1}$ tal que $\alpha \in M_\varphi$.*
*(2) Dada $\varphi \in \imath^m + \mathfrak{m}^{m+1}$, con $m \geq 2$, y $a \in K$, hay una única $\alpha \in \imath + \mathfrak{m}^2$ tal que $\alpha = z + az^m + O(z^{m+1})$ y $\alpha \in M_\varphi$.*

*Demostración.*
(1) (Unicidad). La hipótesis sobre $\alpha$ significa que es de la forma

$$\alpha = z + a_m z^m + O(z^{m+1}), \qquad D\alpha = 1 + m a_m z^{m-1} + O(z^m), \qquad a_m \neq 0.$$

El resultado dice que $M'_\alpha \cap (\imath^m + \mathfrak{m}^{m+1})$ es un punto. Suponer que $\varphi, \psi \in M'_\alpha \cap (\imath^m + \mathfrak{m}^{m+1})$. Entonces $\varphi - \psi \in M'_\alpha \cap \mathfrak{m}^{m+1}$. Se podrá concluir el resultado si podemos demostrar que

$$\alpha \in \imath + \mathfrak{m}^2, \quad \operatorname{ord}(\alpha - \imath) = m \implies M'_\alpha \cap \mathfrak{m}^{m+1} = (0),$$

lo cual equivale a

$$M'_\alpha \cap \mathfrak{m}^n = (0) \quad \alpha \in \imath + \mathfrak{m}^2, \quad n > \operatorname{ord}(\alpha - \imath).$$

Interpretando $\mathfrak{m}^\infty = (0)$, este resultado también es válido para $m = \infty$.

Supongamos que $f \in M'_\alpha \cap \mathfrak{m}^{m+1}$. Si $f \neq 0$, podemos escribir $f = \sum_{n=\mu}^\infty c_n z^n$, con $\mu \geq m+1$ y $c_\mu \neq 0$. Se tiene

$$\begin{aligned} 0 = f \circ \alpha - fD\alpha &= \sum_{n=\mu}^\infty c_n(\alpha^n - z^n D\alpha) \\ &= \sum_{n=\mu}^\infty c_n\big(z^n + na_m z^{m+n-1} - z^n - ma_m z^{m+n-1} + O(z^{m+n})\big) \\ &= \sum_{n=\mu}^\infty c_n(n-m)a_m z^{m+n-1} + \sum_{n=\mu}^\infty O(z^{m+n}) \\ &= \sum_{n=\mu}^\infty c_n(n-m)a_m z^{m+n-1} + O(z^{m+\mu}) \\ &= c_\mu(\mu - m)a_m z^{m+\mu-1} + O(z^{m+\mu}) \end{aligned}$$

y por tanto debe ser $c_\mu(\mu - m)a_m = 0$. Pero por hipótesis, ninguno de estos factores son 0, luego llegamos a una contradicción; por consiguiente $f = 0$.

(2) (Unicidad). Supongamos que $\alpha, \beta \in M_\varphi$ con $\alpha, \beta \in z + az^m + \mathfrak{m}^{m+1}$. Observar que $\alpha, \beta \in \mathfrak{m}^*$. Primero, tenemos que demostrar que

$$f = z + az^m + O(z^{m+1}) \implies f^{-1} = z - az^m + O(z^{m+1}).$$

Esto se hace fácilmente. Sea $g = f^{-1} = \sum_{n=1}^\infty b_n z^n$. Entonces $g^m = b_1^m z^m + O(z^{m+1}) \implies z = f \circ g = g + ag^m + O(z^{m+1}) = b_1 z + \cdots + b_m z^m + ab_1^m z^m + O(z^{m+1}) \implies b_1 = 1, \quad b_m + ab_1^m = b_m + a = 0 \implies b_m = -a$.

Ahora $\alpha, \beta \in M_\varphi^* \implies \alpha \circ \beta^{-1} \in M_\varphi^*$, y $\alpha \circ \beta^{-1} = \beta^{-1} + a(\beta^{-1})^m + O(z^{m+1}) = z - az^m + az^m + O(z^{m+1}) = z + O(z^{m+1}) \in (\imath + \mathfrak{m}^{m+1}) \cap M_\varphi$, luego para concluir que $\alpha = \beta$, basta con demostrar que

$$\operatorname{ord}(\varphi) = m \implies (\imath + \mathfrak{m}^{m+1}) \cap M_\varphi = (\imath)$$

lo cual equivale a

$$(\imath + \mathfrak{m}^n) \cap M_\varphi = (\imath), \quad n > \operatorname{ord}(\varphi).$$

Esto se puede demostrar de manera similar al primer caso. Igual que antes, el caso $m = \infty$ es trivial, así que supongamos $m < \infty$. Si $f \in \imath + \mathfrak{m}^{m+1}$, $f \neq \imath$, entonces $f = z + a_\mu z^\mu + O(z^{\mu+1})$, con $\mu \geq m+1$, $a_\mu \neq 0$. Sea $\varphi = \sum_{n=m}^\infty b_n z^n$, con $b_m \neq 0$. Ahora, si $f \in M_\varphi$, entonces

$$0 = \varphi \circ f - \varphi Df = \sum_{n=m}^\infty b_n(f^n - z^n Df) = b_m(m-\mu)a_\mu z^{m+\mu-1} + O(z^{m+\mu})$$

pero $b_m(m-\mu)a_\mu \neq 0$ ya que $b_m, a_\mu \neq 0$, $m < \mu$. Por tanto si $f \in (\imath + \mathfrak{m}^{m+1}) \cap M_\varphi$, debe ser $f = \imath$.

(1) (Construcción). Dada $\alpha = z + a_m z^m + O(z^{m+1})$, $m \geq 2$, $a_m \neq 0$, construimos por aproximaciones sucesivas una sucesión $\varphi_n = z^m + b_{m+1}z^{m+1} + \cdots + b_{m+n-1}z^{m+n-1}$ tal que $\varphi_n \circ \alpha \equiv \varphi_n\, D\alpha \text{ mód } z^{2m+n-1}$. Tomando el límite cuando $n \to \infty$ nos da la $\varphi$ requerida.

Empezamos con $\varphi_1 = z^m$. Debemos verificar que $\varphi_1 \circ \alpha \equiv \varphi_1\, D\alpha$ mód $z^{2m}$. En general, para cualquier $n \geq 0$,

$$\begin{aligned} z^n \circ \alpha - z^n\, D\alpha &= \alpha^n - z^n\, D\alpha \\ &= z^n + na_m z^{m+n-1} + O(z^{m+n}) - z^n(1 + ma_m z^{m-1} + O(z^m)) \\ &= (n-m)a_m z^{m+n-1} + O(z^{m+n}). \end{aligned}$$

Para $n = m$ esto se reduce a $O(z^{2m})$, como queríamos.

Supongamos que $n \geq 1$ y que hemos encontrado $b_m = 1, b_{m+1}, \ldots, b_{m+n-1}$ tales que $\varphi_n \circ \alpha \equiv \varphi_n\, D\alpha$ mód $z^{2m+n-1}$. Sea $\varphi_n \circ \alpha - \varphi_n\, D\alpha = z^{2m+n-1}\psi$. Poniendo $\varphi_{n+1} = \varphi_n + bz^{m+n}$, tenemos que encontrar $b = b_{m+n}$ tal que

$$\begin{aligned} & \varphi_{n+1} \circ \alpha \equiv \varphi_{n+1}\, D\alpha \text{ mód } z^{2m+n} \\ \iff & \varphi_n \circ \alpha + b\alpha^{m+n} \equiv \varphi_n D\alpha + bz^{m+n} D\alpha \text{ mód } z^{2m+n} \\ \iff & \varphi_n \circ \alpha - \varphi_n D\alpha \equiv b\,(z^{m+n} D\alpha - \alpha^{m+n}) \text{ mód } z^{2m+n} \\ \iff & z^{2m+n-1}\psi \equiv b\,(z^{m+n} D\alpha - \alpha^{m+n}) \text{ mód } z^{2m+n} \\ \iff & z^{2m+n-1}\psi \equiv -b\, na_m z^{2m+n-1} \text{ mód } z^{2m+n} \\ \iff & \psi \equiv -b\, na_m \text{ mód } z \\ \iff & \psi(0) = -b\, na_m \end{aligned}$$

de modo que, efectivamente, la solución es única:

$$b_{m+n} = -\frac{\Psi(0)}{na_m}.$$

Obsérvese la importancia de tener $\alpha \equiv \imath$ mód $\mathfrak{m}^2$. Si hubiera otro coeficiente de primer grado, sus potencias no cancelarían de manera tan efectiva en $z^n \circ \alpha - z^n D\alpha$.

(2) (Construcción). Dada $\varphi = z^m + O(z^{m+1})$, construimos por aproximaciones sucesivas una sucesión $\alpha_n = z + az^m + a_{m+1}z^{m+1} + \cdots + a_{m+n-1}z^{m+n-1}$ tal que $\varphi \circ \alpha_n \equiv \varphi D\alpha_n$ mód $z^{2m+n-1}$. Tomando límites nos da la serie $\alpha$ requerida.

Empezamos con $\alpha_1 = z + az^m$. Debemos verificar que $\varphi \circ \alpha_1 \equiv \varphi D\alpha_1$ mód $z^{2m}$. En general, recordando que si $\varphi = \sum_{n=m}^{\infty} b_n z^n$ y $f = z + a_\mu z^\mu + O(z^{\mu+1})$, con $\mu \geq 2$, entonces $\varphi \circ f - \varphi Df = b_m(m-\mu)a_\mu z^{m+\mu-1} + O(z^{m+\mu})$, para $f = \alpha_1$ se tiene $\mu = m$, y la expresión se reduce a $O(z^{2m})$.

Supongamos que $n \geq 1$ y que hemos encontrado $a_m = a, a_{m+1}, \ldots, a_{m+n-1}$ tales que $\varphi \circ \alpha_n \equiv \varphi D\alpha_n$ mód $z^{2m+n-1}$. Sea $\varphi \circ \alpha_n - \varphi D\alpha_n = z^{2m+n-1}\psi$. Poniendo $\alpha_{n+1} = \alpha_n + cz^{m+n}$, tenemos que encontrar $c = a_{m+n}$ tal que

$$\begin{aligned} & \varphi \circ \alpha_{n+1} \equiv \varphi D\alpha_{n+1} \text{ mód } z^{2m+n} \\ \iff & \varphi \circ (\alpha_n + cz^{m+n}) \equiv \varphi(D\alpha_n + (m+n)cz^{m+n-1}) \text{ mód } z^{2m+n} \\ \iff & \varphi \circ \alpha_n + (D\varphi \circ \alpha_n)cz^{m+n} + O(z^{2m+2n}) \\ & \qquad \equiv \varphi D\alpha_n + (m+n)cz^{m+n-1}\varphi \text{ mód } z^{2m+n} \\ \iff & (\varphi \circ \alpha_n - \varphi D\alpha_n) + (D\varphi \circ \alpha_n)cz^{m+n} \equiv (m+n)cz^{m+n-1}\varphi \text{ mód } z^{2m+n} \\ \iff & z^{2m+n-1}\psi + ((mz^{m-1} + O(z^m)) \circ \alpha_n)cz^{m+n} \end{aligned}$$

$$
\begin{aligned}
&\qquad \equiv (m+n)cz^{m+n-1}(z^m + O(z^{m+1})) \text{ mód } z^{2m+n}\\
&\iff z^{2m+n-1}\psi + (m\alpha_n^{m-1} + O(\alpha_n^m))cz^{m+n} \equiv (m+n)cz^{2m+n-1} \text{ mód } z^{2m+n}\\
&\iff z^{2m+n-1}\psi + cm\alpha_n^{m-1}z^{m+n} + O(z^m)cz^{m+n}\\
&\qquad \equiv (m+n)cz^{2m+n-1} \text{ mód } z^{2m+n}\\
&\iff z^{2m+n-1}\psi + cm(z^{m-1} + O(z^m))z^{m+n} \equiv (m+n)cz^{2m+n-1} \text{ mód } z^{2m+n}\\
&\iff z^{2m+n-1}\psi + cmz^{2m+n-1} \equiv (m+n)cz^{2m+n-1} \text{ mód } z^{2m+n}\\
&\iff \psi(0) + cm = (m+n)c\\
&\iff \psi(0) = nc
\end{aligned}
$$

de modo que esto obliga

$$a_{m+n} = \frac{\psi(0)}{n}.$$

□

*Nota* 5.2. Los enunciados de unicidad en el teorema, en el sentido de haber a lo sumo una serie que cumpla las propiedades, son válidos en cualquier anillo íntegro $R$ de característica 0, ya que en su demostración no hemos necesitado dividir en ningún momento.

Ahora sea $\alpha \in \imath + \mathfrak{m}^2$, y supongamos que $\alpha \neq \imath$, de modo que $2 \leq m = \operatorname{ord}(\alpha - \imath) < \infty$ (ya habíamos considerado las raíces composicionales de $\imath$). Sea $\alpha = z + a_m z^m + O(z^{m+1}), m \geq 2, a_m \neq 0$. Sea $\varphi = z^m + O(z^{m+1})$ la única serie, dada por la primera parte del teorema, tal que $\alpha \in M_\varphi$.

**Definición 5.2.** Dado $a \in K$, sea $\alpha_a$ la única serie en $M_\varphi$ de la forma $z + aa_m z^m + O(z^{m+1})$, dada por la segunda parte del teorema. Veremos que $a \to \alpha_a$ define una «exponenciación composicional».

**Teorema 5.6.**

*(1) $\alpha_n = \alpha^{\circ n}$ para $n \in \mathbb{Z}$, donde $\alpha^{\circ 0} = \imath$ y $\alpha^{\circ(-n)} = (\alpha^{-1})^{\circ n}$ para $n \in \mathbb{N}$.*

*(2) $\alpha_a \circ \alpha_b = \alpha_b \circ \alpha_a = \alpha_{a+b}$ para todo $a, b \in K$. $\alpha_a^{\circ n} = \alpha_{na}$ para todo $n \in \mathbb{N}$.*

*(3) Para $n \in \mathbb{N}, \alpha_{1/n}$ es la raíz $n$-ésima composicional (única) de $\alpha$ en $\imath + \mathfrak{m}^2$.*

*Demostración.*
(1) Por la fórmula de composición iterada (Lema 2.7), para cualquier $n \in \mathbb{N}$ se tiene $\alpha^{\circ n} = z + na_m z^m + O(z^{m+1})$, y como $M_\varphi$ es un submonoide de $\mathfrak{m}$, $\alpha \in M_\varphi \implies \alpha^{\circ n} \in M_\varphi$. Como por definición $\alpha_n$ es la única serie en $M_\varphi$ de la forma $z + na_m z^m + O(z^{m+1})$, se deduce que $\alpha_n = \alpha^{\circ n}$ para $n \in \mathbb{N}$.

Hemos demostrado que $\alpha = z + a_m z^m + O(z^{m+1}) \implies \alpha^{-1} = z - a_m z^m + O(z^{m+1})$, y como $\alpha \in M_\varphi^*$, también $\alpha^{-1} \in M_\varphi^*$. Por otra parte, $\alpha_{-1}$ es la única serie en $M_\varphi$ de la forma $z - a_m z^m + O(z^{m+1})$, luego $\alpha_{-1} = \alpha^{-1}$.

Combinando los dos razonamientos, si $n \in \mathbb{N}$, entonces por la fórmula de composición iterada, $\alpha^{-1} = z - a_m z^m + O(z^{m+1}) \implies \alpha^{\circ(-n)} = (\alpha^{-1})^{\circ n} = z - na_m z^m + O(z^{m+1})$ y $\alpha^{-1} \in M_\varphi \implies \alpha^{\circ(-n)} \in M_\varphi$. Por otra parte, $\alpha_{-n}$ es la única serie en

$M_\varphi$ de la forma $z - na_m z^m + O(z^{m+1})$, luego $\alpha_{-n} = \alpha^{\circ(-n)}$ para $n \in \mathbb{N}$, es decir $\alpha_n = \alpha^{\circ n}$ para $n \in \mathbb{Z}, n < 0$.

Finalmente, $\imath \in M_\varphi$ es obviamente de la forma $z + 0 \cdot a_m z^m + O(z^{m+1})$, de modo que por unicidad, $\imath = \alpha_0$.

(2) Por definición, $\alpha_a = z + aa_m z^m + O(z^{m+1}), \alpha_b = z + ba_m z^m + O(z^{m+1})$, luego $\alpha_a \circ \alpha_b = \alpha_b + aa_m \alpha_b^m + O(\alpha_b^{m+1}) = z + ba_m z^m + aa_m z^m + O(z^{m+1}) = z + (a+b)a_m z^m + O(z^{m+1})$ y por simetría, $\alpha_b \circ \alpha_a$ es también de esta forma. Como $\alpha_a, \alpha_b \in M_\varphi$, también $\alpha_a \circ \alpha_b, \alpha_b \circ \alpha_a \in M_\varphi$. Por otra parte, $\alpha_{a+b}$ es la única serie en $M_\varphi$ de la forma $z + (a+b)a_m z^m + O(z^{m+1})$, con lo cual se deduce (2). Por inducción, para $n \in \mathbb{N}$, $\alpha_a^{\circ n} = \alpha_a \circ \cdots \circ \alpha_a = \alpha_{a+\cdots+a} = \alpha_{na}$.

(3) Por (1) y (2) se tiene $\alpha_{1/n}^{\circ n} = \alpha_1 = \alpha^{\circ 1} = \alpha$, luego $\alpha_{1/n}$ es una raíz $n$-ésima composicional de $\alpha$, y $\alpha_{1/n} \in \imath + \mathfrak{m}^2$ por definición. □

*Nota* 5.3. Sabemos que la raíz $n$-ésima composicional $\alpha_{1/n}$ es única por el primer teorema. Parece más difícil utilizar $M_\varphi$ para demostrar la unicidad, pues no es obvio que cualquier raíz composicional deba pertenecer a $M_\varphi$. Tampoco es inmediato que una raíz composicional en $\imath + \mathfrak{m}^2$ deba tener la forma $z + \frac{1}{n} a_m z^m + O(z^{m+1})$.

Es interesante contrastar estos resultados con los de Labelle [6], que utiliza métodos completamente diferentes para la iteración continua, basados en familias especiales de polinomios auxiliares.

**Proposición 5.7.** *Si* $\operatorname{ord}(\alpha - \imath) = 2$ *y* $n \in \mathbb{N}$, *entonces la única solución de* $\beta^{\circ n} = \alpha$ *es la solución en* $\imath + \mathfrak{m}^2$.

*Demostración.* Sea $\beta = \omega z + bz^2 + O(z^3)$. Por la fórmula de composición iterada $\beta^{\circ n} = \omega^n z + \omega^{n-1} b(1 + \omega + \omega^2 + \cdots + \omega^{n-1})z^2 + O(z^3)$. Si $\beta^{\circ n} = \alpha$, entonces $\omega^n = 1$, luego si $\omega \neq 1$, $1 + \omega + \omega^2 + \cdots + \omega^{n-1} = \frac{\omega^n - 1}{\omega - 1} = 0$; por tanto $\alpha = z + O(z^3)$, es decir, $\operatorname{ord}(\alpha - \imath) \geq 3$. □

*Nota* 5.4. No es cierto por tanto que para series $\alpha \in \imath + \mathfrak{m}^2$ haya siempre una solución de $\beta^{\circ n} = \alpha$ encima de cada solución de $b^n = 1$, incluso si $K$ es algebraicamente cerrado de característica zero. Por ejemplo, ninguna iteración de una serie de la forma $-z + O(z^2)$ puede ser igual a una serie de la forma $z + az^2 + O(z^3)$ con $a \neq 0$.

## 6. Término lineal de torsión

*Nota* 6.1. Supondremos que $R = K$ es un cuerpo, aunque no necesariamente de característica cero.

**Teorema 6.1.** *Sea* $\alpha = \zeta z + O(z^2)$ *con* $\zeta$ *una raíz primitiva* $q$*-ésima de la unidad. Entonces* $\alpha$ *tiene una raíz* $p$*-ésima composicional para todo entero positivo* $p$ *primo con* $q$ *y la característica de* $K$.

*Demostración.* Construiremos $\beta$ tal que $\beta^{\circ p} = \alpha$ hallando por recurrencia coeficientes $b_1, \ldots, b_n$ tales que $\beta_n = b_1 z + b_2 z^2 + \cdots + b_n z^n$ satisface $\beta_n^{\circ p} \equiv \alpha \text{ mód } z^{n+1}$.

Como $\beta_1 = b_1 z = [b_1], \beta_1^{\circ p} \equiv \alpha \text{ mód } z \iff b_1^p = \zeta$, tendremos que elegir $b_1 = \omega \in K^*$ tal que $\omega^p = \zeta$. De momento, dejamos abierta la elección.

Supongamos que hemos encontrado $b_1 = \omega, b_2, \ldots, b_n$ tales que $\beta_n^{\circ p} \equiv \alpha$ mód $z^{n+1}$. Tenemos que encontrar $b = b_{n+1}$ tal que $\beta_{n+1} = \beta_n + bz^{n+1}$ satisface $\beta_{n+1}^{\circ p} \equiv \alpha$ mód $z^{n+2}$. Por la fórmula de composición iterada, $\beta_{n+1} = \beta_n + bz^{n+1} \implies \beta_{n+1}^{\circ p} = \beta_n^{\circ p} + \omega^{p-1}b(1 + \omega^n + \omega^{2n} + \cdots + \omega^{(p-1)n})z^{n+1} + O(z^{n+2})$. Sea $\alpha - \beta_n^{\circ p} = z^{n+1}\rho$. Entonces

$$\begin{aligned} &\beta_{n+1}^{\circ p} \equiv \alpha \text{ mód } z^{n+2} \\ \iff &\beta_n^{\circ p} + \omega^{p-1}b(1 + \omega^n + \omega^{2n} + \cdots + \omega^{(p-1)n})z^{n+1} \equiv \alpha \text{ mód } z^{n+2} \\ \iff &\omega^{p-1}b(1 + \omega^n + \omega^{2n} + \cdots + \omega^{(p-1)n})z^{n+1} \equiv z^{n+1}\rho \text{ mód } z^{n+2} \\ \iff &\omega^{p-1}b(1 + \omega^n + \omega^{2n} + \cdots + \omega^{(p-1)n}) = \rho(0) \end{aligned}$$

de modo que podemos resolver para $b = b_{n+1}$ si y solo si $(1 + \omega^n + \omega^{2n} + \cdots + \omega^{(p-1)n}) \neq 0$. Si $\omega^n = 1$, es decir, $\operatorname{ord}(\omega) \mid n$, la suma es $p$. Si $\omega^n \neq 1$, entonces $(1+\omega^n+\omega^{2n}+\cdots+\omega^{(p-1)n}) = \frac{1-\omega^{pn}}{1-\omega^n} = \frac{1-\zeta^n}{1-\omega^n}$, de modo que necesitamos que $\zeta^n \neq 1$ cuando $\omega^n \neq 1$. Esto es equivalente a $\zeta^n = 1 \implies \omega^n = 1$, que a su vez equivale a $\operatorname{ord}(\zeta) = q \mid n \implies \operatorname{ord}(\omega) \mid n$. Eligiendo $n = q$ muestra que esto equivale a $\operatorname{ord}(\omega) \mid q$. Como necesitamos $\omega^p = \zeta$, se tiene $q = \operatorname{ord}(\zeta) = \operatorname{ord}(\omega^p) = \frac{\operatorname{ord}(\omega)}{(\operatorname{ord}(\omega),p)}$, por tanto $q \mid \operatorname{ord}(\omega)$. Luego de hecho necesitamos que $\operatorname{ord}(\omega) = q$, y como $q = \frac{\operatorname{ord}(\omega)}{(\operatorname{ord}(\omega),p)}$, esto implica $(q,p) = 1$.

Asimismo, si $(q,p) = 1$, elegimos $p^* \in \mathbb{N}$ tal que $pp^* \equiv 1$ mód $q$. Entonces $\omega = \zeta^{p^*} \in K$ satisface $\omega^p = \zeta^{pp^*} = \zeta$, y $\operatorname{ord}(\omega) = \operatorname{ord}(\zeta^{p^*}) = \frac{\operatorname{ord}(\zeta)}{(\operatorname{ord}(\zeta),p^*)} = \frac{q}{(q,p^*)} = q$, de modo que se cumplen todas las condiciones. □

**Proposición 6.2.** *Sea $\zeta$ una raíz primitive $q$-ésima de la unidad. Ninguna serie de la forma $\alpha = \zeta z + az^{q+1} + O(z^{q+2})$, con $a \neq 0$, tiene una raíz $p$-ésima composicional si $(p,q) \neq 1$.*

*Demostración.* Dado cualquier $\omega$ tal que $\omega^p = \zeta$, siempre podemos encontrar $n$ tal que $q \mid n$, luego $\zeta^n = 1$, pero $\omega^n \neq 1$. Efectivamente, $q = \operatorname{ord}(\zeta) = \operatorname{ord}(\omega^p) = \frac{\operatorname{ord}(\omega)}{(\operatorname{ord}(\omega),p)}$, luego $\operatorname{ord}(\omega) = qp'$ donde $p' = (\operatorname{ord}(\omega), p) > 1$ como $(q,p) \mid p'$. Ahora si $n = qm$, entonces $\omega^n = 1 \iff \operatorname{ord}(\omega) = qp' \mid qm = n \iff p' \mid m$, luego eligiendo $m$ de modo que $p' \nmid m$ obtenemos un tal $n$. Por ejemplo, $m = 1$, o sea $n = q$, funciona.

Supongamos que $\beta^{\circ p} = \alpha$. Entonces $\beta = \omega z + O(z^2)$, con $\omega^p = \zeta$. De hecho debe ser $\beta = \omega z + O(z^{q+1})$. Supongamos lo contrario. Entonces $\beta = \omega z + bz^{m+1} + O(z^{m+2})$ con $1 \leq m < q$ y $b \neq 0$. Por la fórmula de composición iterada, $\beta^{\circ p} = \omega^p z + \omega^{p-1}b(1 + \omega^m + \omega^{2m} + \cdots + \omega^{(p-1)m})z^{m+1} + O(z^{m+2}) = \zeta z + cz^{m+1} + O(z^{m+2})$. $\omega^m \neq 1$ ya que $\operatorname{ord}(\omega) > q > m \geq 1$, luego $\operatorname{ord}(\omega) \nmid m$. Entonces $(1 + \omega^m + \omega^{2m} + \cdots + \omega^{(p-1)m}) = \frac{1-\omega^{pm}}{1-\omega^m} = \frac{1-\zeta^m}{1-\omega^m}$ y $\zeta^m \neq 1$ como $\operatorname{ord}(\zeta) = q > m$, luego $c \neq 0$, de modo que $\beta^{\circ p}$ no puede ser de la forma $\zeta z + az^{q+1} + O(z^{q+2})$, para cualquier $a$.

Como $\beta = \omega z + bz^{q+1} + O(z^{q+2})$, aplicando la fórmula de composición iterada una vez más, $\beta^{\circ p} = \omega^p z + \omega^{p-1}b(1 + \omega^q + \omega^{2q} + \cdots + \omega^{(p-1)q})z^{q+1} + O(z^{q+2}) = \zeta z + cz^{q+1} + O(z^{q+2})$ y otra vez, $\omega^q \neq 1$ ya que $\operatorname{ord}(\omega) > q$, pero ahora $(1 + \omega^q +$

$\omega^{2q} + \cdots + \omega^{(p-1)q}) = \frac{1-\omega^{pq}}{1-\omega^q} = \frac{1-\zeta^q}{1-\omega^q} = 0$, luego $c = 0$, y también es imposible que $\beta^{\circ p} = \zeta z + az^{q+1} + O(z^{q+2})$, con $a \neq 0$. □

Este razonamiento con los órdenes de las raíces de la unidad es análogo a la utilización del llamado «lema de teoría de números» citado en [10], § 1.

*Ejemplo* 6.1. $\alpha = -z + z^3$ no tiene raíz cuadrada composicional, ya que corresponde al caso $\zeta = -1$, $p = q = 2$.

## 7. Término lineal nulo

**Lema 7.1.** *Sea* $\operatorname{ord}(f) = \nu > 1$ *y* $f = a_\nu z^\nu + g$ *con* $a_\nu \neq 0$ *y* $\operatorname{ord}(g) = \mu > \nu$. *Entonces*

$$f^{\circ n} = a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}} z^{\nu^n} + \nu^{n-1} a_\nu^{\nu+\nu^2+\cdots+\nu^{n-1}} z^{\nu^n-\nu} g + O(z^{\nu^n-\nu+\mu+1}).$$

*Demostración.* Por inducción en $n$. Para $n = 1$ los dos primeros términos son simplemente $a_\nu z^\nu + g = f$. La fórmula es inmediata si $g = 0$ ($\mu = \infty$), por tanto suponemos que $\mu < \infty$. Supongamos la fórmula cierta para $n$. Observando que $f = O(z^\nu)$ y $g \circ f = O(z^{\mu\nu})$, se tiene entonces

$$\begin{aligned}
f^{\circ(n+1)} &= a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}} f^{\nu^n} + \nu^{n-1} a_\nu^{\nu+\nu^2+\cdots+\nu^{n-1}} f^{\nu^n-\nu}(g \circ f) \\
&\quad + O(f^{\nu^n-\nu+\mu+1}) \\
&= a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}} (a_v z^\nu + g)^{\nu^n} \\
&\quad + O(z^{\nu(\nu^n-\nu)}) O(z^{\mu\nu}) + O(z^{\nu(\nu^n-\nu+\mu+1)}) \\
&= a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}} (a_v z^\nu + g)^{\nu^n} + O(z^{\nu(\nu^n-\nu)+\mu\nu}) + O(z^{\nu(\nu^n-\nu+\mu+1)}).
\end{aligned}$$

Analizamos los términos de orden primero. Observar que $\nu(\nu^n - \nu + \mu + 1) = \nu^{n+1} - \nu^2 + \mu\nu + \nu > \nu^{n+1} - \nu^2 + \mu\nu = \nu(\nu^n - \nu) + \mu\nu$ y $\nu^{n+1} - \nu^2 + \mu\nu \geq \nu^{n+1} - \nu + \mu + 1 \iff -\nu^2 + \mu\nu > -\nu + \mu \iff \mu(\nu - 1) > \nu(\nu - 1)$, lo cual es cierto ya que $\mu > \nu > 1$. Por tanto ambos términos de orden están incorporados en el término $O(z^{\nu^{n+1}-\nu+\mu+1})$ correspondiente a $n + 1$. Ahora estudiamos el término binomial

$$(a_v z^\nu + g)^{\nu^n} = \sum_{l=0}^{\nu^n} \binom{\nu^n}{l} (a_\nu z^\nu)^{\nu^n-l} g^l = \sum_{l=0}^{\nu^n} \binom{\nu^n}{l} a_\nu^{\nu^n-l} z^{\nu^{n+1}-l\nu} g^l.$$

Observar que $\operatorname{ord}(z^{\nu^{n+1}-l\nu} g^l) = \nu^{n+1} - l\nu + l\mu > \nu^{n+1} - \nu + \mu \iff (l-1)\mu > (l-1)\nu$, y como esto se cumple para $l > 1$, los términos con $l > 1$ en el desarrollo del binomio también están en el término $O(z^{\nu^{n+1}-\nu+\mu+1})$, y quedan solo los términos con $l = 0, 1$ $a_\nu^{\nu^n} z^{\nu^{n+1}} + \nu^n a_\nu^{\nu^n-1} z^{\nu^{n+1}-\nu} g$, los cuales al ser multiplicados por la constante que habíamos dejado fuera, dan finalmente

$$\begin{aligned}
&a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}} (a_\nu^{\nu^n} z^{\nu^{n+1}} + \nu^n a_\nu^{\nu^n-1} z^{\nu^{n+1}-\nu} g) \\
&= a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}} a_v^{\nu^n} z^{\nu^{n+1}} + \nu^n a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}} a_\nu^{\nu^n-1} z^{\nu^{n+1}-\nu} g \\
&= a_\nu^{1+\nu+\nu^2+\cdots+\nu^{n-1}+\nu^n} z^{\nu^{n+1}} + \nu^n a_\nu^{\nu+\nu^2+\cdots+\nu^{n-1}+\nu^n} z^{\nu^{n+1}-\nu} g
\end{aligned}$$

lo cual demuestra la fórmula para $n+1$. □

**Corolario 7.2.**
*(1) Sea $R$ cualquier anillo conmutativo. Si $m > 1, a \in R, a \neq 0$, entonces $az^m$ tiene una raíz $n$-ésima composicional si y solo si $m$ es una potencia $n$-ésima, $m = \nu^n$ con $\nu > 1$, y $a$ es una potencia $\frac{\nu^n - 1}{\nu - 1} = \frac{m-1}{\nu-1}$-ésima en $R$.*
*(2) Si $a \in R$ y $\nu \in \mathbb{N}, \nu > 1$ no son divisores de cero, entonces las raíces $n$-ésimas composicionales de $az^{\nu^n}$ son las series $f = bz^\nu$ con*

$$b^{1+\nu+\nu^2+\cdots+\nu^{n-1}} = b^{\frac{\nu^n-1}{\nu-1}} = a.$$

*Demostración.*
(1) Si $az^m = f^{\circ n}$ con $\operatorname{ord}(f) = \nu$, entonces como $\operatorname{ord}(f \circ g) = \operatorname{ord}(f)\operatorname{ord}(g)$, tomando el orden, queda $m = \nu^n$. Poniendo $f = bz^\nu + g$ con $\operatorname{ord}(g) > \nu$, el lema implica que $b^{\frac{\nu^n-1}{\nu-1}} = a$.

Si $a = b^{\frac{\nu^n-1}{\nu-1}}$ entonces por el lema $(bz^\nu)^{\circ n} = az^{\nu^n} = az^m$.
(2) Por el Lema 7.1 cualquier tal $bz^\nu$ es una raíz $n$-ésima composicional de $az^{\nu^n}$.

Si $f^{\circ n} = az^{\nu^n}$, entonces tomando el orden, queda $\operatorname{ord}(f) = \nu$. Poniendo $f = bz^\nu + g$ con $\operatorname{ord}(g) = \mu > \nu$, el lema implica

$$f^{\circ n} = b^{1+\nu+\nu^2+\cdots+\nu^{n-1}} z^{\nu^n} + \nu^{n-1} b^{\nu+\nu^2+\cdots+\nu^{n-1}} z^{\nu^n-\nu} g + O(z^{\nu^n-\nu+\mu+1}) = az^{\nu^n}$$

y el segundo término tiene orden $\nu^n - \nu + \mu > \nu^n$, luego igualando coeficientes queda $g = 0$ y por tanto $f = bz^\nu$ con $b^{\frac{\nu^n-1}{\nu-1}} = a$ (como $a$ no es un divisor de cero, $b$ tampoco lo es). □

Estos resultados están en parte tratados en el Teorema 3 (c) de [10]. No hemos encontrado mención explícita de la fórmula del Lema 7.1.

## Referencias


[1] A. F. Beardon, *Iteration of rational functions: Complex analytic dynamical systems*, GTP **132**, Springer-Verlag, 1991.
[2] R. P. Brent y J. F. Traub, On the complexity of composition and generalized composition of power series, *SIAM J. Comput.* **9** (1980), 54–66.
[3] N. G. de Bruijn, *Asymptotic methods in analysis*, Dover Publications, 1981.
[4] D. Knuth, *The Art of computer programming, vol. 2: Seminumerical algorithms*, Addison-Wesley, 1981.
[5] M. Kuczma, *Functional equations in a single variable*, PWN-Polish Scientific Publishers, Varsovia, 1968.
[6] G. Labelle, Sur l'inversion et l'itération continue des séries formelles, *Europ. J. Combinatorics* **1** (1980), 113–138.
[7] B. Muckenhoupt, Some results on analytic iteration and conjugacy, *Amer. J. Math.* **84** (1962), 161–169.
[8] L. Reich, Iterative roots of formal power series: Universal expressions for the coefficients and analytic iteration, *Grazer. Math. Ber.* **327** (1996), 21–32.
[9] S. Scheinberg, Power series in one variable, *J. Math. Anal. Appl.* **31** (1970), 321–333.
[10] J. Schwaiger, Roots of formal power series in one variable, *Aequationes Math.* **29** (1985), 40–43.



Departamento de Matemática Pura y Aplicada, Universidad de Salamanca, Plaza de la Merced 1-4, 37008 Salamanca, Spain

*Correo electrónico*: navas@gugu.usal.es