Recepción del original: 22/11/2021 . Aceptación: 18/08/2021

Factorización invariante de unidades en el anillo convolucional de Dirichlet

Invariant factorization of units in the convolutional Dirichlet ring

DANIEL PRELAT, NELSON MONZÓN Y MARTÍN MAULHARDT

Facultad de Ingeniería del Ejército, Universidad de la Defensa Nacional, Argentina
dprelat@fie.undef.edu.ar

El anillo convolucional de Dirichlet, estructura central de la Teoría Analítica de Números, es un dominio de factorización única. Pero en este anillo abundan los elementos inversibles, por lo tanto los elementos primos tienen demasiados elementos asociados. Esto disminuye el alcance práctico de la factorización en primos. En este trabajo presentamos una factorización única de los elementos inversibles en términos de funciones fuertemente multiplicativas en potencias. Paralelamente, introducimos una acción del grupo S(∞) en el anillo, que denominamos acción primaria, y obtenemos una invariante del teorema de factorización de unidades. Finalmente, las series de Bell resultan ser las generatrices naturales para el estudio y aplicación de los resultados teóricos obtenidos, aplicación que se puede extender a las series de Fourier fuertemente convergentes.

(2000 MSC): Primary: 11A25 Secondary: 13J99, 20B27

Introducción

El anillo convolucional de Dirichlet, que indicaremos con el símbolo $\mathcal{A}(\mathbb{C})$, es el anillo de las funciones $a: \mathbb{N} \to \mathbb{C}$ con las operaciones de suma punto a punto (i.e. $(a+b)(n) = a(n)+b(n)$ para todas a y b en $\mathcal{A}(\mathbb{C})$ todo entero positivo n) y el producto

$$(a*b)(n) = \sum_{d|n} a(d)\, b\left(\frac{n}{d}\right) = \sum_{hk=n} a(h)\, b(k) \qquad (1.1)$$

$\mathcal{A}(\mathbb{C})$ todo entero positivo n. La primera suma se extiende sobre los divisores enteros positivos d de n y la segunda sobre todos los pares de factores enteros positivos h, k de n. Para el producto punto a punto utilizaremos la notación habitual ab, es decir: $(ab)(n)= a(n)b(n)$ para todas a y b en $\mathcal{A}(\mathbb{C})$ todo entero positivo n. A diferencia de este producto, la multiplicación (1.1) no tiene divisores de cero, lo que tiene una importancia no menor para las aplicaciones. El elemento neutro es la función e_1: $\mathbb{N}\to\{0,1\}$ tal que $e_1(1)=1$ y $e_1(n)=0$ para todo $n \geq 2$. Los elementos inversibles, es decir, sus unidades, son las funciones $a: \mathbb{N} \to \mathbb{C}$ tales que $a(1)\neq 0$. En este caso, el inverso es la función $a^{*-1}: \mathbb{N} \to \mathbb{C}$ definida mediante las fórmulas de recurrencia

$$a^{*-1}(1) = \frac{1}{a(1)}$$

$$a^{*-1}(n) = -\frac{1}{a(1)} \sum_{\substack{d|n \\ d<n}} a\left(\frac{n}{d}\right) a^{*-1}(d) \text{ si } n \geq 2 \qquad (1.2)$$

La estructura de este anillo conmutativo, que es un objeto central en la teoría de números, ha sido extensamente estudiada, por ejemplo en Shapiro, H. (1972); Cashwell, E. D. y Everett, C. J. (1959); Elliott, J. (2008) y Tóth, L. y Haukkanen, P. (2009). Se trata de un dominio de factorización única, y además es un anillo local con ideal maximal $\mathfrak{m} = \{ a \in \mathcal{A}(\mathbb{C}) : a$

$(1)=0\}$. No es noetheriano, más aún: admite una cadena estrictamente creciente de ideales no estacionaria y por lo tanto tiene dimensión de Krull infinita. Al grupo de unidades lo indicaremos con el símbolo usual $\mathcal{A}(\mathbb{C})^{x}$. Este grupo admite el subgrupo

$$\mathcal{A}(\mathbb{C})_1^{x}=\{a\in\mathcal{A}(\mathbb{C}):a(1)=1\} \tag{1.1}$$

que va a jugar un papel central en este trabajo. Desde el punto de vista de la teoría analítica de números, recordemos que cada elemento $a\in\mathcal{A}(\mathbb{C})$ tiene asociada su correspondiente serie de Dirichlet: $\varphi_a(s)=\sum_{n=1}^{\infty}\frac{a(n)}{n^s}$, donde s es una variable compleja. La propiedad clave de estas series es que para cada par de elementos a y b en $\mathcal{A}(\mathbb{C})$ se tienen las relaciones $\varphi_{a+b}(s)=\varphi_a(s)+\varphi_b(s)$ y $\varphi_{a*b}(s)=\varphi_a(s)\varphi_b(s)$. Es decir: la aplicación $a\mapsto\varphi_a$ es un homomorfismo de anillos (del anillo $\mathcal{A}(\mathbb{C})$ en el anillo de series formales de una variable compleja). Una referencia excelente –y ya clásica– sobre los elementos más importantes de este anillo (v.gr. la función de Möbius, la función de Euler, la función de Liouville, la función de von Mangoldt, etc.) y sus correspondientes series de Dirichlet siguen siendo los dos siguientes libros de Apostol mencionados en la bibliografía: Apostol, T. (1976) y su continuación, Apostol, T. (1990).

El anillo $\mathcal{A}(\mathbb{C})$ admite una topología muy interesante, dada por una distancia ultramétrica $d:\mathcal{A}(\mathbb{C})x\mathcal{A}(\mathbb{C})\to\{0\}\cup\{(1/n):\in N\}$, que ha sido estudiada, por ejemplo, por H. Shapiro. Su definición es bastante natural para un algebrista:

$$d(a,b)=\begin{cases}0 & \text{si } a=b\\ \dfrac{1}{\min\{n\in N:a(n)\neq b(n)\}} & \text{si } a\neq b\end{cases} \tag{1.2}$$

Esta métrica interactúa fuertemente con las propiedades algebraicas del anillo, dado que para toda terna a, b, c de elementos de $\mathcal{A}(\mathbb{C})$ se verifica $d(a+c,b+c)=d(a,b)$ y $d(a*c,b*c)=d(a,b)$. Observe que con esta distancia, $\mathcal{A}(\mathbb{C})$ es

un espacio métrico acotado y se puede probar fácilmente que las operaciones del anillo son continuas (es decir: respecto de esta distancia, $\mathcal{A}(\mathbb{C})$es un anillo topológico). Entre otras propiedades topológicas, podemos mencionar:

1. el producto $(t,a) \mapsto ta$ de elementos $a \in \mathcal{A}(\mathbb{C})$ por escalares complejos t, no es continuo (por lo tanto la estructura de álgebra compleja de $\mathcal{A}(\mathbb{C})$ no es relevante para esta topología).
2. cada elemento $a \in \mathcal{A}(\mathbb{C})$ es un punto de acumulación.
3. los únicos conexos no vacíos son los conjuntos con un solo elemento.
4. para cada entero positivo n, la bola

$$B\left(0;\frac{1}{n}\right)=\left\{a \in \mathcal{A}(\mathbb{C}): \ d(a,0)<\frac{1}{n}\right\}$$

es un ideal, al igual que su clausura. En particular para $n = 1$, $B(0;1)$es el ideal maximal y su clausura topológica es todo el anillo. Es fácil de probar que el grupo de inversibles es exactamente la esfera $\{a \in \mathcal{A}(\mathbb{C}) : d(a,0) = 1\}$.

5. para $n \geq 2$, $B\left(0;\frac{1}{n}\right)$ es cerrada y su clausura es abierta.
6. para cada entero positivo n, la función $\mathcal{A}(\mathbb{C}) \to \mathbb{C}$, es $a \mapsto a(n)$ continua.
7. $\mathcal{A}(\mathbb{C})$ es un espacio métrico completo no compacto ni localmente compacto.
8. el grupo $\mathcal{A}(\mathbb{C})^{x}$ no es compacto ni localmente compacto y no es discreto, por lo tanto no es un grupo topológico profinito.

Shapiro estudia las derivaciones en el anillo $\mathcal{A}(\mathbb{C})$ utilizando, entre otras herramientas, la siguiente propiedad: todo elemento $a \in \mathcal{A}(\mathbb{C})$ admite la expresión $a \sum_{n=1}^{\infty} a(n)e_n$

donde para cada entero positivo n, $e_n(n)=1$ y $e_n(k)=0$ para todo

$k \neq n$ y la serie converge en el sentido de la métrica d, es decir:

$$ {}_{k}\underrightarrow{Lim}_{\infty}\ d\left(a, \sum_{n=1}^{k} a(n)e_n\right) = 0 $$

Hemos resumido muy brevemente algunas de las propiedades algebraicas y topológicas de este anillo. Pero no podemos dejar de mencionar que la estructura de este anillo merece una investigación más profunda. Por ejemplo, el álgebra de Lie (de dimensión infinita) de las derivaciones en $\mathcal{A}(\mathbb{C})$ parece tener una estructura muy interesante y no ha sido estudiada aún, hasta donde tenemos conocimiento. Tampoco hemos visto en la literatura ninguna mención a ciertos aspectos homológicos, como por ejemplo el funtor representable $R \mapsto \mathcal{A}_1^{x}(R)$ y la correspondiente álgebra de Hopf (R es cualquier álgebra conmutativa con unidad sobre un cuerpo de característica 0).

En las dos secciones siguientes presentaremos y demostraremos dos resultados originales, el primero referido a una acción del grupo infinito de permutaciones en el anillo $\mathcal{A}(\mathbb{C})$ y el segundo sobre dos teoremas de factorización de unidades. En la última sección cerraremos el trabajo con aplicaciones a la factorización de series de Bell y de series de Fourier fuertemente convergentes.

La acción primaria del grupo $S(\infty)$

El grupo $S(\infty)$ es el límite directo de los grupos simétricos S_n, es decir, es el grupo de permutaciones de soporte finito en un conjunto infinito numerable. Este grupo ha sido objeto de estudio intensivo en los últimos decenios –ver, por ejemplo, Okounkov, A. Yu. (1994)– y nosotros utilizaremos una versión adaptada a nuestros propósitos, que es el grupo de permutaciones de soporte finito del conjunto $P \subset \mathbb{N}$ de números primos, con el orden inducido por el de los enteros positivos. Utilizaremos la notación $S(P)$ para este grupo, es decir, el de las

permutaciones $\gamma: \mathbb{P} \to \mathbb{P}$ de soporte finito. Este grupo actúa en $\mathbb{N}$ de la siguiente manera: dada $\gamma \in S(\mathbb{P})$ definimos $\gamma.1=1$, y para cada $n \geq 2$, siendo $n=\prod_{p \in \mathbb{P}} p^{v_p(n)}$ su descomposición en factores primos (es un producto finito), definimos:

$$\gamma . n=\prod_{p \in \mathbb{P}} \gamma(p)^{v_p(n)} \tag{2.1}$$

La comprobación de que se trata, efectivamente, de una acción de $S(\mathbb{P})$ en $\mathbb{N}$ es inmediata. Indicando con $S_{\mathbb{N}}$ el grupo de permutaciones en $\mathbb{N}$ (de soporte finito o no), lo que tenemos es un monomorfismo de grupos $S(\mathbb{P}) \xrightarrow{\theta} S_{\mathbb{N}}$ $\gamma \mapsto \theta_{-} \gamma: n \mapsto \gamma . n$. Este monomorfismo tiene la interesante propiedad que ningún elemento de su imagen (excepto la identidad) tiene soporte finito. Obsérvese que para cada $\gamma \in S(\mathbb{P})$ se tiene el elemento $\alpha_{-} \gamma \in \mathbb{A}(\mathbb{C})$ definido por $\alpha_{-} \gamma \ (n)=\gamma . n$ para todo $n \in \mathbb{N}$. Estas funciones son fuertemente multiplicativas, es decir: para todos m y n en $\mathbb{N}$ tenemos que $\alpha_{\gamma}(mn)=\alpha_{\gamma}(m) \alpha_{\gamma}(n)$. La razón es muy sencilla:

$$\gamma .(mn)=\prod_{p \in \mathbb{P}} \gamma(p)^{v_p(mn)}=\prod_{p \in \mathbb{P}} \gamma(p)^{v_p(m)+\ v_p(n)}=$$

$$=\left(\prod_{p \in \mathbb{P}} \gamma(p)^{v_p(m)}\right)\left(\prod_{p \in \mathbb{P}} \gamma(p)^{v_p(n)}\right)=(\gamma . m)(\gamma . n) \tag{2.2}$$

Ahora, la acción (2.1) se transfiere al anillo $\mathbb{A}(\mathbb{C})$ de manera natural: para cada $\gamma \in S(\mathbb{P})$ y cada $a \in \mathbb{A}(\mathbb{C})$:

$$\forall n \in \mathbb{N}: a^{\gamma}(n)=a(\gamma . n) \tag{2.3}$$

Obsérvese que, efectivamente, para cada par de elementos $\gamma, \sigma \in S(\mathbb{P}): ((a^{\gamma})^{\sigma})(n)=(a^{\gamma})(\sigma . n)=a(\gamma .(\sigma . n))=a((\gamma \circ \sigma) . n)=(a^{(\gamma \circ \sigma)})(n)$. Lo notable de esta acción es que es compatible con las operaciones del anillo, y además es continua (para la topología ultramétrica).

Proposición:

i. Para cada par de elementos a y b en $\mathcal{A}(\mathbb{C})$ y cada $\gamma \in S(P)$: $(a+b)^{\gamma} = a^{\gamma} + b^{\gamma}$ y $(a*b)^{\gamma} = a^{\gamma} * b^{\gamma}$. Es decir: la aplicación $\Theta_{\gamma}: \mathcal{A}(\mathbb{C}) \to \mathcal{A}(\mathbb{C})$ tal que $\Theta_{\gamma}(a) = a^{\gamma}$ es un automorfismo en el anillo $\mathcal{A}(\mathbb{C})$.

ii. Para cada $\gamma \in S(P)$, el automorfismo Θ_{γ} es continuo (respecto de la distancia (1.2)).

Demostración:

La identidad $(a+b)^{\gamma} = a^{\gamma} + b^{\gamma}$ se deduce trivialmente de la definición de la suma en el anillo $\mathcal{A}(\mathbb{C})$. Ahora, para cada n:

$$(a^{\gamma} * b^{\gamma})(n) = \sum_{(hk=n)} a^{\gamma}(h) b^{\gamma}(k) = \sum_{(hk=n)} a(\gamma.h) b(\gamma.k) = \sum_{\substack{l=\gamma.h \\ m=\gamma.k}} a(l) b(m) \overset{(2.2)}{=}$$

$$\sum_{(\gamma^{-1}.l)(\gamma^{-1}.m)=n} a(l) b(m) = \sum_{\gamma^{-1}(lm)=n} a(l) b(m) = \sum_{lm=\gamma.n} a(l) b(m) = (a*b)(\gamma*n) = (a*b)^{\gamma}(n)$$

Probemos la continuidad de Θ_{γ}: dados $a \in \mathcal{A}$, y $\varepsilon > 0$, sea $m \in \mathbb{N}$ t al que $m > \frac{1}{\varepsilon}$. Eligiendo

$$\delta = \frac{1}{max\{\gamma.1=1, \gamma.2, \ldots, \gamma.m\}}$$ se tiene (para cualquier $b \neq a$):

$$d(a,b) < \delta \Rightarrow min\{n \in \mathbb{N} : a(n) \neq b(n)\} > max\{1, \gamma.2, \ldots, \gamma.m\} \Rightarrow$$

$$b(1) - a(1) = 0, \ldots, b(\gamma.m) - a(\gamma.m) = 0 \Rightarrow$$

$$\Rightarrow b^{\gamma}(1) - a^{\gamma}(1) = 0, \ldots, b^{\gamma}(m) - a^{\gamma}(m) = 0 \Rightarrow$$

$$\Rightarrow min\{n \in \mathbb{N} : a^{\gamma}(n) \neq b^{\gamma}(n)\} > m \Rightarrow d(a^{\gamma}, b^{\gamma}) < (1/m) < \epsilon$$

Es decir: θ_γ es continua en a. □

Es fácil comprobar que el homomorfismo de grupos $S(P) \xrightarrow{\theta} Aut(\mathcal{A}(\mathbb{C}))$ es inyectivo: sea $I_{\mathbb{N}}$ la identidad en $\mathbb{N}$; entonces $\theta_\gamma\ (I_{\mathbb{N}}) = I_{\mathbb{N}}{}^{\gamma} = I_{\mathbb{N}} \Leftrightarrow$ para todo $n \in \mathbb{N}$: $\gamma . n = n \Rightarrow$ para todo primo $p : \gamma(p) = p$, es decir: $\gamma = 1_{(S(P))}$. Tenemos, entonces, el subanillo $\mathcal{A}(\mathbb{C})^{S(P)}$ de invariantes y los subgrupos $\mathcal{A}(\mathbb{C})^{x^{S(P)}}$, $\mathcal{A}(\mathbb{C})_1{}^{x^{S(P)}}$ del grupo de unidades. El anillo de invariantes contiene funciones muy importantes para la teoría de números, como por ejemplo la función de Möbius y la de Liouville. Dado que este anillo es isomorfo al anillo de funciones $\mathbb{N}/(\mathrm{S}(P)) \to \mathbb{C}$, la clasificación de los elementos invariantes puede llevarse a cabo a partir del estudio del cociente $\mathbb{N}/(\mathrm{S}(P))$. Este estudio puede encararse desde un punto de vista combinatorio y las órbitas quedan identificadas mediante objetos similares a los diagramas de Young. Insistimos en que no hemos encontrado ninguna mención a esta acción del grupo $S(\infty) \cong S(P)$ en la literatura existente hasta el momento. Ahora, dado que $\mathcal{A}(\mathbb{C})$ es un dominio de integridad, la acción pasa naturalmente al cuerpo de cocientes $Q\ (\mathcal{A}(\mathbb{C}))$ y se tiene la inclusión obvia $Q\ (\mathcal{A}(\mathbb{C})^{S(P)}) \subset Q\ \ (\mathcal{A}(\mathbb{C}))^{S(P)}$. Un problema interesante para investigar es esta extensión de cuerpos, y para ello puede ser útil el resultado que presentamos en el siguiente párrafo.

La factorización *MB*

Hemos mencionado que el anillo $\mathcal{A}(\mathbb{C})$ es de factorización única. En general, esta propiedad es una herramienta decisiva para el estudio de la estructura de un anillo, pero la desventaja que tenemos en este caso es que cada elemento primo de $\mathcal{A}(\mathbb{C})$ tiene demasiados asociados, pues el grupo de unidades $\mathcal{A}(\mathbb{C})^{\mathrm{x}}$ es "muy grande". Nosotros hemos descubierto una factorización única de estas unidades que pasamos a describir y demostrar. Observemos en primer lugar que alcanza con factorizar los elementos de $\mathcal{A}(\mathbb{C})_1{}^{\mathrm{x}}$, pues para cada $a \in \mathcal{A}(\mathbb{C})^x$ tenemos que

$\frac{1}{a(1)}$ $a \in \mathcal{A}\ (\mathbb{C})_1^{\times}$

En el caso en que $a(1) = 1$, las fórmulas para el elemento inverso se simplifican un poco:

$$(1)\ a^{*-1}(1) = 1$$

$$(n)a^{*-1}(n) = -\sum_{\substack{d|n \\ d<n}} a\left(\frac{n}{d}\right) a^{*-1}(d) \qquad (3.1)$$

Para aliviar un poco la escritura, escribiremos $\mathcal{A}_1^{\times}$ en lugar de $\mathcal{A}(\mathbb{C})_1^{\times}$. Consideremos los siguientes subconjuntos de $\mathcal{A}_1^{\times}$: $(M.1)\ M_1 \subset \mathcal{A}_1^{\times}$ es el conjunto de las funciones $a \in \mathcal{A}_1^{\times}$ fuertemente multiplicativas, es decir $a(1) = 1$ y $a(mn) = a(m)\, a(n)$: y para todo par de naturales m y n.

Observación 3.1: Recordemos que las funciones multiplicativas son aquellas que verifican $a(mn) = a(m)\, a(m)$ para todo par de naturales coprimos m y n; el producto de $a * b$ dos funciones multiplicativas es multiplicativa, pero esto no ocurre con las fuertemente multiplicativas. Por lo tanto, M_1 no es cerrado sobre el producto.

$(M.2)\ M_2 \subset \mathcal{A}_1^{\times}$ es el conjunto de las funciones "fuertemente multiplicativas en cuadrados" y que se anulan en los no-cuadrados, es decir: (*i*) $a(1) = 1$, (*ii*) $a(n) = 0$ si $n \geq 2$ no es un cuadrado y (*iii*) $a(m^2\ n^2) = a(m^2)\, a(n^2)$ para todo par de naturales m y n.

En general, para cada entero $k \geq 2$ definimos

$$(M.k)\, a \in M_k \Leftrightarrow \begin{cases} a(1) = 1 \\ n \notin \{m^k : m \in \mathbb{N}, m \geq 2\} \Rightarrow a(n) = 0 \\ a(m^k n^k) = a(m^k)\ a(n^k) \text{ para } m, n \in \mathbb{N} \end{cases}$$

Estos conjuntos no son subgrupos de $\mathcal{A}_1^x$, pues no son cerrados sobre el producto. Obsérvese que todos ellos contienen a la unidad e_1. La siguiente familia de subconjuntos es una familia decreciente de subgrupos de $\mathcal{A}_1^x$:

(*B*.1) $B_1=\{a\in\mathcal{A}_1^x/\forall p\in P: a(p)=0\}$

(*B*.2) $B_2=\{a\in\mathcal{A}_1^x/\forall p\in P: a(p)=a(p^2)=0\}$

En general, para cada entero positivo k:

(*B*.k) $B_k==\{a\in\mathcal{A}_1^x/\forall p\in P: a(p)=(p^2)=a(p^3)=\ldots.=a(p^k)=0\}$

La comprobación de que los B_k son subgrupos de $\mathcal{A}_1^x$ es bastante sencillo. En primer lugar, es evidente que $e_1\in B_k$ para todo k. Ahora, dadas a y b en B_k, para todo primo p y todo exponente $i\in\{1,2,3,\ldots,k\}$

$$(a*b)(p^i)=\sum_{d/p^i} a(d)\,b(p^i/d)=\sum_{j=0}^{i} a(p^j)\,b(p^{i-j})=$$

$$=\overbrace{a(1)}^{=1}\overbrace{b(p^j)}^{=0}+\sum_{j=1}^{i-1}a(p^j)\overbrace{b(p^{i-j})}^{=0}+\overbrace{a(p^i)}^{=0}\overbrace{b(1)}^{=1}=0$$

Finalmente, dada $a\,B_k$, para todo primo p y todo exponente $i\in\{1,2,3,\ldots,k\}$, de (3.1) tenemos

$$a^{*-1}(p^i)=-\sum_{\substack{d/p^i\\ d<p^i}} a(p^i/d)\,a^{*-1}(d)=\sum_{j=0}^{i-1} a(p^j)\,a^{*-1}(p^{i-j})=-a(1)a$$

$$=-a(1)\,a^{*-1}(p^i)+\sum_{j=1}^{i-1}\overbrace{a(p^j)}^{=0}\;a^{*-1}(p^{i-j})=-a^{*-1}(p^i)$$

Es decir, $a^{*-1}(p^i)=0$.

La primera propiedad importante de estos conjuntos está relacionada con la acción primaria.

LEMA 3. 1: Los conjuntos M_k y los grupos B_k son S(P)- estables.

Demostración:

(*a*) Sean $a\in M_k$ y $\gamma\in S(P)$. En primer lugar, $a^{\gamma}(1)=a(\gamma.1)=a(1)=1$.

Ahora, para cada $n>1$, n es una potencia k-ésima de algún $m=\prod_p p^{v_p(m)}$ sii $n=\prod_p p^{kv_p(m)}$ sii $\gamma.n=\prod_p \gamma(p)^{kv_p(m)}=(\gamma.m)^k$. Es decir: n no es una potencia k-ésima sii $\gamma.n$ ino es una potencia k-ésima. Por lo tanto, $a^{\gamma}(n)=a(\gamma.n)=0$ si n no es una potencia k-ésima.

Finalmente:

$$a^{\gamma}(m^k n^k)=a^{\gamma}(\prod_p p^{kv_p(m)+kv_p(n)})=a(\prod_p \gamma(p)^{kv_p(m)+kv_p(n)})=$$

$$=a((\gamma.m)^k(\gamma.n)^k)$$

$$=a((\gamma.m)^k)a((\gamma.n)^k)=a(\gamma.(m^k))a(\gamma.(n^k))=a^{\gamma}(m^k)a^{\gamma}(n^k)$$

(*b*) La estabilidad de cada B_k es más sencilla aún de probar: sean y . Entonces, para cada $i\in\{1,2,3,\ldots,k\}$: $b^{\gamma}(p^i)=$ b($\gamma.(p^i)$)=$b((\gamma(p))i)=0$ □

Ahora, presentamos los dos resultados principales (y originales) de este trabajo.

TEOREMA 3.1: Para cada $a\in\mathcal{A}_1^{x}$ y cada entero positivo k, existe una única secuencia $(\hat{a}_1,\hat{a}_2,\ldots,\hat{a}_k)\in M_1\times M_2\times\ldots\times M_k$ y un único $a''_k\in B_k$ tales que:

$$a=\hat{a}_1*\hat{a}_2*\ldots*\hat{a}_k*a''_k \qquad (3.2)$$

Demostración: Probaremos primero la existencia de la secuencia del enunciado mediante inducción sobre k.

(1) $k=1$: Dada $a\in\mathcal{A}_1^{x}$, necesitamos encontrar un elemento $\hat{a}_1\in\mathcal{A}_1^{x}$ fuertemente multiplicativo y un elemento $a''_1\in\mathcal{A}_1^{x}$ que se anula en los primos y tales que $a=\hat{a}_1*a''_k$. Para esto, consideremos la aplicación $\Theta_1:\mathcal{A}_1^{x}\to\mathcal{A}_1^{x}$ tal que:

$$\Theta_1(a)(1)=a(1)=1$$

$$\Theta_1(a)(\overbrace{\prod_p p^{v_p(n)}}^{n>1})\overset{def}{=}\prod_p a(p)^{v_p(n)} \qquad (3.3)$$

Esta aplicación verifica:

(*i*) $a \in \mathcal{A}_1^{\times}$ es fuertemente multiplicativa sii $\Theta_1(a)=a$. La verificación es bastante sencilla: si a es fuertemente multiplicativa entonces $a(\overbrace{\prod_p p^{v_p(n)}}^{n>1})=\prod_p a(p)^{v_p(n)}$ para todo $n > 1$. La recíproca se deduce de la siguiente propiedad:

(*ii*) Para toda $a \in \mathcal{A}_1^{\times}$, $\Theta_1(a)$ es fuertemente multiplicativa:

$$\Theta_1(a)(\overbrace{\prod_p p^{v_p(n)+v_p(m)}}^{mn})=\prod_p a(p)^{v_p(n)+v_p(m)}=(\prod_p a(p)^{v_p(n)})(\prod_p a(p)^{v_p(m)})=$$

$$\Theta_1(a)(n)\,\Theta_1(a)(m)$$

De estas dos propiedades se deduce:

(*iii*) $\Theta_1 \circ \Theta_1 = \Theta_1$ y $\Theta_1(\mathcal{A}_1^{\times})=M_1$.

Ahora, definimos $\hat{a}_1=\Theta_1(a)$ and $a''_1=\hat{a}_1^{*-1}*a$. Como $\hat{a}_1$ es fuertemente multiplicativa, su inversa es $\hat{a}_1^{*-1}=\mu\,\hat{a}_1$, pues

$$(\hat{a}_1*(\mu\hat{a}_1))(n)=\sum_{d|n}\overbrace{\hat{a}_1(n/d)\,\hat{a}_1(d)}^{=\hat{a}1(n)1}\mu(d)=\hat{a}_1(n)(1*\mu)(n)=$$
$$=\hat{a}_1(n)e_1(n)\overset{\hat{a}_1(1)=1}{=}e_1(n)$$

Pero para entender mejor el paso siguiente es preferible prescindir de esta fórmula, que por otra parte no es realmente necesaria para lo que sigue.

Ahora, debemos probar que $a''_1(p)$ para todo primo p (recordemos que $\mathcal{A}_1^{\times}$ es cerrado sobre el producto, por lo tanto tenemos garantizada la igualdad $a''_1(1)=1$). Veamos:

$$\hat{a}_1^{*-1}(p)=\sum_{\substack{d|p\\ d<p}}\hat{a}_1(p/d)\,\hat{a}_1^{*-1}(d)=\hat{a}_1(p)\,\hat{a}_1^{*-1}(1)=-\hat{a}_1(p)\overset{(3.3)}{=}-a(p)$$

Por lo tanto:

$$a''_1(p)=(\hat{a}_1^{*-1}*a)(p)=\hat{a}_1^{*-1}(p)a(1)+\hat{a}_1^{*-1}(1)\,a(p)=\hat{a}_1^{*-1}(p)+a(p)=$$

$$=-a(p)+a(p)=0$$

(2): $k \to k+1$: Supongamos (hipótesis inductiva) que $a = \hat{a}_1 * \hat{a}_2 * \ldots * \hat{a}_k * a''_k$, donde $(\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_k, a''_k) \in M_1 \times M_2 \times \ldots \times M_k \times B_k$. La idea natural, ahora, es factorizar $a''_k = \hat{a}_{k+1} * a''_{k+1}$, con $\hat{a}_{k+1} \in M_{k+1}$ y $a''_{k+1} \in B_{k+1}$. Definamos $\Theta_{k+1}: \mathcal{A}_1^{\times} \to \mathcal{A}_1^{\times}$ tal que

$\Theta_{k+1}(b)(1) = b(1) = 1$

$\Theta_{k+1}(b)(n) = 0$ si $n \geq 2$ no es una potencia $k+1$-ésima (3.4)

$$\Theta_{k+1}(b)\Big(\overbrace{\prod_p p^{(k+1)v_p(n)}}^{n^{k+1}>1}\Big) \stackrel{def}{=} \prod_p b(p^{k+1})^{v_p(n)}$$

Entonces:

(i) $b \in M_{(k+1)} \Leftrightarrow \Theta_{(k+1)}(b) = b$: en primer lugar, si $b \in M_{(k+1)}$, entonces

$b(1) = 1$

$b(n) = 0$ si $n \geq 2$ no es una potencia $k+1$-ésima

y $$b\Big(\overbrace{\prod_p p^{(k+1)v_p(n)}}^{n^{k+1}>1}\Big) = \prod_p b(p^{k+1})^{v_p(n)}$$

(pues b es multiplicativa en potencias (k+1)-ésimas). De (3.4) se deduce que $\Theta_{k+1}(b) = b$

La recíproca se deduce de la propiedad siguiente.

(ii) Para toda $b \in B_k$: $\Theta_{k+1}(b) \in M_{k+1}$: es consecuencia inmediata de (3.4).

(iii) $\Theta_{k+1} \circ \Theta_{k+1} = \Theta_{k+1}$ y $\Theta_{k+1}(B_k) = M_{k+1}$: es consecuencia inmediata de (i) y (ii).

Ahora, definimos $\hat{a}_{k+1} = \Theta_{k+1}(a''_k) \in M_{k+1}$ y $a''_{k+1} = \hat{a}_{k+1}^{*-1} * a''_k$. Lo que nos queda por probar es que $a''_{k+1}(p) = a''_{k+1}(p^2) = \ldots = a''_{k+1}(p^{k+1}) = 0$ para todo primo p (recordemos que $a''_1(1) = 1$ es automático). Para cada $i \in \{1, 2, \ldots, k\}$:

$$\hat{a}_{k+1}^{*-1}(p^i) = -\sum_{\substack{d \mid p^i \\ d < p^i}} \hat{a}_{k+1}(p^i/d)\, \hat{a}_{k+1}^{*-1}(d) = \sum_{j=0}^{i-1} \overbrace{\hat{a}_{k+1}(p^{i-j})\, \hat{a}_{k+1}^{*-1}(p^j)}^{=0} = 0$$

Para la potencia (k+1)-ésima:

$$\hat{a}_{k+1}^{*-1}(p^{k+1}) = -\sum_{\substack{d|p^{k+1}_{k+1} \\ d<p^{k+1}_{k+1}}} \hat{a}_{k+1}((p^{k+1})/d)\ \hat{a}_{k+1}^{*-1}(d) =$$

$$= -\hat{a}_{k+1}(p^{k+1})\ \overbrace{\hat{a}_{k+1}^{*-1}(1)}^{1} + \sum_{j=1}^{k-1} \overbrace{\hat{a}_{k+1}(p^{k+1-j})}^{=0} \hat{a}_{k+1}^{*-1}(p^j) = -\hat{a}_{k+1}(p^{k+1}) \overset{(3.4)}{=} -a''_k(p^{k+1})$$

Por lo tanto, para cada $i \in \{1, 2, \ldots, k\}$:

$$a''_{k+1}(p^i) = (\hat{a}_{k+1}^{*-1} * a''_k)(p^i) = \sum_{j=0}^{i-1} \overbrace{\hat{a}_{k+1}^{*-1}(p^{i-j})}^{0} a''_k(p^j) + \hat{a}_{k+1}^{*-1}(1)\ \overbrace{a''_k(p^i)}^{0} = 0$$

Finalmente:

$$a''_{k+1}(p^{k+1}) = (a_{k+1}^{*-1} * a''_k)(p^{k+1}) =$$

$$= \overbrace{\hat{a}_{k+1}^{*-1}(p^{k+1})}^{-a''_k(p^{k+1})} \overbrace{a''_k(1)}^{1} + \sum_{j=1}^{k-1} \overbrace{\hat{a}_{k+1}^{*-1}(p^{k+1-j})}^{0} a''_k(p^j) + \overbrace{\hat{a}_{k+1}^{*-1}(1)}^{1}\ a''_{k+1}(p^{k+1}) = 0$$

Ahora, nos queda por probar la unicidad de la factorización, para lo cual supongamos, en primer lugar, que $a = a_1 * b_1 = \tilde{a}_1 * \tilde{b}_1$, donde $a_1, \tilde{a}_1 \in M_1$ y $b_1, \tilde{b}_1 \in B_1$. Entonces, para todo primo p:

$$0 = (a_1 * b_1)(p) - (\tilde{a}_1 * \tilde{b}_1)(p) = a_1 \overbrace{(p) b_1(1)}^{1} + \overbrace{a_1(1) b_1(p)}^{1}$$

$$- \tilde{a}_1(p) \overbrace{\tilde{b}_1(1)}^{1} - \overbrace{\tilde{a}_1(1) \tilde{b}_1(p)}^{1}$$

Es decir: $a_1(p) = \tilde{a}_1(p)$. Pero $a_1, \tilde{a}_1 \in M_1$ quedan determinadas por su valores en los primos (pues son fuertemente multiplicativas), por lo tanto $a_1 = \tilde{a}_1$. Ahora, de $a_1 * b_1 = \tilde{a}_1 * \tilde{b}_1$ y la inversibilidad de a_1 se deduce que también $b_1 = \tilde{b}_1$.
Ahora, sea $k \geq 2$. Tenemos que probar:

$$\left.\begin{array}{l} a_1 * a_2 * \ldots * a_k * b_k = \tilde{a}_1 * \tilde{a}_2 * \ldots * \tilde{a}_k * \tilde{b}_k \\ (a_1, a_2, \ldots, a_k, b_k) \in M_1 \times M_2 \times \ldots \times M_k \times B_k \\ (\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_k, \tilde{b}_k) \in M_1 \times M_2 \times \ldots \times M_k \times B_k \end{array}\right\} \Rightarrow a_i = \tilde{a}_i, i = 1, k \text{ y } b_k = \tilde{b}_k \qquad (3.5)$$

Lo haremos en un par de pasos.

(1) Par cada primo p:

$$a_1(p)=(a_1*a_2*\ldots*a_k*b_k)(p)= (\tilde{a}_1*\tilde{a}_2*\ldots*\tilde{a}_k*\tilde{b}_k)(p)= \tilde{a}_1(p) \qquad (3.6)$$

Para demostrar (3.6), probemos primero que $a_1(p)=(a_1*a_2*\ldots*a_k)(p)$: Si $k = 1$, esto es trivial. Ahora supongamos que $k\geq 2$ y que (hipótesis inductiva) $(a_1*a_2*\ldots*a_{k-1})(p)= a_1(p)$. Entonces:

$$(a_1*a_2*\ldots*a_k)(p)=(a_1*a_2*\ldots*a_{k-1})(p)\overbrace{a_k(1)}^{1}+\overbrace{(a_1*a_2*\ldots*a_{k-1})(1)}^{1}\overbrace{a_k(p)}^{0}=$$

$$= (a_1*a_2*\ldots*a_{k-1})(p)=a_1(p) \text{ (por hipótesis inductiva)}$$

[$a_k(p)=0$ pues el primo p no puede ser una potencia k-ésima cuando $k\geq 2$].

Finalmente, si $k = 1$ $(a_1* b_1)(p)=a_1(p)\overbrace{b_1(1)}^{1}+\overbrace{a_1(1)}^{1}\overbrace{b_1(p)}^{0}= a_1(p)$; para $k\geq 2$:

$$(a_1*a_2*\ldots*a_k*b_k)(p)=(a_1*a_2*\ldots*a_k)(p)\overbrace{b_k(1)}^{1}+\overbrace{(a_1*a_2*\ldots*a_k)(1)}^{1}\overbrace{b_k(p)}^{0}$$
$$= a_1(p)$$

Obviamente, también tenemos que $(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_k,\tilde{b}_k)(p)= \tilde{a}_1(p)$ y la igualdad (3.6) queda probada.

Ahora, como a_1 y $\tilde{a}_1$ son fuertemente multiplicativas, si se verifica $a_1(p) = \tilde{a}_1(p)$ para cada primo p, entonces $a_1(n) = \tilde{a}_1(n)$ para todo $n\geq 2$. Por otra parte, $a_1= \tilde{a}_1$ es inversible, por lo tanto, de la hipótesis $a_1*a_2*\ldots*a_k*b_k = \tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_k,\tilde{b}_k$ se deduce que $a_2*a_3*\ldots*a_k*b_k = \tilde{a}_2,\tilde{a}_3,\ldots,\tilde{a}_k,\tilde{b}_k$ (3.7)

(2) Ahora, supongamos que $k\geq 2$ y probemos que $a_2(p^2)=(a_2*a_3*\ldots*a_k)(p^2)$ para cualquier primo p. Si $k = 2$, esto es trivial. Supongamos ahora que $k\geq 3$ (hipótesis indductiva), $a_2(p^2)=(a_2*a_3*\ldots*a_{k-1})(p^2)$. Entonces:

$$(a_2*a_3*\ldots*a_k)(p^2)=$$

$$=(a_2*a_3*\ldots*a_{k-1})(p^2)\overbrace{a_k(1)}^{1}+(a_2*a_3*\ldots*a_{k-1})(p)\overbrace{a_k(p)}^{0}+$$

$$\overbrace{(a_2*a_3*\ldots*a_{k-1})(1)}^{1}\overbrace{a_k(p^2)}^{0}=(a_2*a_3*\ldots*a_{k-1})(p^2)=a_2(p^2)$$

(por hipótesis inductiva)

[obsérvese que $a_k(p)=a_k(p^2)=0$, pues ni el primo p ni su cuadrado p^2 pueden ser potencias k-ésimas cuando $k\geq 3$].

Finalmente, si

$$k=2\ (a_2*b_2)(p^2)=a_2(p^2)\overbrace{b_2(1)}^{1}+\overbrace{a_2(p)}^{0}\overbrace{b_2(p)}^{0}+a_2(1)\overbrace{b_2(p^2)}^{0}=a_2(p^2);$$

y si $k\geq 3$:

$$(a_2*a_3*\ldots*a_k*b_k)(p^2)=$$

$$=(a_2*a_3*\ldots*a_k)(p^2)\overbrace{b_k(1)}^{1}+(a_2*a_3*\ldots*a_k)(p)\overbrace{b_k(p)}^{0}+(a_2*\ldots*a_k)$$

$$(1)\overbrace{b_k(p^2)}^{0}=a_2(p^2)$$

Obviamente también tenemos que $(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_k,\tilde{b}_k)(p^2)=\tilde{a}_2(p^2)$. Entonces, de (3.7) resulta que $a_2(p^2)=\tilde{a}_2(p^2)$. Pero $a_2(1)=\tilde{a}_2(1)$ y a_2, $\tilde{a}_2$ son fuertemente multiplicativas en cuadrados, por lo tanto $a_2=\tilde{a}_2$. De (3.7) resulta entonces, si $k\geq 3$:

$$a_3*a_4*\ldots*a_k*b_k=\tilde{a}_3,\tilde{a}_4,\ldots,\tilde{a}_k,\tilde{b}_k \tag{3.8}$$

Ahora, supongamos que $k\geq 3$ y que

$$a_j*a_{j+1}*\ldots*a_k*b_k=\tilde{a}_j,\tilde{a}_{j+1},\ldots,\tilde{a}_k,\tilde{b}_k \tag{3.9}$$

para algún $j<k$. Probemos primero que $(a_j*a_{j+1}*\ldots*a_k)(p^j)=a_j(p^j)$:

$$(a_j*a_{j+1}*\ldots*a_k)(p^j)=(a_j*a_{j+1}*\ldots*a_{k-1})(p^j)\overbrace{a_k(1)}^{1}+\sum_{i=1}^{i}(a_j*a_{j-1}*\ldots*a_{k-1})$$

$$(p^{j-i})\overbrace{a_k(p^i)}^{0}$$

[$a_k(p)=a_k(p^2)=\ldots=a_k(p^j)=0$, pues ni el primo p ni $p^2,p^3,\ldots,p^j$ sus potencias pueden ser potencias k-ésimas cuando $j<k$]

Es decir: $(a_j * a_{j+1} * \ldots * a_k)(p^j) = (a_j * a_{j+1} * \ldots * a_{k-1})(p^j)$. Si $k=j+1$, ya hemos probado lo que queríamos. Si $k > j+1$, el mismo procedimiento anterior permite afirmar que

$$(a_j * a_{j+1} * \ldots * a_k)(p^j) = (a_j * a_{j+1} * \ldots * a_{k-1})(p^j) = (a_j * a_{j+1} * \ldots * a_{k-2})(p^j)$$

Podemos continuar reduciendo los factores («inducción inversa») hasta llegar al resultado deseado: $(a_j * a_{j+1} * \ldots * a_k)(p^j) = a_j(p^j)$. Obsérvese que esta igualdad es trivial si $j = k$. Ahora, si $1 \leq j \leq k$:

$$(a_j * a_{j+1} * \ldots * a_k\, b_k)(p^j) =$$

$$= (a_j * a_{j+1} * \ldots * a_k)(p^j)\overbrace{b_k(1)}^{1} + \sum_{i=1}^{j} (a_j * a_{j+1} * \ldots * a_k)(p^{j-i})\overbrace{b_k(p^i)}^{0}$$

$$(a_j * a_{j+1} * \ldots * a_k)(p^j) = a_j(p^j)$$

[obsérvese que $b_k(p) = b_k(p^2) = \ldots = b_k(p^j) = 0$ pues $1 \leq j \leq k$]

El mismo resultado se obtiene para la segunda secuencia y entonces, para todo j tal que $1 \leq j \leq k$ se verifica, para cualquier primo p:

$$a_j(p^j) = (a_j * a_{j+1} * \ldots * a_k\, b_k)(p^j) = (\tilde{a}_j, \tilde{a}_{j+1}, \ldots, \tilde{a}_k, \tilde{b}_k)(p^j) = \tilde{a}_j(p^j)$$

Ahora, $a_j(1) = \tilde{a}_j(1) = 1$ y a_j, $\tilde{a}_j$ ambas son fuertemente multiplicativas en potencias j-ésimas, por lo tanto $a_j = \tilde{a}_j$ para todo j tal que $1 \leq j \leq k$. De (3.9) se deduce entonces que también $b_k = \tilde{b}_k$ y la unicidad queda probada. □

COROLARIO 3.1 (de la demostración) Sea $(a_1 * a_2 * \ldots * a_k * b_k) \in M_1 \times M_2 \times \ldots \times M_k \times B_k$. Entonces para todo primo p y cada $j \in \{1, 2, \ldots, k\}$: $(a_j * a_{j+1} * \ldots * a_k * b_k)(p^j) = a_j(p^j)$. □

***Nota* 3.1:** Un aspecto importante de esta factorización es que cada factor $\hat{a}_i$ es fuertemente multiplicativo en las potencias

i-ésimas y por lo tanto queda determinado por sus valores en las correspondientes potencias de primos, mientras que el factor a''_k se anula en dichas potencias. Es decir: (3.2) exhibe el comportamiento de a en las potencias de los números primos mediante funciones multiplicativas; en este sentido, podemos decir que, cuanto mayor es k, se obtiene una "mejor aproximación", pues el factor a''_k, a medida que k crece, es cada vez más cercano a la unidad e_1: para todo primo p y todo $i \in \{0,1,2,\ldots,k\}: a''_k(p^i) - e_1(p^i) = 0$. Resulta natural, entonces, que esta factorización tenga una relación especial con las series de Bell, relación que estudiaremos en el siguiente parágrafo. Por último, y de acuerdo con lo mencionado, observemos que, en particular, si a es fuertemente multiplicativa, su factorización es trivial, pues $\hat{a}_1(\prod_p p^{v_p(n)}) \stackrel{def}{=} \prod_p a(p)^{v_p(n)} = a(\prod_p p^{v_p(n)})$. Es decir: si a es fuertemente multiplicativa, es $\hat{a}_1 = a$ y la factorización (3.2) se reduce a la trivial $a = a * e_1$.

Para el cálculo efectivo de los factores b_j, son útiles el siguiente lema y su corolario.

LEMA 3. 2: Sea $a \in M_k$, es decir:

$$\begin{cases} a(1)=1 \\ n \notin \{ m^k : m \in \mathbb{N}_{\geq 2}\} \Rightarrow a(n)=0 \\ a(m^k n^k) = a(m^k)a(n^k) \text{ para } m,n \in \mathbb{N} \end{cases}$$

Entonces: $a^{*-1} = a\rho_k$, donde

$$\rho_k(n) = \begin{cases} =1 & \text{si } n=1 \\ =\mu(n^{1/k}) & \text{si } n \in \{m^k : m \in \mathbb{N}_{\geq 2}\} \end{cases} \qquad (3.10)$$

***Observación* 3.2:** las funciones ρ_k no son únicas: pueden definirse arbitrariamente fuera del conjunto $\{m^k : m \in \mathbb{N}_{\geq 1}\}$.

Demostración: Lo que tenemos que probar es que $a*(a\rho_k)=e_1$. La igualdad $[a*(a\rho_k)](1)=a(1)a(1)\rho_k(1)=1$ es trivial. Ahora, para $n=\prod_p p^{v_p(n)}=p_1^{v_1}p_2^{v_2}\dots p_s^{v_s}\geq 2$, consideremos las divisiones euclídeas $v_i=ku_i+r_i$, $0\leq r_i\leq k-1$, de manera que

$$n=p_1^{v_1}p_2^{v_2}\dots p_s^{v}=p_1^{ku_1}p_2^{ku_2}\dots p_s^{ku_s}p_1^{r_1}p_2^{r_2}\dots p_s^{r_s}=$$

$$=\overbrace{(p_1^{u_1}p_2^{u_2}\dots p_s^{u_s})^k}^{\tilde{n}^k}\overbrace{(p_1^{r_1}p_2^{r_2}\dots p_s^{r_s})}^{\tilde{n}} \qquad (3.11)$$

Ahora, en la sumatoria del último miembro de las igualdades

$$[a*(a\rho_k)](n)=\sum_{d/n}a(n/d)a(d)\rho_k(d)=$$
$$=a(n)+\sum_{\substack{d/n\\1<d<n}}a(n/d)a(d)\rho_k(d)+a(1)a(n)\rho_k(n)$$
$$=a(n)+\sum_{\substack{d/n\\1<d<n}}a(n/d)a(d)\rho_k(d)+a(n)\rho_k(n) \qquad (3.12)$$

los factores $a(d)$ se anulan salvo que $d\in\{m^k: m\in\mathbb{N}_{\geq 2}\}$, es decir,

$$d=p_1^{kw_1}p_2^{kw_2}\dots p_s^{kw_s}=\overbrace{(p_1^{w_1}p_2^{w_2}\dots p_s^{w_s})}^{\tilde{d}}{}^k=\tilde{d}^k \qquad (3.13)$$

donde $0\leq w_i\leq u_i$ para todo $i\in\{1,2,\dots,s\}$. Entonces, de (3.12) obtenemos

$$[a*(a\rho_k)](n)=a(n)+\sum_{\substack{\tilde{d}^k/n\\1<\tilde{d}^k<n}}a(n/\tilde{d}^k)a(\tilde{d}^k)\rho_k(\tilde{d}^k)+a(n)\rho_k(n) \qquad (3.14)$$

donde

$$(n/\tilde{d}^k)=p_1^{k(u_1-w_1)+r_1}p_2^{k(u_2-w_2)+r_2}\dots p_s^{k(u_s-w_s)+r_s}\in\{m^k: m\in\mathbb{N}\}$$

$$\Rightarrow r_1=r_2=\dots=r_s=0\Leftrightarrow n=\tilde{n}^k\in\{m^k: m\in\mathbb{N}\}$$

La razón es simple: si $p_1^{k(u_1-w_1)+r_1}p_2^{k(u_2-w_2)+r_2}\dots p_s^{k(u_s-w_s)+r_s}=$

$p_1^{kh}p_2^{kh}\dots p_s^{kh}$, entonces $k(u_i - w_i) + r_i = kh_i$, es decir $r_i = k(h_i - u_i + w_i)$. Si $h_i - u_i + w_i \neq 0$, tendríamos $r_i \geq k$, lo que es absurdo. Por lo tanto, necesariamente $h_i = u_i - w_i$, y por ende [de las igualdades $k(u_i - w_i) + r_i = kh_i$] obtenemos $r_i = 0$.

Hemos probado que si $n \notin \{m^k : m \in \mathbb{N}_{\geq 2}\}$ entonces $(n/\tilde{d}^k) \notin \{m^k : m \in \mathbb{N}_{\geq 2}\}$ y por lo tanto, de (3.14) tenemos, en este caso:

$$[a * (a\rho_k)](n) = a(n) + a(n)\rho_k(n) = 0$$

Ahora, si $n = \tilde{n}^k \in \{m^k : m \in \mathbb{N}_{\geq 2}\}$, entonces $\tilde{d}^k / \tilde{n}^k$ sii $\tilde{d} / \tilde{n}$: basta observar los factores primos en las descomposiciones $\tilde{n}^k = p_1^{ku_1} p_2^{ku_2} \dots p_s^{ku_s}$ y $\tilde{d}^k = p_1^{kw_1} p_2^{kw_2} \dots p_s^{kw_s}$. Entonces, en este caso tenemos

$$[a * (a\rho_k)](\tilde{n}^k) = a(\tilde{n}^k) + \sum_{\substack{\tilde{d}/\tilde{n} \\ \tilde{d}>1}} a(\tilde{n}^k/\tilde{d}^k)\ a(\tilde{d}^k)\rho_k(\tilde{d}^k) \overset{a \in M_k}{=}$$

$$\overset{a \in M_k}{=} a(\tilde{n}^k) + \sum_{\substack{\tilde{d}/\tilde{n} \\ \tilde{d}>1}} a(\tilde{n}^k)\ \rho_k(\tilde{d}^k) = a(\tilde{n}^k) + a(\tilde{n}^k) \sum_{\substack{\tilde{d}/\tilde{n} \\ \tilde{d}>1}} \rho_k(\tilde{d}^k) =$$

$$= a(\tilde{n}^k)[1 + \sum_{\substack{\tilde{d}/\tilde{n} \\ \tilde{d}>1}} \rho_k(\tilde{d}^k)] = a(\tilde{n}^k) \sum_{\tilde{d}/\tilde{n}} \rho_k(\tilde{d}^k) =$$

$$= a(\tilde{n}^k) \sum_{\tilde{d}/\tilde{n}} \mu(\tilde{d}) = a(\tilde{n}^k)[1 * \mu](\tilde{n}) = a(\tilde{n}^k) e_1(\tilde{n}) = 0$$

para todo $\tilde{n} > 1$ □

Corolario 3.2: Si $a \in M_k$, entonces para cada primo p y cada entero positivo m:

$$a^{*-1}(p^m) = \begin{cases} = 1 & if\ m = 0 \\ = 0 & if\ m \neq 0, k \\ = -a(p^k) & m = k \end{cases} .$$

Demostración: $a^{*-1}(p^m) = a(p^m)\ \rho_k(p^m) = 0$ si $m \neq k, 1$, pues $a(p^m) = 0$ en este caso. Ahora: $a^{*-1}(p^k) = a(p^k)\rho_k(p^k) = a(p^k)$

$\mu(p) = -a\ (p^k)$ □

El siguiente teorema es la versión invariante del anterior.

TEOREMA 3.2 Para cada $a \in (\mathcal{A}_1^{\times})^{S(\mathbb{P})}$ y cada entero positivo k, existe una única secuencia $(\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_k) \in (M_1)^{S(\mathbb{P})} \times (M_2)^{S(\mathbb{P})} \times \ldots \times (M_k)^{S(\mathbb{P})}$ y un único $a''_k \in (B_k)^{S(\mathbb{P})}$ tales que $a = \hat{a}_1 * \hat{a}_2 * \ldots * \hat{a}_k * a''_k$.

Demostración: De la factorización $a = \hat{a}_1 * \hat{a}_2 * \ldots * \hat{a}_k * a''_k$ tenemos que para cada $\gamma \in S(\mathbb{P})$:

$$a^{\gamma} = (\hat{a}_1)^{\gamma} * (\hat{a}_2)^{\gamma} * \ldots * (\hat{a}_k)^{\gamma} * (a''_k)^{\gamma} \qquad (3.15)$$

Si a es invariante:

$$a = (a_1)^{\gamma} * (a_2)^{\gamma} * \ldots * (a_k)^{\gamma} * (a''_k)^{\gamma} \qquad (3.16)$$

Por el Lema 3.1, tenemos que $(\hat{a}_i)^{\gamma} = a'_i \in M_i\ (i = 1, k)$ y $(a''_k)^{\gamma} = a'''_k \in B_k$, es decir:

$$a = a'_1 * a'_2 * \ldots * a'_k * a'''_k \qquad (3.17)$$

Ahora, la unicidad de la factorización $a = \hat{a}_1 * \hat{a}_2 * \ldots * \hat{a}_k * a''_k$ implica que $(\hat{a}_i)^{\gamma} = a'_i = \hat{a}_i\ (i = 1,\ k)$ y $(a_k'')^{\gamma} = a'''_k = a_k''$. Dado que esto ocurre con cada $\gamma \in S(\mathbb{P})$, hemos demostrado que si a es invariante, sus factores son necesariamente invariantes. □

***Observación* 3.3:** Si a es invariante, entonces es constante sobre el conjunto de primos, digamos $a(p)=\alpha$ para todo primo p; si además es fuertemente multiplicativa, entonces

$$a\left(\prod_p p^{v_p(n)}\right) = \prod_p a(p)^{v_p(n)} = \prod_p \alpha^{v_p(n)} = \alpha^{\sum_p v_p(n)} = \alpha^{\Omega(n)}$$

Fórmulas análogas se obtienen para las funciones fuertemente multiplicativas en cuadrados, cubos, etc. Por lo tanto, cuando a es invariante, sus primeros factores son de la forma $\hat{a}_1(n) =$

$\alpha_1{}^{\Omega(n)}, \hat{a}_2(n^2) = \alpha_2{}^{\Omega(n)}$, (y se anula en los no-cuadrados), etc. Esto facilita el cálculo de los factores $\hat{a}_i$.

***Ejemplo* 3.1:** Algunos factores de la función divisor. Utilizaremos, para abreviar, la notación para esta función, en lugar de la más actual . Existen varias expresiones conocidas para esta función, que cuenta la cantidad de divisores de cada número entero positivo $\tau(n)=\sum_{d/n}1=(1*1)(n)=\prod_p[1+v_p(n)]$: . Se trata de una función claramente invariante y en su factorización de tercer orden $\tau = \hat{\tau}_1 * \hat{\tau}_2 * \hat{\tau}_3 * \tau''_3$ tenemos (los cálculos no son triviales):

$$\hat{\tau}_1(n) = 2^{\Omega(n)},\ \hat{\tau}_2(n) = \begin{cases} 0 & \textit{si n no es un cuadrado} \\ \lambda(\sqrt{n}) = (-1)^{\Omega(\sqrt{n})} & \textit{si n es un cuadrado,} \end{cases}$$

$$\hat{\tau}_3(n) = \begin{cases} 0 & \textit{si n no es un cubo} \\ (-2)^{\Omega(\sqrt{n})} & \textit{si n es un cubo,} \end{cases}$$

$$\tau''_3(n) = \begin{cases} 1 \quad si \quad n = 1 \\ 0 \quad si \quad \exists p : v_p(n) \in \{1,2\} \\ 3\prod_p [3 - v_p(n)] \quad \textit{en otro caso} \end{cases}$$

La función λ del segundo factor es la función de Liouville.

***Ejemplo* 3.2**: Factorización de la función de Möbius: mediante un cálculo directo o bien utilizando la serie de Dirichlet de la función de Liouville, se obtiene la factorización (para cada entero positivo k)

$$\mu = \lambda^{(1)} * \lambda^{(2)} * \lambda^{(2^2)} * \ldots * \lambda^{(2^k)} * \ \mu^{(2^{k+1})} \qquad (3.18)$$

donde

$$\lambda^{(j)}(n)=\begin{cases} 1 & si \quad n=1 \\ 0 & si \quad n\notin\{m^j : m\in\mathbb{N}_{\geq 2}\} \\ \lambda(\sqrt[j]{n}) & si \quad n\in\{m^j : m\in\mathbb{N}_{\geq 2}\} \end{cases}$$

y, análogamente.

$$\mu^{(k+1)}(n)=\begin{cases} 1 & si \quad n=1 \\ 0 & si \quad n\notin\{m^{k+1} : m\in\mathbb{N}_{\geq 2}\} \\ \mu(\sqrt[k+1]{n}) & si \quad n\in\{m^{k+1} : m\in\mathbb{N}_{\geq 2}\} \end{cases}$$

Es evidente que la factorización de una función $a\in\mathbb{A}_1^{\times}$ induce una factorización de su serie de Dirichlet y recíprocamente. Según los casos, puede resultar más sencillo una factorización que otra, pero no cualquier factorización de la serie de Dirichlet de a induce la factorización de a dada por el Teorema 3.1, pues en ésta los factores tienen una forma muy específica. Un fenómeno totalmente análogo ocurre con las series de Bell, como veremos a continuación.

4. Factorización de series de Bell y de series de Fourier fuertemente convergentes

Para cada función $a:\mathbb{N}\to\mathbb{C}$ y cada primo p, la p-serie de Bell de a es, por definición, la serie formal

$$\beta_{a,p}(x)=\sum_{n=0}^{\infty} a(p^n)\,x^n \qquad (4.1)$$

Las series de Bell, al igual que las series de Dirichlet, tienen la siguiente propiedad, muy conocida y sencilla de probar: para todo par de funciones numéricas a y b y cada primo p:

$$\beta_{a*b,p}(x)=\beta_{a,p}(x)\;\beta_{b,p}(x) \qquad (4.2)$$

Algunos ejemplos notables:

1) $\beta_{e_1,p}(x)=1\;;\;e_1(n)=\delta_{1,n}$ (es la unidad para el producto $*$).

2) $\beta_{1,p}(x)=\frac{1}{1-x}1/(1-x)$; $1(n) = 1$ (constante).

3) $\beta_{\mu,p}(x) = 1-x$; μ es la función de Möbius:

$\mu(1)=1$ y $\mu(p_1^{v_1} p_2^{v_2} \ldots p_r^{v_r}) = \begin{cases} (-1)^r & si \quad v_1 = v_2 = \ldots = v_r = 1 \\ 0 & si \quad \exists v_i \geq 2 \end{cases}$

4) $\beta_{\phi,p}(x)=\frac{1-x}{1-px}$; ϕ es la «*función fi*» de Euler:

$\phi(n) = card\{k \in \{1,2,\ldots,n\} : mcd(k,n) = 1\}$

5) $\beta_{Id_k p}(x) = \frac{1}{1-p^k x}$; $Id_k(n) = n^k$

6) $\beta_{\sigma_k p})(x) = \frac{1}{(1-p^k x)(1-x)}$; $\sigma_k(n) = \sum_{d/n} d^k$

7) $\beta_{\lambda,p}(x) = \frac{1}{1+x}$; λ es la función de Liouville: $\lambda(n)=(-1)^{\Omega(n)}$, donde

$\Omega(n) = \Omega\ (\prod_p p^{v_p(n)}) = \sum_p v_p(n)$

Varias de estas expresiones se obtienen utilizando otra propiedad muy conocida (y aún más sencilla de deducir) de estas series: si a es fuertemente multiplicativa, entonces:

$$\beta_{a,p}(x) = \sum_{n=0}^{\infty} a(p^n) x^n = \sum_{n=0}^{\infty} a(p)^n x^n \frac{1}{1-a(p)x} \qquad (4.3)$$

Ahora, comenzaremos a ver algunas consecuencias de los resultados originales presentados en los párrafos anteriores. En primer lugar, si $a(1)=1$, para cada entero positivo k, la factorización $a = \hat{a}_1 * \hat{a}_2 * \ldots * \hat{a}_k * a''_k$ y la identidad (4.2) inducen, para cada primo p, una factorización

$$\beta_{a,p}(x) = \beta_{\hat{a}_1,p}(x)\beta_{\hat{a}_2,p}(x)\ldots\beta_{\hat{a}_k,p}(x)\ \beta_{a''_k,p}(x) \qquad (4.4)$$

Dado que $\hat{a}_1$ es fuertemente multiplicativa,

$$\beta_{\hat{a}_{1,p}}(x)=\frac{1}{1-\hat{a}_1(p)x}=\frac{1}{1-a(p)x} \qquad (4.5)$$

(Respecto de la segunda igualdad, ver corolario 3.1). Ahora bien, $\hat{a}_2$ se anula en los no-cuadrados y es fuertemente multiplicativa en cuadrados, por lo tanto

$$\beta_{\hat{a}_2,p}(x)=\sum_{n=0}^{\infty}=\hat{a}_2(p^n)x^n=\sum\hat{a}_2(p^{2k})x^{2k}=\sum\hat{a}_2(p^2)^k x^{2k}=\frac{1}{1-\hat{a}_2(p^2)x^2} \qquad (4.6)$$

Procediendo de la misma manera con los subsiguientes factores del miembro derecho de (4.4), obtenemos la siguiente factorización de la *p*-serie de Bell de *a*:

$$\beta_{a,p}(x)=\frac{\beta_{a''k,p}(x)}{[1-a(p)x][1-\hat{a}_2(p^2)x^2]....[1-\hat{a}_k(p^k)x^k]} \qquad (4.7)$$

Finalmente $a_k''\in B_k$, la función se anula en todas las potencias $p,p^2,\ldots,p^k$ y es $a_1''(1)=1$, por lo tanto,

$$\beta_{a_k'',p}(x)=\sum_{n=0}^{\infty}a_k''(p^n)x^n=1+x^{k+1}\sum_{n=0}^{\infty}a_k''(p^{k+1+n})x^n \qquad (4.8)$$

Obsérvese que, respecto de la topología dada por el ideal maximal en el anillo de series formales $\mathbb{C}[[x]]$, se tiene $\underset{k\to\infty}{Lim}\,\beta_{a_k'',p}(x)=0$. Para observar esto desde el punto analítico, conviene considerar a la variable x como un infinitésimo, con lo cual resulta que x^{k+1} es un infinitésimo de orden $k+1$. Pero esta observación es parte de la relación natural que existe entre las series formales de coeficientes complejos y las funciones analíticas en torno del 0. En este sentido, es interesante comparar la factorización (4.7) con el Teorema de Factorización de Weierstrass y su primo cercano, el Teorema de Mitag-Leffler: asociando la serie de Bell del miembro izquierdo con una función meromorfa, el miembro derecho es una factorización de dicha función en la que sus polos aparecen explícitamente. Más precisamente: sea

$a \in \mathcal{A}_1^{\times}(\mathbb{C})$ un elemento de orden polinómico, es decir: existe una constante real c tal que $|a(n)| \leq n^c$ para todo n. No es difícil (aunque no trivial) probar que el conjunto de los elementos de orden polinómico de $\mathcal{A}_1^{\times}(\mathbb{C})$ es un subgrupo de $\mathcal{A}_1^{\times}(\mathbb{C})$. Dado un primo p, sea $f_{a,p}$ la función de variable compleja tal que $f_{a,p}(z) = \sum_{n=0}^{\infty} a(p^n) z^n$. El radio de convergencia de esta serie es $\geq 1/p^c$ y por lo tanto $f_{a,p}$ es analítica en –al menos– el disco . En este disco $D_{p^{-c}} = \{z \in \mathbb{C} : |z| < p^{-c}\}$, la identidad (4.7) induce la factorización

$$f_{a,p}(z) = \frac{1 + z^{k+1} \sum_{n=0}^{\infty} a_k''(p^{k+1+n}) z^n}{[1 - a(p)z][1 - \hat{a}_2(p^2)z^2] \ldots [1 - \hat{a}_k(p^k)z^k]} \tag{4.9}$$

en un entorno de 0.

Veamos ahora las consecuencias del otro concepto original presentado en este trabajo: si a es invariante, entonces para todo primo p, todo entero positivo n y toda permutación $\gamma \in S(\mathbb{P})$:

$$a(p^n) = a^{\gamma}(p^n) = a(\gamma(p)^n) \tag{4.10}$$

y dado que el grupo $S(\mathbb{P})$ actúa transitivamente en $\mathbb{P}$, los coeficientes $a(p^n)$ de la serie de Bell de a no dependen del número primo p, es decir:

$$\beta_{a,p}(x) = \sum_{n=0}^{\infty} a(p^n) x^n = \sum_{n=0}^{\infty} \alpha_n x^n \overset{\text{notación}}{=} \beta_a(x) \tag{4.11}$$

Obsérvese, en la lista de ejemplos anterior, que algunas series de Bell no dependen, efectivamente, del primo p. Es muy sencillo de ver que la función de Möebius y de Liouville son invariantes, así como la función divisor $\sigma(n) = \sum_{d/n} 1 =$ cantidad de divisores de n. De todos modos, que las series de Bell de a no dependan de p es condición necesaria no suficiente para la invariancia de a. Por ejemplo, la función $a : \mathbb{N} \to \mathbb{C}$ tal que $a(1) = 1$, $a(p^k) = 0$ para todo primo p y todo entero positivo k, y $a(n) = n$ si n no es potencia de un primo, es un contraejemplo sencillo.

Utilizando el Teorema de Factorización Invariante, vemos que para toda $a \in \mathbb{A}_1^{\times}(\mathbb{C})^{S(P)}$ y todo entero positivo k:

$$\beta_a(x) = \frac{\beta_{a''_k}(x)}{[1-\alpha_1 x][1-\alpha_2 x^2]....[1-\alpha_k x^k]} \qquad (4.12)$$

donde $\alpha_1, \alpha_2, ..., \alpha_k$ son constantes que dependen de a. Terminaremos esta exposición con un ejemplo de factorización series de Fourier fuertemente convergentes, es decir, de series de la forma

$$f(\theta) = \sum_{n=0}^{\infty} \frac{u_n}{2^n} e^{in\theta} \qquad (4.13)$$

donde la sucesión de coeficientes u_n es de orden polinómico: existe una constante real c tal que $|u_n| \leq n^c$ para todo n. El radio de convergencia es al menos 2. Entonces, la función f definida en (4.13) es la restricción a la circunferencia central unitaria de la función $h(z) = \sum_{n=0}^{\infty} \frac{u_n}{2^n} z^n = \sum_{n=0}^{\infty} u_n \left(\frac{z}{2}\right)^n$, holomorfa en el disco $D_2 = \{z \in \mathbb{C} : |z| < 2\}$ (al menos).

Para la función de Möbius, con la notación precedente y la utilizada en la factorización (3.18), tenemos:

$$\beta_\mu(x) = \sum_{n=0}^{\infty} \mu(p^n) x^n = 1 - x$$

$$\beta_{\mu^{(2^{k+1})}}(x) = \sum_{n=0}^{\infty} \mu^{(2^{k+1})}(p^n) x^n = \sum_{h=0}^{\infty} \mu^{(2^{k+1})}((p^h)^{2^{k+1}}) x^{h 2^{k+1}} = \sum_{h=0}^{\infty} \mu(p^h)$$

$$x^{h 2^{k+1}} = 1 - x^{2^{k+1}}$$

$$\beta_\lambda(x) = \sum_{n=0}^{\infty} \lambda(p^n) x^n = \sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}, \quad |x| < 1$$

$$\beta_{\lambda^{(i)}}(x) = \sum_{n=0}^{\infty} \lambda^{(i)}(p^n) x^n = \sum_{n=0}^{\infty} \lambda^{(i)}((p^h)^i) x^{hi} = \sum_{n=0}^{\infty} \lambda(p^h) x^{hi} = \sum_{n=0}^{\infty} (-1)^h (x^i)^h =$$

$$=\frac{1}{1+x^{i}},\ |x|<1$$

Entonces, la factorización (3.18) induce la identidad (para cada complejo x tal que $|x|<1$ y cada entero positivo k):

$$1-x=\frac{1}{(1+x)}\ \frac{1}{(1+x^{2}=}\ \frac{1}{(1+x^{2^{2}}}\frac{1}{(1+x^{2^{3}})}\ \cdots\frac{1}{(1+x^{2^{k}})}(1-x^{2^{k+1}}) \tag{4.14}$$

Es decir:

$$\frac{1-x^{2^{k+1}}}{1-x}=\prod_{n=0}^{k}(1+x^{2^{n}}),\ |x|<1 \tag{4.15}$$

Para $k\to\infty$ se obtiene un producto infinito conocido (y no trivial). Ahora, eligiendo $x=(1/2)e^{i\theta},\ \theta\in[-\pi,\pi]$:

$$\sum_{n=0}^{\infty}=\frac{e^{in\theta}}{2^{n}}=\frac{1}{1-(1/2)e^{i\theta}}\approx\frac{1-\frac{e^{2^{k+1}i\theta}}{2^{2^{k+1}}}}{1-(e^{i\theta}/2)}=\prod_{n=0}^{k}(1+1\ \ e^{2^{n}i\theta}) \tag{4.16}$$

(tomando límite para $k\to\infty$ se obtiene la igualdad exacta).

APOSTOL, T. M. (1976). "Introduction to Analytic Number Theory", en *Undergraduate Texts in Mathematics*. Nueva York: Springer-Verlag.

Apostol, Tom. M. (1990) "Modular Functions and Dirichlet Series in Number Theory", en *Graduate Texts in Mathematics*. Nueva York: Springer- Verlag.

CASHWELL, E. D. y EVERETT, C. J. (1959). "The ring of number theoretic functions". *Pacific Journal of Mathematics*, *9*(4): págs. 975-985.

Elliott, J. (2008). "Ring structures on groups of arithmetic functions". *Journal of Number Theory*, *128*: págs. 709-730.

OKOUNKOV, A. Yu. (1994). ·Thoma's Theorem and Representations of the Infinite Bisymmetric Group". *Funktsional. Anal. i Prilozhen.*, *28*(2): págs. 31-40; *Funct. Anal. Appl.*, *28*(2): págs. 100-107.

SHAPIRO, H. (1972). "On the convolution ring of arithmetic functions". *Communications on pure and applied mathematics*, *25*: págs. 287-336.

TÓTH, L. y HAUKKANEN, P. (2009) "On the binomial convolution of arithmetic functions". *Journal of Combinatorics and Number Theory*, *1*(1).

Palabras clave: funciones aritméticas - convolución de Dirichlet - series de Bell - grupo simétrico infinito.

Key words: number theoretical functions - Dirichlet convolution - Bell series - infinite symmetric group.

Abstract

It is well known that the ring of the number theoretical functions, a central object in the analytical number theory, is a UFD. But the units abound in this ring, thus each prime element has too many associates and this fact reduces the effectiveness of the unique factorization property. In this work we found a factorization of the units that may be a useful complement for the classical prime factorization. On the other hand, we introduce an action - which we call the *prime action* - of the infinite permutation group $S(\infty)$on the ring, and we obtain an invariant version of the factorization theorem. The Bell series are the natural generating series for the invariant functions and we close the present article with an application of our results to a natural factorization of the Bell series and the strongly convergent Fourier series.