

Sobre las propiedades analíticas del anillo de polinomios $\mathbb{F}_q[X]$

OSCAR FRANCISCO CASAS
Universidad Nacional de Colombia, Bogotá

RESUMEN. Se hace una introducción coherente de algunas propiedades analíticas de las funciones aritméticas definidas sobre el monoide de los polinomios unitarios de coeficientes en un cuerpo finito.

Key words and phrases. Finite fields, arithmetical functions, polynomials.

2000 Mathematics Subject Classification. Primary 13M10. Secondary 11A25.

ABSTRACT. A short coherent introduction of some analytic properties of arithmetical functions defined on the monoid of monic polynomials with coefficients in a finite field is presented.

1. Introducción

En 1932 CARLITZ [7] extiende la noción de función aritmética al anillo de polinomios sobre un cuerpo de Galois (cuerpo finito) definiéndolas en

analogía con las conocidas en la teoría clásica de números y considera algunas de sus propiedades aritméticas. Luego el mismo CARLITZ [8] encuentra relaciones entre las funciones aritméticas y la función zeta de Riemann. Más tarde, en 1975, KNOPFMACHER [3], en una serie de artículos publicados en el *Journal de Crelle*, generaliza resultados conocidos de la teoría clásica de números extendiendo la idea de función aritmética, a toda una gama de monoides interesantes y establece propiedades analíticas de estas nuevas funciones.

En este artículo se realiza una presentación coherente de las ideas fundamentales de la teoría de CARLITZ y KNOPFMACHER [3] para el caso particular de los polinomios unitarios $(a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n)$ de coeficientes en un cuerpo finito \mathbb{F}_q de q elementos y característica $p > 0$ ($q = p^s$, para algún s entero ≥ 1). Se dan algunos hechos que no aparecen de manera explícita en la bibliografía y se intenta mejorar algunas demostraciones. Todo esto con el objetivo de ejemplificar, en el caso antes mencionado, la teoría analítica abstracta de números desarrollada por KNOPFMACHER. Este caso, de por sí, tiene un gran interés intrínseco.

En la primera sección recordamos y establecemos algunas de las propiedades aritméticas del anillo de polinomios $\mathbb{F}_q[X]$ y adaptamos, para nuestros propósitos, algunos resultados de SMITS [10] sobre la estructura de los anillos residuales $\mathbb{F}_q[X]/(h(X))$, $h(X) \in \mathbb{F}_q[X]$. En la segunda sección introducimos el concepto de función aritmética definida sobre el monoide $\mathbb{M}(X, q)$ de los polinomios unitarios en $\mathbb{F}_q[X]$, y en la tercera definimos los análogos en el caso polinómico de algunas de las funciones aritméticas del caso clásico. En particular, demostramos el análogo de la fórmula de inversión de Möbius. En la cuarta sección, establecemos un isomorfismo entre el álgebra de las funciones aritméticas y el de las series formales de Dirichlet. Mostramos también que es posible dotar al álgebra de las funciones aritméticas de una métrica no arquimediana, indicando que de esta estructura topológica es posible obtener resultados algebraicos (proposiciones 5.3 y 5.4) y expresar situaciones algebraicas en términos topológicos.

En la sección quinta, examinamos las series de Dirichlet desde el punto de vista de su convergencia como funciones de variable compleja. En

particular, vemos que es posible expresar las series de Dirichlet correspondientes a las más conocidas funciones aritméticas como cocientes o productos de funciones ζ de Riemann.

2. Preliminares

Sea p un número primo y sea s un entero positivo. Con \mathbb{F}_q denotaremos un cuerpo finito con $q = p^s$ elementos (para ver la construcción de este cuerpo pueden consultarse HERSTEIN [1] o FRALEIGH [2], por ejemplo). Sea $\mathbb{F}_q[X]$ el anillo de polinomios en la indeterminada X con coeficientes en el cuerpo \mathbb{F}_q .

Definición 2.1. Si $a(X) = a_0 + a_1X + \dots + a_nX^n \neq 0$ y $a_n \neq 0$ entonces el grado de $a(X)$, escrito como $\text{gr}(a(X))$, es n . Diremos que el polinomio $a(X)$ es unitario si $a_n = 1$.

La siguiente proposición es muy conocida y su demostración puede encontrarse en [4].

Proposición 2.1. $\mathbb{F}_q[X]$ es un anillo euclídeo, para la función (algoritmo euclídeo) definida por:

$$\Phi(a(X)) = \begin{cases} \text{gr}(a(X)) & \text{si } a(X) \neq 0, \\ -1 & \text{en otro caso.} \end{cases}$$

$\mathbb{F}_q[X]$ es entonces un dominio de factorización única, ya que todo anillo euclídeo lo es.

Definición 2.2. Diremos que los polinomios $p(X)$ y $q(X)$ son asociados si existe $a \in \mathbb{F}_q^\times$ tal que $p(X) = aq(X)$

Proposición 2.2. Todo polinomio $p(X) \in \mathbb{F}_q[X]$ es el asociado de un polinomio de la forma $a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n$.

Demostración. Sea $p(X) = b_1 + b_2X^2 + \dots + b_nX^n$ con $b_n \neq 0$, como $b_n \neq 0$ entonces

$$p(X) = b_n \left(\frac{b_1}{b_n} + \frac{b_2}{b_n}X^2 + \dots + X^n \right)$$

con $\frac{b_i}{b_n} \in \mathbb{F}_q$, ya que \mathbb{F}_q es un cuerpo. El polinomio entre paréntesis es unitario y está claramente asociado con $p(X)$. \square

Proposición 2.3. *La relación definida por*

$$p(X) \sim q(X) \quad \text{si, y solo si, existe } a \in \mathbb{F}_q^\times \quad \text{tal que } p(x) = aq(X)$$

es una relación de equivalencia.

Demostración. La demostración es inmediata. \square

Sea $\mathbb{M}(X, q) = \mathbb{F}_q[X]/\sim$ y tomemos como representante de cada clase al único polinomio unitario de la forma $a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n$ que existe en cada clase por la proposición (2.2).

De la teoría de los polinomios en la indeterminada X con coeficientes en un cuerpo conmutativo arbitrario, obtenemos los siguientes resultados.

- Las unidades en $\mathbb{F}_q[X]$ son los elementos constantes distintos de cero.
- Los elementos primos de $\mathbb{F}_q[X]$ son los polinomios irreducibles unitarios y sus asociados. Por lo tanto, de ahora en adelante un elemento primo de $\mathbb{F}_q[X]$ será un polinomio irreducible y unitario.
- Sea $h(X) = up_1(X)^{\alpha_1} \dots p_r(X)^{\alpha_r}$ y consideremos el ideal $(h(X))$ generado por este polinomio. Por el teorema chino de los restos para el anillo de polinomios tenemos que

$$\mathbb{F}_q[X]/(h(X)) \approx \prod_{i=1}^r \mathbb{F}_q[X]/(p_i(X)^{\alpha_i}).$$

$$\mathbb{F}_q[X]/(h(X))^\times \approx \prod_{i=1}^r \left(\mathbb{F}_q[X]/(p_i(X)^{\alpha_i}) \right)^\times.$$

Por lo tanto, podemos restringirnos a estudiar los anillos de la forma $\mathbb{F}_q[X]/(p(X)^\alpha)$ donde $p(X)$ es un polinomio irreducible.

Por otra parte, a $\mathbb{M}(X; q)$ se trasladan de manera natural las propiedades de divisibilidad de polinomios y las nociones de máximo común divisor y mínimo común múltiplo.

Las siguientes proposiciones son adaptaciones de resultados contenidos en SMITS [10].

Proposición 2.4. *Si $p(X) = p_0 + p_1X + \dots + p_nX^n$ es un polinomio irreducible de $\mathbb{F}_q[X]$ y x designa la clase de equivalencia de X módulo $(p(X)^\alpha)$, entonces:*

1. $\mathbb{F}_q[X]/(p(X)^\alpha)$ es una \mathbb{F}_q -álgebra de dimensión αn y $q^{\alpha n}$ elementos.
2. $1, x, x^2, \dots, x^{\alpha n-1}$ es una \mathbb{F}_q base de esta álgebra.
3. $\theta(p(X)) = z$ cumple la condición $z^k \neq 0$ si $0 \leq k < \alpha$, donde θ es el epimorfismo canónico.
4. los polinomios de $\mathbb{F}_q[X]$ de grado $< \alpha n$ forman un sistema completo de restos módulo $(p(X)^\alpha)$.

Demostración. Sea $\theta : \mathbb{F}_q[X] \rightarrow \mathbb{F}_q[X]/(p(X)^\alpha)$ el epimorfismo canónico. Veamos ahora que θ induce un isomorfismo \mathbb{F}_q sobre $\theta(\mathbb{F}_q)$. Esto nos permite afirmar que $\mathbb{F}_q[X]/(p(X)^\alpha)$ contiene una copia de \mathbb{F}_q , la cual identificaremos con \mathbb{F}_q . Si $a \in \mathbb{F}_q^\times$ y $\theta(a) = 0$, podemos escribir $a = h(X)p(X)^\alpha$, y, por consiguiente, $0 = \text{gr}(h(X)) + \alpha \text{gr}(p(X))$, igualdad que es imposible si $h(X) \neq 0$. Luego $\theta(a) \neq 0$ si $a \in \mathbb{F}_q^\times$. En vista de lo anterior, podemos escribir

$$\theta(a(X)) = \theta\left(\sum_{k=0}^m a_k X^k\right) = \sum_{k=0}^m a_k x^k,$$

donde $x = \theta(X)$. Como claramente $\mathbb{F}_q[X]/(p(X)^\alpha)$ es una \mathbb{F}_q -álgebra, resulta que $1 (= \theta(1)), x, x^2, \dots, x^m, \dots$, conforman un sistema de generadores de esta álgebra. Ahora bien, si $p(X) = p_0 + p_1X + \dots + p_nX^n$ es la expresión explícita del polinomio $p(X)$, entonces $\theta(p(X)) = \sum_{k=0}^n p_k x^k = z$ cumple $z^\alpha = 0$ en $\mathbb{F}_q[X]/(p(X)^\alpha)$; es decir,

$$(p_0 + p_1x + \dots + p_{n-1}x^{n-1} + p_nx^n)^\alpha = \gamma_0 + \gamma_1x + \dots + \gamma_{\alpha n-1}x^{\alpha n-1} + \gamma_{\alpha n}x^{\alpha n} = 0,$$

donde $\gamma_i \in \mathbb{F}_q$. Esta relación muestra la manera cómo $x^{\alpha n}$ puede expresarse como una combinación lineal de $1, x, x^2, \dots, x^{\alpha n-1}$. A partir de esto vemos que $x^{\alpha n+m}$, $m > 0$, puede obtenerse a partir de estos elementos; es decir, todo polinomio $a(X)$ es equivalente módulo

$(p(X)^\alpha)$ a un polinomio de grado $< \alpha n$. Finalmente $0 = \sum_{k=0}^{\alpha n-1} \lambda_k x^k$ cuando, y sólo cuando, $\sum_{k=0}^{\alpha n-1} \lambda_k X^k = h(X)p(X)^\alpha$. Si $h(X) = 0$ es claro que $\lambda_1 = \lambda_2 = \dots = \lambda_{\alpha n-1} = 0$; si $\text{gr}(h(X)) \geq 0$, tendríamos $\alpha n - 1 = \text{gr}(h(X)) + \alpha n \geq \alpha n$, lo cual es imposible. Luego $1, x, x^2, \dots, x^{\alpha n-1}$ es una base de la \mathbb{F}_q -álgebra $\mathbb{F}_q[X]/(p(X)^\alpha)$. Esto significa que todo polinomio $a(X)$ es equivalente módulo $(p(X)^\alpha)$ a un único polinomio de grado estrictamente menor que αn . Dado que \mathbb{F}_q tiene q elementos, resulta entonces que $\mathbb{F}_q[X]/(p(X)^\alpha)$ tiene exactamente $q^{\alpha n}$ elementos. \square

Es conocido que $\mathbb{F}_q^{(p)} = \mathbb{F}_q$, lo cual implica que $\pi^{q^m} = \pi$ para todo $\pi \in \mathbb{F}_q$. Por tanto, si $m = \min\{k; q^k > \alpha\}$ y $u = x^{q^m}$, tenemos

$$0 = z^{q^m} = (p_0 + p_1x + \dots + p_{n-1}x^{n-1} + x^n)^{q^m} = \\ p_0 + p_1u + \dots + p_{n-1}u^{n-1} + u^n$$

Vemos pues que u satisface el polinomio irreducible $p(X) \in \mathbb{F}_q[X]$; por lo tanto, $\mathbb{F}_q[X]/(p(X)^\alpha)$ contiene a $\mathbb{F}_q(u)$ copia isomorfa de $\mathbb{F}_q[X]/(p(X))$. Hagamos $L = \mathbb{F}_q(u)$ de modo que $\mathbb{F}_q \subset L \subset \mathbb{F}_q[X]/(p(X)^\alpha)$. Consideremos ahora la L -álgebra $L[z] = \{\lambda_0 + \lambda_1z + \dots + \lambda_{\alpha-1}z^{\alpha-1}; z^\alpha = 0, \lambda_i \in L\}$. Se puede ver que $1, z, z^2, \dots, z^{\alpha-1}$ es una L -base de $L[z]$. Como $[L : \mathbb{F}_q] = n = \text{gr}(p(X))$, entonces L tiene q^n elementos y, por consiguiente, $L[z]$ tiene $(q^n)^\alpha = q^{n\alpha}$ elementos. Ahora bien, de $L[z] \subset \mathbb{F}_q[X]/(p(X)^\alpha)$ y de que ambos tienen el mismo número de elementos, resulta que $L[z] = \mathbb{F}_q[X]/(p(X)^\alpha)$. Tenemos pues la siguiente proposición.

Proposición 2.5. *Si $p(X) = p_0 + p_1X + \dots + p_nX^n$ es un polinomio irreducible de \mathbb{F}_q y $z = \theta(p(X))$ es la clase de $p(X)$ módulo $(p(X)^\alpha)$, entonces:*

1. $\mathbb{F}_q[X]/(p(X)^\alpha)$ contiene un cuerpo L isomorfo a $\mathbb{F}_q/(p(X))$.
2. $\mathbb{F}_q[X]/(p(X)^\alpha) = L[z] = \{\lambda_0 + \lambda_1z + \dots + \lambda_{\alpha-1}z^{\alpha-1}; z^\alpha = 0, \lambda_i \in L\}$ es una L -álgebra de dimensión α , una de cuyas bases es $1, z, z^2, \dots, z^{\alpha-1}$.

Proposición 2.6. $L[z]^\times = L^\times \times \{1 + \lambda_1z + \dots + \lambda_{\alpha-1}z^{\alpha-1}; z^\alpha = 0, \lambda_i \in L\}$.

Demostración. Sea $\lambda_0 + \lambda_1 z + \cdots + \lambda_{\alpha-1} z^{\alpha-1} \in L[z]$. Si $\lambda_0 = 0$, $z(\lambda_1 + \cdots + \lambda_{\alpha-1} z^{\alpha-2})$ no puede ser invertible, pues z es un divisor de cero. Luego los elementos invertibles de $L[z]$ están entre los de la forma $\lambda_0 + \lambda_1 z + \cdots + \lambda_{\alpha-1} z^{\alpha-1} = \lambda_0 [1 + (\lambda_0^{-1} \lambda_1) z + \cdots + (\lambda_0^{-1} \lambda_{\alpha-1}) z^{\alpha-1}]$, con $\lambda_0 \in L^\times$. Ahora bien, todo elemento de la forma $1 + \beta_1 z + \cdots + \beta_{\alpha-1} z^{\alpha-1}$ es invertible, pues,

$$\begin{aligned} 1 &= (1 + \beta_1 z + \cdots + \beta_{\alpha-1} z^{\alpha-1})(1 + \mu_1 z + \cdots + \mu_{\alpha-1} z^{\alpha-1}) \\ &= 1 + \mu_1 z + \mu_2 z^2 + \cdots + \mu_{\alpha-1} z^{\alpha-1} + \\ &\quad + \beta_1 \mu_1 z + \beta_1 \mu_2 z^2 + \cdots + \beta_1 \mu_{\alpha-2} z^{\alpha-1} + \\ &\quad \dots \\ &\quad + \beta_{\alpha-1} z^{\alpha-1}, \end{aligned}$$

lo que es equivalente al sistema

$$\begin{aligned} 0 &= \mu_1 + \beta_1 \\ 0 &= \mu_2 + \beta_1 \mu_1 + \beta_2 \\ &\dots \\ 0 &= \mu_{\alpha-1} + \beta_1 \mu_{\alpha-2} + \beta_2 \mu_{\alpha-3} + \cdots + \beta_{\alpha-1}, \end{aligned}$$

el cual es soluble para $\mu_1, \mu_2, \dots, \mu_{\alpha-1}$ en términos de las β_i . La proposición queda pues demostrada. \square

De la anterior proposición podemos concluir que $L[z]^\times$ tiene $(q^n - 1)q^{n(\alpha-1)}$ elementos.

Como $L[z] = \mathbb{F}_q[X]/(p(X)^\alpha)$ obtenemos que $[\mathbb{F}_q[X]/(p(X)^\alpha)]^\times$ tiene $(q^n - 1)q^{n(\alpha-1)}$ elementos.

De ahora en adelante en vez de $a(X), b(X), \dots$ escribiremos a, b, \dots , si no hay posibilidad de confusión. La norma de un polinomio $a \in \mathbb{M}(X, q)$ la definimos de la siguiente manera: $|a| = q^n$, donde q representa el número de elementos \mathbb{F}_q y n el grado del polinomio a .

3. Funciones aritméticas en $\mathbb{M}(X, q)$

Las siguientes proposiciones son adaptaciones de la teoría clásica de números al caso que nos ocupa. Sus demostraciones no difieren en mucho

de las del caso clásico y se pueden encontrar, por ejemplo, en [5, cap. 2], por lo que las dejamos al cuidado del lector.

Definición 3.1. *Una función $f : \mathbb{M}(X, q) \rightarrow \mathbb{C}$, se dice una función aritmética.*

El conjunto de las funciones aritméticas se notará con $\text{Dir}(\mathbb{M}(X, q))$.

Definición 3.2. *Sean $f, g \in \text{Dir}(\mathbb{M}(X, q))$. Definimos el producto de Dirichlet (o convolución de Dirichlet) a la operación dada por la expresión*

$$(f \star g)(a) := \sum_{d|a} f(d)g\left(\frac{a}{d}\right) \quad (1)$$

Definición 3.3. *Sean $a \in \mathbb{M}(X, q)$, $f, g \in \text{Dir}(\mathbb{M}(X, q))$ y $\delta \in \mathbb{C}$, entonces definimos:*

$$(f + g)(a) := f(a) + g(a) \quad (2)$$

$$(\delta f)(a) := \delta f(a) \quad (3)$$

En la siguiente proposición expresamos el hecho de que $\text{Dir}(\mathbb{M}(X, q))$ conforma una \mathbb{C} -álgebra, para las operaciones definidas anteriormente.

Proposición 3.1. *Las operaciones definidas por la ecuaciones (1), (2) y (3) tienen las siguientes propiedades, donde $f, g, h \in \text{Dir}(\mathbb{M}(X, q))$ y $\delta, \gamma \in \mathbb{C}$*

- (a) $f + g = g + f$.
- (b) $f + (g + h) = (f + g) + h$.
- (c) *Si 0 está definida por $0(a) = 0$ para todo $a \in \mathbb{M}(X, q)$, entonces para toda $f \in \text{Dir}(\mathbb{M}(X, q))$ se tiene:*

$$0 + f = f.$$

- (d) *Dada $f \in \text{Dir}(\mathbb{M}(X, q))$, la función $-f$, definida por $(-f)(a) = -f(a)$, para todo $a \in \mathbb{M}(X, q)$, satisface:*

$$f + (-f) = 0.$$

- (e) $f \star g = g \star f$.

- (f) $(f \star g) \star h = f \star (g \star h)$
 (g) Si I esta definida por $I(1) = 1$; $I(a) = 0$ para todo $a \neq 1$, entonces para todo $f \in \text{Dir}(\mathbb{M}(X, q))$ se tiene:

$$I \star f = f.$$

- (h) $f \star (g + h) = f \star g + f \star h$.
 (i) $\delta(f + g) = \delta f + \delta g$.
 (j) $(\delta + \gamma)f = \delta f + \gamma f$.
 (k) $(\delta\gamma)f = \delta(\gamma f)$.

Demostración. A título de ejemplo demostraremos sólo el literal (h), dejando las otras al cuidado del lector. Sea $a \in \mathbb{M}(X, q)$

$$\begin{aligned} (f \star (g + h))(a) &= \sum_{d|a} f(a)(g + h)\left(\frac{a}{d}\right) \\ &= \sum_{d|a} f(a)g\left(\frac{a}{d}\right) + f(a)h\left(\frac{a}{d}\right) \\ &= \sum_{d|a} f(a)g\left(\frac{a}{d}\right) + \sum_{d|a} f(a)h\left(\frac{a}{d}\right) \\ &= (f \star g)(a) + (f \star h)(a) \end{aligned}$$

con lo cual se establece el resultado. \checkmark

Las propiedades (a)–(h) nos muestran que $\text{Dir}(\mathbb{M}(X, q))$ conforma un anillo con elemento identidad para las operaciones definidas por (1) y (2), y la conjunción de aquellas con las propiedades (i)–(k) nos muestran que es además una \mathbb{C} -álgebra para las operaciones definidas por (1),(2) y (3).

Proposición 3.2. Si f es una función aritmética con $f(1) \neq 0$, entonces existe una función aritmética f^{-1} , llamada la inversa de Dirichlet de f , tal que:

$$f \star f^{-1} = I = f^{-1} \star f. \quad (4)$$

Más aún, f^{-1} está dada recursivamente por:

$$f^{-1}(1) = \frac{1}{f(1)},$$

$$f^{-1}(a) = -\frac{1}{f(1)} \left[\sum_{\substack{d|a \\ \text{gr}(d) < \text{gr}(a)}} f^{-1}(d) f\left(\frac{a}{d}\right) \right] \quad (5)$$

Demostración. La demostración puede hacerse utilizando inducción sobre el grado del polinomio.

Definición 3.4. Una función aritmética f se dice multiplicativa si no es idénticamente cero y si

$$f(ab) = f(a)f(b) \quad \text{cuando } (a, b) = 1, \quad a, b \in \mathbb{M}(X, q).$$

Diremos que la función f es completamente multiplicativa si

$$f(ab) = f(a)f(b) \quad \text{para todo } a, b \in \mathbb{M}(X, q).$$

Proposición 3.3. Si f es multiplicativa entonces $f(1) = 1$

Proposición 3.4. Dada f con $f(1) = 1$. Entonces
a) f es multiplicativa si y solo si:

$$f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k})$$

para todo polinomio irreducible p_i y todo entero $\alpha_i \geq 1$

b) Si f es multiplicativa entonces f es completamente multiplicativa si y solo si:

$$f(p^\alpha) = f(p)^\alpha$$

para todo polinomio irreducible p y todo entero $\alpha \geq 1$.

Proposición 3.5. Si f y g son multiplicativas, entonces $f \star g$ es multiplicativa.

Proposición 3.6. Si g y $f \star g$ son multiplicativas, entonces f es multiplicativa.

4. Algunas funciones aritméticas especiales

Una función aritmética de importancia capital en el caso clásico es la llamada *función de Möbius*. Esta función la generalizaremos a $\mathbb{M}(X, q)$ de la siguiente manera:

$$\mu(a) := \begin{cases} 1 & \text{si } a = 1 \\ (-1)^k & \text{si } a = p_1 \cdots p_k \text{ con } p_i \neq p_j \text{ para } i \neq j \\ 0 & \text{en otro caso} \end{cases}$$

Proposición 4.1. *Sea $a \in \mathbb{M}(X, q)$ entonces :*

$$\sum_{d|a} \mu(d) = \begin{cases} 1 & \text{si } a = 1, \\ 0 & \text{en otro caso.} \end{cases}$$

- Definimos la función aritmética: $u(a) := 1$, para todo $a \in \mathbb{M}(X, q)$.
- La función φ de **Euler**:

$$\varphi(a) := \text{card} \left[\left(\mathbb{F}_q[X]/(a) \right)^\times \right],$$

donde (a) representa el ideal generado por el polinomio $a = a(X)$.

Proposición 4.2. *Para p un polinomio irreducible de grado d , tenemos*

$$\varphi(p^\alpha) = |p|^\alpha - |p|^{\alpha-1}$$

Demostración. La demostración se hace a partir de la definición y de la proposición(2.6).

Proposición 4.3. *Si $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \in \mathbb{M}(X, q)$, entonces*

$$\varphi(a) = |a| \prod_{i=1}^n \left(1 - \frac{1}{|p_i|} \right)$$

Demostración. Es inmediata de la proposición anterior si se observa que si $(m, n) = 1$, donde (m, n) designa al máximo común divisor de los polinomios m y n , entonces

$$\left[\mathbb{F}_q[X]/(mn) \right]^\times = \left[\left(\mathbb{F}_q[X]/(m) \right) \right]^\times \times \left[\left(\mathbb{F}_q[X]/(n) \right) \right]^\times . \quad \square$$

Proposición 4.4. Si $a \in \mathbb{M}(X, q)$, entonces

$$\varphi(a) = \sum_{d|a} \mu(d) \frac{|a|}{|d|} \quad (6)$$

Demostración. Primero veamos que

$$\begin{aligned} \prod_{i=1}^n \left(1 - \frac{1}{|p_i|}\right) &= 1 - \sum \frac{1}{|p_i|} + \sum \frac{1}{|p_i||p_j|} - \\ &\quad \sum \frac{1}{|p_i||p_j||p_k|} + \cdots + \sum \frac{(-1)^s}{|p_{i_1}| \cdots |p_{i_s}|} + \cdots + \frac{(-1)^n}{|p_1|p_2| \cdots |p_n|}, \end{aligned}$$

donde el término $\sum \frac{(-1)^s}{|p_{i_1}| \cdots |p_{i_s}|}$ significa que estamos tomando todos los productos $|p_{i_1}| \cdots |p_{i_s}|$ de s factores irreducibles distintos de a . Notemos que cada uno de estos términos es de la forma $\pm \frac{1}{|d|}$, donde d es un divisor de a que es o 1 o el producto de irreducibles diferentes de a . El numerador ± 1 es exactamente $\mu(d)$. Como $\mu(d) = 0$ si d es divisible por el cuadrado de algún irreducible, vemos que la suma es exactamente la misma que

$$\sum_{d|a} \frac{\mu(d)}{|d|}.$$

Combinando lo anterior con la proposición (4.3) obtenemos el resultado.

✓

La *función de Liouville*:

$$\lambda(a) = \begin{cases} 1 & \text{si } a = 1 \\ (-1)^{(\alpha_1 + \dots + \alpha_k)} & \text{si } a = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \end{cases}$$

Proposición 4.5. Para todo $a \in \mathbb{M}(X, q)$ se tiene:

$$\sum_{d|a} \lambda(d) = \begin{cases} 1 & \text{si } a \text{ es un cuadrado,} \\ 0 & \text{en otro caso.} \end{cases}$$

La demostración es muy similar al caso de los números naturales.

- Las *funciones divisoriales*:

$$\sigma_\alpha(a) = \sum_{d|a} |d|^\alpha,$$

donde α es un número complejo.

Proposición 4.6 (Fórmula de inversión de Möbius). *La ecuación*

$$f(a) = \sum_{d|a} g(d) \tag{7}$$

implica la ecuación

$$g(a) = \sum_{d|a} f(d) \mu\left(\frac{a}{d}\right). \tag{8}$$

Recíprocamente, (8) implica (7).

La demostración se sigue del hecho de que $\mu \star u = I$ (proposición 4.1).

5. Series de Dirichlet

Definición 5.1. *Sea f una función aritmética. Por una serie formal de Dirichlet entenderemos una expresión del siguiente tipo*

$$f(z) = \sum_{a \in \mathbb{M}(X,q)} \frac{f(a)}{|a|^z}.$$

Por el momento dejaremos de lado que como función de la variable compleja z una serie formal de Dirichlet converja o no.

Definición 5.2. *Diremos que dos series*

$$\sum_{a \in \mathbb{M}(X,q)} \frac{f(a)}{|a|^z} \quad \text{y} \quad \sum_{a \in \mathbb{M}(X,q)} \frac{g(a)}{|a|^z}$$

son iguales si $f(a) = g(a)$, para todo $a \in \mathbb{M}(X, q)$.

Definición 5.3. Sean $\sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z}$ y $\sum_{a \in \mathbb{M}(X, q)} \frac{g(a)}{|a|^z}$ dos series y $\delta \in \mathbb{C}$. Entonces definimos

$$\begin{aligned} \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z} + \sum_{a \in \mathbb{M}(X, q)} \frac{g(a)}{|a|^z} &:= \sum_{a \in \mathbb{M}(X, q)} \frac{f(a) + g(a)}{|a|^z} \\ \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z} \sum_{a \in \mathbb{M}(X, q)} \frac{g(a)}{|a|^z} &:= \sum_{a \in \mathbb{M}(X, q)} \sum_{b \in \mathbb{M}(X, q)} \frac{f(a)g(b)}{|a|^z|b|^z} \\ \delta \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z} &:= \sum_{a \in \mathbb{M}(X, q)} \frac{\delta f(a)}{|a|^z}. \end{aligned}$$

Con lo anterior se puede verificar fácilmente que el conjunto de las series formales de Dirichlet con las operaciones anteriores que acabamos de definir conforma una \mathbb{C} -álgebra.

Proposición 5.1. *El álgebra de las funciones aritméticas y el álgebra de las series formales de Dirichlet son isomorfas.*

Demostración. Denotemos con $\text{DIR}(\mathbb{M}(X, q))$ al álgebra de las series formales de Dirichlet y consideremos la siguiente función:

$$\begin{aligned} F : \text{Dir}(\mathbb{M}(X, q)) &\longrightarrow \text{DIR}(\mathbb{M}(X, q)) \\ f &\longmapsto f(z) = \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z}. \end{aligned}$$

Es claro, que los coeficientes $f(a)$ de una de estas series define una función aritmética $f \in \text{Dir}(\mathbb{M}(X, q))$, y, recíprocamente, una función aritmética f define una serie formal de Dirichlet. Además, por la definición (5.2) tenemos que F es inyectiva, teniéndose así que F es una biyección.

Ahora observemos que

$$\begin{aligned}
 F(f + g) &= \sum_{a \in \mathbb{M}(X, q)} \frac{(f + g)(a)}{|a|^z} = \sum_{a \in \mathbb{M}(X, q)} \frac{f(a) + g(a)}{|a|^z} \\
 &= \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z} + \sum_{a \in \mathbb{M}(X, q)} \frac{g(a)}{|a|^z} = F(f) + F(g) \\
 F(\delta f) &= \sum_{a \in \mathbb{M}(X, q)} \frac{(\delta f)(a)}{|a|^z} = \sum_{a \in \mathbb{M}(X, q)} \frac{\delta f(a)}{|a|^z} \\
 &= \delta \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z} = \delta F(f).
 \end{aligned}$$

Por lo tanto para demostrar que F es un isomorfismo de álgebras basta ver que respeta el producto. En efecto, esto resulta de

$$\begin{aligned}
 F((f \star g)) &= \sum_{a \in \mathbb{M}(X, q)} \frac{(f \star g)(a)}{|a|^z} = \sum_{a \in \mathbb{M}(X, q)} \left(\sum_{cb=a} f(c)g(b) \right) |a|^{-z} \\
 &= \sum_{c \in \mathbb{M}(X, q)} \sum_{b \in \mathbb{M}(X, q)} \frac{f(c)g(b)}{|cb|^z} = F(f)F(g).
 \end{aligned}$$

Luego F es un isomorfismo de álgebras. \square

Para el estudio de $\text{Dir}(\mathbb{M}(X, q))$, es conveniente algunas veces considerar la norma $\| \cdot \|$ de una función $f \in \text{Dir}(\mathbb{M}(X, q))$. De hecho esto permite conseguir de la estructura topológica así obtenida resultados puramente algebraicos y, recíprocamente, expresar situaciones algebraicas en términos topológicos.

Definición 5.4. *El orden $\langle f \rangle$ de una función $f \in \text{Dir}(\mathbb{M}(X, q))$ viene dado por:*

$$\langle f \rangle = \begin{cases} \text{mín}\{|a| : f(a) \neq 0\} & \text{si } f \neq 0, \\ \infty & \text{si } f = 0, \end{cases}$$

donde formalmente tomamos $0 = 1/\infty$.

A partir del orden de una función $f \in \text{Dir}(\mathbb{M}(X, q))$ definimos la norma de la siguiente manera.

Definición 5.5. La norma $\| \cdot \|$ de una función $f \in \text{Dir}(\mathbb{M}(X, q))$ está dada por:

$$\|f\| = \frac{1}{\langle f \rangle}.$$

Proposición 5.2. La norma $\| \cdot \|$ es una valuación no arquimediana sobre $\text{Dir}(\mathbb{M}(X, q))$, es decir:

- (a) $\|f\| \geq 0$ y $\|f\| = 0$ si, y solo si, $f = 0$;
- (b) $\|f + g\| \leq \max\{\|f\|, \|g\|\}$;
- (c) $\|f \star g\| = \|f\| \|g\|$.

Demostración. La propiedad (a) resulta del hecho de que $\langle f \rangle \geq 1$ si $f \neq 0$. Por otra parte, (b) se demuestra observando que $\langle f + g \rangle \geq \min\{\langle f \rangle, \langle g \rangle\}$. Para demostrar (c) supongamos que $f \neq 0$ y $g \neq 0$ y trabajemos en el álgebra de las series formales de Dirichlet, observando que $|a|^{-z} = h(z)$ corresponde a la función aritmética definida por $h(a) = 1$ y $h(b) = 0$ para $b \neq a$. Sean, pues, $a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_s$ los elementos de $\mathbb{M}(X, q)$ que cumplen $|a_i| = \langle f \rangle$ y $|b_i| = \langle g \rangle$. Si p_1, p_2, \dots, p_n son los irreducibles que dividen a alguno de los a_i o b_j , entonces las series $|a_1|^{-z}, |a_2|^{-z}, \dots, |a_r|^{-z}, |b_1|^{-z}, |b_2|^{-z}, \dots, |b_s|^{-z}$ están en la subálgebra generada sobre \mathbb{C} por las series $|p_k|^{-z}$ ($k = 1, \dots, n$). Si definimos $p_k \mapsto x_k$, obtenemos un isomorfismo entre las álgebras $\mathbb{C}[p_1, \dots, p_k]$ y $\mathbb{C}[x_1, \dots, x_k]$, donde las x_k son algebraicamente independientes sobre \mathbb{C} . Luego $\mathbb{C}[p_1, \dots, p_k]$ es un dominio de integridad y, por consiguiente, las series

$$\sum_{i=1}^r f(a_i) |a_i|^{-z} \quad \text{y} \quad \sum_{j=1}^s g(b_j) |b_j|^{-z},$$

que son diferentes de la serie nula, tienen un producto no nulo. Esto implica que $f \star g \neq 0$ y que $\langle f \star g \rangle = \langle f \rangle \langle g \rangle$. \square

Proposición 5.3. $\text{Dir}(\mathbb{M}(X, q))$ es un dominio de integridad.

La demostración es inmediata por la proposición anterior.

Proposición 5.4. $\text{Dir}(\mathbb{M}(X, q))$ es un anillo factorial.

Demostración. Como en $\mathbb{M}(X, q)$ el número de irreducibles es infinito enumerable, tenemos que $\mathbb{M}(X, q)$ es algebraicamente isomorfo a \mathbb{N}^*

(véase CARLITZ [9]), lo que implica que $\text{Dir}(\mathbb{M}(X, q))$ es isomorfo a $\text{Dir}(\mathbb{N}^*)$. Pero un teorema de CASHWELL y EVERETT [6] nos dice que ya $\text{Dir}(\mathbb{N}^*)$ es un dominio factorial, teniéndose así el resultado. \checkmark

Proposición 5.5. *Una función $f \in \text{Dir}(\mathbb{M}(X, q))$ es invertible si, y solo si, $\|f\| = 1$.*

Demostración. Por la proposición (3.2), sabemos que f es invertible si, y solo si, $f(1) \neq 0$, lo que es claramente equivalente a decir que $\|f\| = 1$. \checkmark

Proposición 5.6. *$\text{Dir}(\mathbb{M}(X, q))$ es un espacio topológico completo con respecto de $\| \quad \|$.*

Demostración. Sea $f_1, f_2, \dots, f_n, \dots$ una sucesión de Cauchy en $\text{Dir}(\mathbb{M}(X, q))$; es decir una sucesión para la cual, dado $\epsilon > 0$ existe un entero N_ϵ tal que $\|f_m - f_n\| < \epsilon$, para todo $m, n \geq N_\epsilon$. Esto equivale a lo siguiente: $f_m(a) = f_n(a)$ para todo a que cumpla $|a| \leq 1/\epsilon$, si $m, n \geq N_\epsilon$. Lo que implica que dado $a \in \mathbb{M}(X, q)$ la sucesión $f_1(a), f_2(a), \dots, f_n(a), \dots$ es constante a partir de un cierto subíndice $N_{|a|}$. Sea $f(a)$ este valor constante, de modo que $f_n(a) = f(a)$ si $n \geq N_{|a|}$. Como $\{N_{|a|} : |a| \leq 1/\epsilon\}$ es finito, podemos considerar su máximo M_ϵ . Luego, si $|a| \leq 1/\epsilon$, entonces $f_n(a) = f(a)$ si $n \geq M_\epsilon$, o lo que es lo mismo, $\|f_n - f\| \leq \epsilon$ si $n \geq M_\epsilon$. \checkmark

Conectado con la convergencia con respecto de $\| \quad \|$ está el siguiente concepto puramente algebraico: Sea $f_1, f_2, \dots, f_n, \dots$ una sucesión de elementos de $\text{Dir}(\mathbb{M}(X, q))$ tal que, para cada $a \in \mathbb{M}(X, q)$, $f_n(a) \neq 0$ para a lo sumo un número finito de índices n . En tal caso, $\sum_{n=1}^{\infty} f_n$, será llamada una *serie pseudoconvergente*, definiendo su suma por la relación

$$\sum_{n=1}^{\infty} f_n = \sum_{n=1}^{\infty} f_n(z) := \sum_{a \in \mathbb{M}(X, q)} \left(\sum_{n=1}^{\infty} f_n(a) \right) |a|^{-z},$$

donde la suma $\sum_{n=1}^{\infty} f_n(a)$ es de hecho una suma finita.

Proposición 5.7. *$\sum_{n=1}^{\infty} f_n$ es pseudoconvergente si, y solo si, $\sum_{n=1}^{\infty} f_n$ es convergente con respecto de $\| \quad \|$.*

Demostración. (\Leftarrow) Supongamos que la serie sea convergente con respecto de $\|\cdot\|$, o lo que es lo mismo que $\|f_n\| \rightarrow 0$. Entonces, como en la demostración de la proposición anterior, dado $a \in \mathbb{M}(X, q)$, existe un entero positivo N_a tal que $f_n = 0$ para $n \geq N_a$; lo que muestra que la serie es pseudoconvergente.

(\Rightarrow) Recíprocamente, si la serie es pseudoconvergente y teniendo en cuenta que $\{N_a : |a| \leq 1/\epsilon\}$, es finito, al tomar $N_\epsilon = \max\{N_a : |a| \leq 1/\epsilon\}$, vemos que para todo a que cumpla $|a| \leq 1/\epsilon$, $f_n(a) = 0$ si $n \geq N_\epsilon$; es decir $\|f_n\| \rightarrow 0$. \checkmark

Proposición 5.8. *Si $g \in \text{Dir}(\mathbb{M}(X, q))$ y $\sum_{n=1}^{\infty} f_n$ es pseudoconvergente, entonces $\sum_{n=1}^{\infty} (f_n \star g)$ es pseudoconvergente y*

$$\sum_{n=1}^{\infty} (g \star f_n) = g \star \sum_{n=1}^{\infty} f_n.$$

Demostración. La serie $\sum_{n=1}^{\infty} (g \star f_n)$ es pseudoconvergente pues $\|g \star f_n\| = \|g\| \|f_n\| \rightarrow 0$ si $\|f_n\| \rightarrow 0$. Por otra parte, si $h = \sum_{n=1}^{\infty} f_n$, tenemos

$$\begin{aligned} \sum_{n=1}^{\infty} (g \star f_n) &= \sum_{n=1}^{\infty} (g(z) f_n(z)) = \sum_{a \in \mathbb{M}(X, q)} \left(\sum_{n=1}^{\infty} (g \star f_n)(a) \right) |a|^{-z} \\ &= \sum_{a \in \mathbb{M}(X, q)} \left((g \star \sum_{n=1}^{\infty} f_n)(a) \right) |a|^{-z} = \sum_{a \in \mathbb{M}(X, q)} (g \star h)(a) |a|^{-z} \\ &= g(z) h(z) = g \star \sum_{n=1}^{\infty} f_n, \end{aligned}$$

puesto que $\sum_{n=1}^{\infty} (g \star f_n)(a)$ es una suma finita. \checkmark

6. La función zeta

En esta sección nos interesa la convergencia de las funciones $f(z)$ definidas anteriormente. Para estudiarla hacemos $z = \sigma + it \in \mathbb{C}$ y recordemos que $\|b\|^z = |b|^\sigma$ para todo $b \in \mathbb{M}(X, q)$.

Proposición 6.1. *La serie de Dirichlet $\sum_{a \in \mathbb{M}(X,q)} |a|^{-z}$, converge absolutamente para $\sigma > 1$. La suma de esta serie se denota con $\zeta(z)$ y se llama la función zeta de Riemann.*

Demostración. No es difícil ver que el número de polinomios de grado n en $\mathbb{M}(X, q)$ es q^n . Por lo tanto tenemos

$$\left| \sum_{a \in \mathbb{M}(X,q)} \frac{1}{|a|^z} \right| = \left| \sum_{d=0}^{\infty} \frac{q^d}{q^{dz}} \right| \leq \sum_{d=0}^{\infty} \left| \frac{q^d}{q^{dz}} \right| = \sum_{d=0}^{\infty} \left(\frac{1}{q^{\sigma-1}} \right)^d.$$

Esta última serie es una serie geométrica que converge si $\frac{1}{q^{\sigma-1}} < 1$ o equivalentemente, converge si $\sigma - 1 > 0$, teniéndose así la convergencia absoluta para $\sigma > 1$. Su suma está dada por

$$\zeta(s) = \frac{1}{1 - \frac{1}{q^{\sigma-1}}},$$

con lo que se termina la demostración. \square

Proposición 6.2. *Dadas dos funciones $f(z)$ y $g(z)$ representadas por las series de Dirichlet*

$$f(z) = \sum_{a \in \mathbb{M}(X,q)} \frac{f(a)}{|a|^z} \quad \text{convergente para } \sigma > u$$

y

$$g(z) = \sum_{a \in \mathbb{M}(X,q)} \frac{g(a)}{|a|^z} \quad \text{convergente para } \sigma > v,$$

entonces, en el semiplano donde ambas series convergen absolutamente, tenemos

$$f(z)g(z) = \sum_{a \in \mathbb{M}(X,q)} \frac{h(a)}{|a|^z}, \tag{9}$$

donde $h = f \star g$.

Demostración. Como $f(z), g(z)$ son absolutamente convergentes entonces su producto es absolutamente convergente en el semiplano donde

ambas series convergen y además su suma está dada por $f(z)g(z)$. Por la proposición (5.1) tenemos que $h = f \star g$. \square

Utilizando la anterior proposición, vamos a mostrar que las series de Dirichlet correspondientes a las funciones aritméticas μ , ϕ , y λ se pueden expresar en términos de la función ζ . En efecto:

1) Como ambas series $\zeta(z)$ y $\mu(z)$ convergen absolutamente para $\sigma > 1$, entonces por la ecuación (9) tenemos que:

$$\zeta(z)\mu(z) = \zeta(z) \sum_{a \in \mathbb{M}(X,q)} \frac{\mu(a)}{|a|^z} = 1 \quad \text{si } \sigma > 1.$$

En particular, esto muestra que $\zeta(z) \neq 0$ si $\sigma > 1$ y que

$$\mu(z) = \frac{1}{\zeta(z)} \quad \text{si } \sigma > 1.$$

2) Tomando $\zeta(z)$ y $\varphi(z)$, tenemos que como $\varphi(a) \leq |a|$ entonces la serie $\varphi(z)$ converge absolutamente para $\sigma > 2$, lo que implica que

$$\zeta(z)\varphi(z) = \zeta(z) \sum_{a \in \mathbb{M}(X,q)} \frac{\varphi(a)}{|a|^z} = \sum_{a \in \mathbb{M}(X,q)} \frac{|a|}{|a|^z} = \zeta(z-1) \quad \text{si } \sigma > 2.$$

De donde

$$\varphi(z) = \frac{\zeta(z-1)}{\zeta(z)} \quad \text{si } \sigma > 2.$$

3) Si tomamos $\zeta(z)$ y $g(a) = |a|^\alpha$ tenemos que

$$\zeta(z)\zeta(z-\alpha) = \sum_{a \in \mathbb{M}(X,q)} \frac{\sigma_\alpha(a)}{|a|^z} \quad \text{si } \sigma > \max\{1, 1 + \operatorname{Re}(\alpha)\}.$$

4) Si tomamos $\zeta(z)$ y $\lambda(z)$ entonces

$$\begin{aligned} \zeta(z)\lambda(z) &= \zeta(z) \sum_{a \in \mathbb{M}(X,q)} \frac{\lambda(a)}{|a|^z} = \sum_{\substack{a \in \mathbb{M}(X,q) \\ a=b^2 \text{ para algún } b}} \frac{1}{|a|^z} = \\ &= \sum_{b \in \mathbb{M}(X,q)} \frac{1}{|b|^{2z}} = \zeta(2z), \end{aligned}$$

de donde tenemos que

$$\lambda(z) = \frac{\zeta(2z)}{\zeta(z)} \quad \text{si } \sigma > 1.$$

Queremos ahora expresar las anteriores funciones como productos infinitos.

Proposición 6.3. *Sea $f \in \text{Dir}(\mathbb{M}(X, q))$ multiplicativa. Si la serie $\sum_{a \in \mathbb{M}(X, q)} f(a)$ es absolutamente convergente, entonces su suma puede expresarse como el producto infinito absolutamente convergente siguiente*

$$\sum_{a \in \mathbb{M}(X, q)} f(a) = \prod_p \{1 + f(p) + f(p^2) + \dots\}, \quad (10)$$

extendido sobre todos los irreducibles. Si f es completamente multiplicativa, el producto se simplifica y toma la forma

$$\sum_{a \in \mathbb{M}(X, q)} f(a) = \prod_p \frac{1}{1 - f(p)}. \quad (11)$$

Cada uno de estos productos se llama un producto de Euler.

Basta adaptar la demostración que se encuentra en [5, pág. 230] al caso de los polinomios.

Aplicando la anterior proposición a las series de Dirichlet absolutamente convergentes tenemos inmediatamente el siguiente resultado

Proposición 6.4. *Si $f(z)$ converge absolutamente para $\sigma > \sigma_a$, y si f es multiplicativa entonces*

$$f(z) = \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z} = \prod_p \left\{ 1 + \frac{f(p)}{|p|^z} + \frac{f(p^2)}{|p|^{2z}} + \dots \right\} \quad \text{si } \sigma > \sigma_a. \quad (12)$$

Si f es completamente multiplicativa tenemos

$$f(z) = \sum_{a \in \mathbb{M}(X, q)} \frac{f(a)}{|a|^z} = \prod_p \frac{1}{1 - f(p)|p|^{-z}} \quad \text{si } \sigma > \sigma_a.$$

Demostración. Basta aplicar la proposición anterior a la serie $f(z) = \sum_{a \in \mathbb{M}(X, q)} f(a)|a|^{-z}$. \square

Proposición 6.5. *Por la proposición anterior tenemos*

$$\begin{aligned}\zeta(z) &= \sum_{a \in \mathbb{M}(X, q)} \frac{1}{|a|^z} = \prod_p \frac{1}{1 - |p|^{-z}}, \quad \text{si } \sigma > 1; \\ \frac{1}{\zeta(z)} &= \mu(z) = \prod_p (1 - |p|^{-z}), \quad \text{si } \sigma > 1; \\ \frac{\zeta(z-1)}{\zeta(z)} &= \varphi(z) = \prod_p \frac{1 - |p|^{-z}}{1 - |p|^{1-z}}, \quad \text{si } \sigma > 2; \\ \zeta(z)\zeta(z-\alpha) &= \sum_{a \in \mathbb{M}(X, q)} \frac{\sigma_\alpha(a)}{|a|^z} \\ &= \prod_p \frac{1}{(1 - |p|^{-z})(1 - |p|^{\alpha-z})}, \quad \text{si } \sigma > \max\{1, 1 + \operatorname{Re}(\alpha)\}; \\ \frac{\zeta(2z)}{\zeta(z)} &= \lambda(z) = \prod_p \frac{1}{1 + |p|^{-z}}, \quad \text{si } \sigma > 1.\end{aligned}$$

7. Agradecimientos

Al profesor VICTOR SAMUEL ALBIS, mis más sinceros agradecimientos por su motivación para realización de este artículo, así como por su esmero y dedicación al corregirlo y guiarme en la elaboración del mismo.

Referencias

- [1] I. N. HERSTEIN. *Topics in Algebra*, New York (Wesley), 1975.
- [2] J. FRALEIGH. *A First Course in Abstract Algebra*, (Addison-Wesley), 1967.
- [3] J. KNOPFMACHER. *Abstract Analytic Number Theory*, New York (Dover), 1990.
- [4] K. IRELAND AND M. ROSEN. *A Classical Introduction to Modern Number Theory*, New York (Springer-Verlag), 1982.
- [5] T. APOSTOL. *Introduction to Analytic Number Theory*, New York (Springer-Verlag), 1976.

- [6] CASHWELL, E. AND C. EVERETT. *The ring of number-theoretic functions*, Pacific J. Math. **9** (1959), 975-985.
- [7] L. CARLITZ. *The arithmetic of polynomials in a Galois field*, Am. J. Math. **54** (1932), 39-50.
- [8] L. CARLITZ. *On polynomials in a Galois field*, Bull. Am. Math. Soc. **38** (1932), 736-744.
- [9] L. CARLITZ. *Rings of arithmetic functions*, Pacific J. Math. **14** (1964), 1165-1171.
- [10] SMITS. *On the group of units of $GF(q)[X]/(a(X))$* , Indag. Math. **44** (1982), págs. 355-358.

(Recibido en enero de 2001; la versión revisada mayo de 2001)

OSCAR FRANCISCO CASAS
DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD NACIONAL DE COLOMBIA
BOGOTÁ, COLOMBIA