Sumas exponenciales, número de soluciones de ecuaciones algebraicas y series de Poincaré

Víctor S. Albis

Universidad Nacional de Colombia, Bogotá,

Edilmo Carvajal Márquez

Universidad Central de Venezuela, Caracas

Introducción

En [16] E. Kummer generaliza las sumas cuadráticas de Gauss a los anillos $\mathbb{Z}/p^\ell\mathbb{Z}$, donde p es un número primo y $\ell > 0$ es un número natural, y obtiene algunas de sus más importantes propiedades. Usando el teorema chino de los restos estas sumas y sus propiedades se pueden extender a los anillos $\mathbb{Z}/m\mathbb{Z}$, en particular, la representación de las funciones aritméticas módulo m como *series de Fourier discretas* (*finitas*) (véase, por ejemplo, [4, Chap. x]). En el siglo XX se estudian las sumas de Gauss en un cuerpo finito $\mathbb{F}_q$, $q = p^t$, donde p es un número primo y $t > 1$, para, por ejemplo, estudiar el número de soluciones de formas en $\mathbb{F}_q[t_1, \dots, t_n]$ (véase [14]) o decidir si un polinomio $f(t_1, \dots, t_n) \in \mathbb{F}_q[t_1, \dots, t_n]$ es o no un polinomio de permutación (veánse [23] y [24]). Dada la estrecha analogía entre los anillos $\mathbb{Z}$ y $\mathbb{F}_q[X]$, la generalización natural la hace L. Carlitz en [5] y [6] y la precisa luego Cohen en [9], quienes obtienen análogamente que toda función aritmética definida sobre $\mathbb{F}_q[X]$, módulo un polinomio unitario $h(X)$, también admite una serie de Fourier discreta. En la década de los años 50 del siglo pasado, E. Lamprecht [17] extiende la noción y las propiedades de las sumas de Gauss a una amplia clase de anillos finitos conmutativos. En un informe posterior [20], Carlos J. Moreno expone los resultados de Gauss, Kummer y Lamprecht e indica cómo, bajo ciertas condiciones bastante naturales, los resultados sobre sumas de Gauss tienen análogos a los resultados de Kummer. Esclarece también su importancia, tanto en el caso clásico como en desarrollos recientes, en áreas tan diversas como el procesamiento de señales digitales, el desarrollo de códigos con control de errores y el *método de la fase estacionaria* de **Igusa** [3], por sólo mencionar algunas. En 1967, K. Nageswara Rao [21] extiende resultados previos en el caso racional sobre el número de soluciones de ciertas ecuaciones algebraicas (algunas con condiciones partitivas) (por ejemplo, [10], [11], [12] y [22]) al caso de los anillos $\mathbb{F}_q[X]/(h(X))$, donde $h(X)$ es un polinomio unitario. Nuestro propósito en este artículo es presentar de una manera un poco diferente los resultados de K. Nageswara Rao, en forma tal que nos permitan escribir las *series de Poincaré* (véase *infra* y también [1], [2] y [3]) de las ecuaciones algebraicas estudiadas. En la primera sección explicitaremos, en primer lugar, las estructuras de los anillos $\Lambda = \mathbb{F}_q[X]/(h(X))$ y $L_v = \mathbb{F}_q[X]/(p(X)^v)$, donde $p(X) \in \mathbb{F}_q[X]$ es un polinomio irreducible unitario. En segundo lugar, estableceremos las sumas exponenciales definidas sobre estos anillos y sus propiedades (esto en beneficio de la exposición). En la segunda sección, definimos las sumas de Gauss y Ramanujan en este contexto En la tercera sección aplicaremos los anteriores resultados para obtener un análogo de viejos resultados de G. Libri ([18] y [19]), el cual usaremos para obtener el número de soluciones de ciertas ecuaciones algebraicas definidas sobre las $L-$álgebras sobre Λ y L_v, recobrando algunos de los resultados en [21] y escribiendo las correspondientes series de Poincaré.

1. Notaciones y preliminares

Sean $K = \mathbb{F}_q$ un cuerpo finito con $q = p^t$ (t entero positivo) elementos. Si F es una extensión de K de grado $s = [F : K]$, para $\alpha \in F$, definimos la *traza de* α *sobre* K por la relación

$$\mathrm{tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}} .$$

La siguiente proposición reúne las principales propiedades de la función $\mathrm{tr}_{F/K}$ (véase [14, Chap. xxx]).

Proposición 1. *Sean $K \subseteq F$ cuerpos finitos. Si α, $\beta \in F$ y $a \in K$, entonces*

i) $\mathrm{tr}_{F/K}(\alpha) \in K$.
ii) $\mathrm{tr}_{F/K}(\alpha+\beta) = \mathrm{tr}_{F/K}(\alpha) + \mathrm{tr}_{F/K}(\beta)$.
iii) $\mathrm{tr}_{F/K}(a\alpha) = a\mathrm{tr}_{F/K}(\alpha)$.
iv) $\mathrm{tr}_{F/K} : F \to K$ *es sobreyectiva.*

Si $h(X) = \alpha p_1(X)^{a_1} \cdots p_r(X)^{a_r} \in \mathbb{F}_q[X]$, donde $\alpha \in \mathbb{F}_q^\times$ y $p_i(X)$ un polinomio irreducible en $\mathbb{F}_q[X]$, designamos con $(h(X))$ al ideal generado por este polinomio. El teorema chino de los restos para el anillo de polinomios $\mathbb{F}_q[X]$ nos dice:

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

y

$$[\mathbb{F}_q[X]/(h(X))]^\times = \prod_{i=1}^{r} [\mathbb{F}_q[X]/(p_i(X)^{a_i})]^\times. \tag{2}$$

Por tanto, podemos restringir nuestro estudio a los anillos de la forma $\mathbb{F}_q[X]/(p(X)^v)$ donde $p(X)$ es un polinomio irreducible. Es bien conocido que $\mathbb{F}_q[X]/(p(X)) = L$ es un cuerpo finito que contiene una copia isomorfa de $\mathbb{F}_q$ y si el grado de $p(X)$ es d, entonces el grado de la extensión $L/\mathbb{F}_q$ es d. En consecuencia, L tiene q^d elementos. Para estos anillos residuales se tiene los siguientes resultados, expuestos de manera detallada en [2].

Proposición 2. *Con las anteriores notaciones se tiene:*

i) $\mathbb{F}_q[X]/(p(X)^v)$ *contiene un cuerpo* L *isomorfo a* $\mathbb{F}_q[X]/(p(X))$.
ii) $\mathbb{F}_q[X]/(p(X)^v) = L_v$ *es una* L*-álgebra de dimensión* v *con* q^{vd} *elementos.*
iii) $L_v = \{\lambda(z_v) = \lambda_0 + \lambda_1 z_v + \cdots + \lambda_{v-1} z_v^{v-1} \ : \lambda_i \in L\}$, *donde* $z_v^i \neq 0$ *para* $i = 1, 2, \ldots, v-1$ *y* $z_v^k = 0$ *si* $k \geq v$. *Además el conjunto* $\{1, z_v, \ldots, z_v^{v-1}\}$ *constituye una base de esta* L*-álgebra.*
iv) $L_v^\times = L^\times \times \{1 + \lambda_1 z_v + \lambda_2 z_v^2 + \cdots + \lambda_{v-1} z_v^{v-1} \ : \lambda_j \in L\}$ *donde* $z_v^i \neq 0$ *para* $i = 1, 2, \ldots, v-1$ *y* $z_v^k = 0$ *si* $k \geq v$. *Por tanto,* $L_v^\times$ *tiene* $(q^d - 1)q^{d(v-1)}$ *elementos.*

Usando las siguientes notaciones $\Lambda = \mathbb{F}_q[X]/(h(X))$ y $L_{v_i} = \mathbb{F}_q[X]/(p_i(X)^{v_i})$ tenemos los siguientes isomorfismos:

$$\Lambda \approx \bigoplus_{i=1}^{r} L_{v_i} \tag{3}$$

$$\Lambda^\times \approx \bigoplus_{i=1}^{r} L_{v_i}^\times \tag{4}$$

De manera que un elemento de la $\mathbb{F}_q$-álgebra Λ es de la forma $(\alpha(z_{v_1}), \ldots, \alpha(z_{v_r}))$ donde $\alpha(z_{v_i})$ es un elemento de la $\mathbb{F}_q$-álgebra L_{v_i} para $i = 1, \ldots, r$. En lo que sigue y si no cabe confusión alguna a $(\alpha(z_{v_1}), \ldots, \alpha(z_{v_r}))$ lo notaremos con $\boldsymbol{\alpha}(z_v)$. Es claro que $\boldsymbol{\alpha}(z_v) \in \Lambda^\times$ si, y sólo si, $\alpha(z_{v_i}) \in L_{v_i}^\times$.

El conjunto $M(X, \mathbb{F}_q)$ de todos lo polinomios unitarios de $\mathbb{F}_q[X]$, conforma un monoide aritmético multiplicativo sobre el cual extendemos la noción de *función multiplicativa* conocida y estudiada extensamente en el caso del monoide multiplicativo de los números naturales (veánse y [2] y [15]). De particular interés aquí son las *funciones mutiplicativas periódicas* de período $h(X) \in M(X, \mathbb{F}_q)$, es decir, funciones aritméticas $F : M(X, \mathbb{F}_q) \to \mathbb{C}$ que cumplen $F(a(X)) = F(b(X))$ cada vez que $a(x) \equiv b(X) (\text{mód } h(X))$. Un ejemplo de esta situación lo constituyen los caracteres de las álgebras finitas Λ y L_v. Más precisamente, si A es una $L-$álgebra unitaria abeliana y finita, una función $\chi : A \to \mathbb{C}$ que satisface las siguientes condiciones:

i) $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$, para todo α y $\beta \in A$.
ii) $\chi(\alpha) = 0$ si α no es invertible.
iii) χ restringida a $A^\times$ es un homomorfismo de grupos con valores en $\mathbb{T} = \{z \in \mathbb{C}\,;\, |z| = 1\}$,

se dice un *carácter multiplicativo de Dirichlet* del álgebra A.

También haremos uso de caracteres aditivos, que no son otra cosa que homomorfismos definidos $\psi : A^+ \to \mathbb{T}$ que cumplen $\psi(\alpha+\beta) = \psi(\alpha)\psi(\beta)$.

Observemos que la restricción de χ a $A^\times$ es un carácter del grupo abeliano finito $A^\times$ y recíprocamente, dado un carácter multiplicativo $\chi^\times$ de $A^\times$ éste se puede extender de manera única a un carácter de Dirichlet χ de A con solo definir $\chi(\alpha) = \chi^\times(\alpha)$ si $\alpha \in A^\times$ y $\chi(\alpha) = 0$ si $\alpha \notin A^\times$.

Por abuso de lenguaje, en lo que sigue designaremos los dos caracteres χ y $\chi^\times$ con el mismo símbolo χ y diremos sencillamente carácter de un álgebra finita A al referirnos a uno de sus caracteres de Dirichlet.

Probaremos a continuación que cada carácter del álgebra Λ es el producto de caracteres de las álgebras L_{v_i} para $i = 1, \ldots, r$. De manera que nuestro estudio de los caracteres del álgebra Λ se puede restringir al estudio de caracteres del álgebra L_v.

Proposición 3. *Dado θ un carácter del álgebra Λ, existen caracteres multiplicativos χ_i del álgebra L_{v_i} para $i = 1, \ldots, r$ tales que $\theta = \prod_{i=1}^r \chi_i$. Y, viceversa, dados caracteres los χ_i del álgebra L_{v_i} para $i = 1, \ldots, r$, se tiene que $\prod_{i=1}^r \chi_i$ es un carácter del álgebra Λ*

Demostración. Supongamos que χ_i, $i = 1, \ldots, r$, son caracteres multiplicativos de L_{v_i} y hagamos $\chi = \prod_{i=1}^r \chi_i$. Veamos que χ es un carácter multiplicativo del álgebra Λ. Tenemos

$$\begin{aligned}\chi(\boldsymbol{\alpha}(z_v)\boldsymbol{\beta}(z_v)) &= \prod_{i=1}^r \chi_i(\alpha(z_{v_i})\beta(z_{v_i}))\\ &= \prod_{i=1}^r \chi_i(\alpha(z_{v_i})) \prod_{i=1}^r \chi_i(\beta(z_{v_i})) = \chi(\boldsymbol{\alpha}(z_v))\chi(\boldsymbol{\beta}(z_v))\end{aligned}$$

En efecto, recordemos que $\boldsymbol{\alpha}(z_v) \notin \Lambda^\times$ si, y sólo si, $\alpha(z_{v_i}) \notin L_{v_i}^\times$ para algún $i = 1, \ldots, r$. En vista de que cada χ_i es un carácter del álgebra L_{v_i} tenemos que si $\boldsymbol{\alpha}(z_v) \notin \Lambda^\times$, $\chi(\boldsymbol{\alpha}(z_v)) = 0$. Por otro lado, $\boldsymbol{\alpha}(z_v) \in \Lambda^\times$ si, y sólo si, $\alpha(z_{v_i}) \in L_{v_i}^\times$ para $i = 1, \ldots, r$ y χ_i restringido a $L_{v_i}^\times$ es un homomorfismo de grupos con valores en $\mathbb{T}$. Por consiguiente, χ, restringido a $\Lambda^\times$, resulta ser un homomorfismo de grupos con valores en $\mathbb{T}$. Es decir, χ es un carácter del álgebra Λ.

Recíprocamente, es claro que para cualquier $\boldsymbol{\alpha}(z_v) \in \Lambda$ se tiene que:

$$\boldsymbol{\alpha}(z_v) = (\alpha(z_{v_1}), 1, \ldots, 1) \ldots (1, \ldots, \alpha(z_{v_i}), \ldots, 1) \ldots (1, \ldots, \alpha(z_{v_r})), \tag{5}$$

de modo que

$$\begin{aligned}\theta(\boldsymbol{\alpha}(z_v)) &= \theta((\alpha(z_{v_1}), 1, \ldots, 1) \ldots (1, \ldots, \alpha(z_{v_i}), \ldots, 1) \ldots (1, \ldots, \alpha(z_{v_r})))\\ &= \theta((\alpha(z_{v_1}), 1, \ldots, 1)) \ldots \theta((1, \ldots, \alpha(z_{v_i}), \ldots, 1)) \ldots \theta((1, \ldots, \alpha(z_{v_r}))). \qquad (6)\end{aligned}$$

Utilizando el isomorfismo evidente

$$1 \times \cdots \times 1 \times L_{v_i} \times 1 \times \cdots \times 1 \approx L_{v_i}, \tag{7}$$

podemos definir el siguiente carácter del álgebra L_{v_i}:

$$\chi_i(\alpha(z_{v_i})) = \theta((1, \ldots, \alpha(z_{v_i}), \ldots, 1)). \tag{8}$$

De (6) y (8) se sigue que

$$\theta(\boldsymbol{\alpha}(z_v)) = \chi_1(\alpha(z_{v_1}))\dots\chi_i(\alpha(z_{v_i}))\dots\chi_r(\alpha(z_{v_r}))\,, \tag{9}$$

tal como se queria. □

El carácter definido de la siguiente manera $\chi_0(\alpha(z_v)) = 1$ si $\alpha(z_v)$ es invertible y $\chi_0(\alpha(z_v)) = 0$ en caso contrario, se llama el *carácter principal* del álgebra L_v. Es claro que $L_v^{\times}$ es un grupo abeliano finito y por tanto de [4, Theo.] tenemos que el grupo de caracteres de Dirichlet de L_v tiene cardinal $(q^d-1)q^{d(v-1)}$.

Los siguientes resultados son análogos de resultados demostrados en [4, págs. –].

Proposición 4. *Si χ es un carácter de L_v, se tiene:*

i) $\chi(1) = 1$.
ii) *Definiendo* $\bar{\chi}(\lambda(z_v)) = \overline{\chi(\lambda(z_v))}$ *para todo* $\lambda(z_v) \in L_v$, $\bar{\chi}$ *es un carácter de* L_v.
iii) *Para todo* $\lambda(z_v) \in L_v^{\times}$ *se tiene* $\bar{\chi}(\lambda(z_v)) = \chi(\lambda(z_v))^{-1} = \chi(\lambda(z_v)^{-1})$

Proposición 5.

$$\sum_{\lambda(z_v)\in L_v} \chi(\lambda(z_v)) = \begin{cases} (q^d-1)q^{d(v-1)}, & \textit{si } \chi = \chi_0, \\ 0, & \textit{si } \chi \neq \chi_0. \end{cases}$$

Proposición 6.

$$\sum_{\chi \text{ carácter de } L_v} \chi(\lambda(z_v)) = \begin{cases} (q^d-1)q^{d(v-1)}, & \textit{si } \lambda(z_v) = 1, \\ 0, & \textit{en otro caso.} \end{cases}$$

Proposición 7. *Sean $\alpha(z_v)$, $\lambda(z_v) \in L_v^{\times}$ y χ un carácter de L_v, entonces*

$$\sum_{\chi \text{ carácter de } L_v} \bar{\chi}(\lambda(z_v))\chi(\alpha(z_v)) = \begin{cases} (q^d-1)q^{d(v-1)}, & \textit{si } \lambda(z_v) = \alpha(z_v), \\ 0, & \textit{en otro caso,} \end{cases}$$

Siguiendo el camino trazado por **Carlitz**, definimos la función τ_v de la L–álgebra L_v en $\mathbb{F}_p$, de la siguiente manera: $\tau_v(\lambda(z_v)) = \tau_v(\lambda_0 + \lambda_1 z_v + \cdots + \lambda_{v-1}z_v^{v-1}) := \operatorname{tr}_{L/\mathbb{F}_p}(\lambda_{v-1})$, y la llamamos la *traza de* $\lambda(z_v)$. Esta definición tiene sentido pues $\lambda_{v-1} \in L$ y L es una extensión finita de $\mathbb{F}_p$. El siguiente resultado se sigue de la definición de τ_v.

Proposición 8. *La función $\tau_v : L_v \to \mathbb{F}_p$ es una aplicación $\mathbb{F}_p$−lineal sobreyectiva.*

Demostración. Es inmediata de las propiedades de la traza definida anteriormente. □

Para abreviar, hacemos $\tau' = \operatorname{tr}_{L/\mathbb{F}_p}$, de modo que

$$\tau_v(\alpha(z_v)) = \operatorname{tr}_{L/\mathbb{F}_p}(\alpha_{v-1}) = \tau'(\alpha_{v-1})\ .$$

Si $\zeta_p = \exp(2\pi i/p)$ es una raíz p-ésima primitiva de la unidad en $\mathbb{C}$, definimos la función

$$e(\alpha) = \zeta_p^{\tau'(\alpha)}, \qquad \alpha \in L$$

y tenemos la siguiente

Proposición 9.

$$\sum_{\beta\in L} e(\alpha\beta) = \begin{cases} q^d, & \textit{si } \alpha = 0, \\ 0, & \textit{en caso contrario} \end{cases}$$

Demostración. Por la sobreyectividad de τ', existe un $\gamma \in L$ tal que $\tau'(\gamma) \neq 0$ de modo que $e(\gamma) \neq 1$. Calculemos ahora la suma,

$$e(\gamma)\sum_{\beta\in L} e(\alpha\beta) = \sum_{\beta\in L} e(\gamma)e(\alpha\beta) = \sum_{\beta\in L} e(\gamma+\alpha\beta) = \sum_{\beta\in L} e(\alpha\delta)\,.$$

Si $\alpha \neq 0$ tomando $\delta = \beta + \dfrac{\gamma}{\alpha}$. Ahora cuando β recorre a L de manera únivoca, δ también lo hace. En consecuencia,

$$e(\gamma)\sum_{\beta\in L} e(\alpha\beta) = \sum_{\delta\in L} e(\alpha\delta) = \sum_{\beta\in L} e(\alpha\beta),$$

de donde, $\{e(\gamma)-1\}\sum_{\beta\in L} e(\alpha\beta) = 0$ y por tanto $\sum_{\beta\in L} e(\alpha\beta) = 0$. Si $\alpha = 0$, entonces $\displaystyle\sum_{\beta\in L} e(\alpha\beta) = \sum_{\beta\in L} 1 = q^d$. □

Designemos con $\boldsymbol{\mu}_p$ al grupo de la raíces p-ésimas de la unidad en $\mathbb{C}$ y definamos $\psi_v : L_v \to \boldsymbol{\mu}_p$ mediante la relación

$$\psi_v(\lambda(z_v)) := \zeta_p^{\tau_v(\lambda(z_v))} = \zeta_p^{\tau'(\lambda_{v-1})}\,.$$

Esta expresión tiene sentido pues $\tau'(\lambda_{v-1}) \in \mathbb{F}_p$.

Proposición 10. *La función ψ_v tiene las siguientes propiedades:*

i) $\psi_v(0) = 1$.
ii) *ψ_v es un epimorfismo del grupo aditivo de la L–álgebra L_v en el grupo multiplicativo $\boldsymbol{\mu}_p$ (es decir, ψ_v es un carácter aditivo).*
iii) *Existe $\lambda(z_v) \in L_v$ tal que $\psi_v(\lambda(z_v)) \neq 1$.*
iv) $\sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)) = 0$.
v) $$\sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)\alpha(z_v)) = \begin{cases} q^{vd}, & \textit{si } \alpha(z_v) = 0, \\ 0, & \textit{en caso contrario.} \end{cases}$$

Demostración. La propiedad i) se sigue de la definición. De la linealidad de la función τ_v y la parte *i)* se sigue que ψ_v es un homomorfismo de grupos. Tome $a \in \boldsymbol{\mu}_p$, existe $b \in \mathbb{F}_p$ tal que $a = \zeta_p^b$. Como τ_v es sobreyectiva existe un $\lambda(z_v) \in L_v$ tal que $\tau_v(\lambda(z_v)) = b$ y por tanto $\psi_v(\lambda(z_v)) = a$. Es decir, ψ_v es un epimorfismo de grupos y esto prueba ii). De lo anterior, iii) es inmediata. Para demostrar iv), observemos que de iii) existe un $\alpha(z_v) \in L_v$ tal que $\psi_v(\alpha(z_v)) \neq 1$. Entonces

$$\psi_v(\alpha(z_v))\sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)) = \sum_{\lambda(z_v)\in L_v} \psi_v(\alpha(z_v)+\lambda(z_v)) = \sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)),$$

donde hemos utilizado ii) y el hecho de que cuando $\lambda(z_v)$ recorre a L_v en forma unívoca, $\alpha(z_v)+\lambda(z_v)$ también lo hace. De aquí resulta

$$\{\psi_v(\alpha(z_v))-1\}\sum_{\lambda(z_v)\in L_v}\psi_v(\lambda(z_v))=0\ .$$

En consecuencia, $\sum_{\lambda(z_v)\in L_v}\psi_v(\lambda(z_v))=0$.

Para la afirmación v), consideremos $\alpha(z_v)=\alpha_0+\alpha_1 z_v+\cdots+\alpha_{v-1}z_v^{v-1}$ y $\lambda(z_v)=\lambda_0+\lambda_1 z_v+\cdots+\lambda_{v-1}z_v^{v-1}$. Tenemos que $\alpha(z_v)\lambda(z_v)=\alpha_0\lambda_0+(\alpha_0\lambda_1+\alpha_1\lambda_0)z_v+\cdots+(\sum_{k=0}^{v-1}\alpha_k\lambda_{v-1-k})z_v^{v-1}$, pues $z_v^k=0$ si $k\geq v$. Por lo tanto,

$$\begin{aligned}\sum_{\lambda(z_v)\in L_v}\psi_v(\alpha(z_v)\lambda(z_v)) &= \sum_{\lambda(z_v)\in L_v}\zeta_p^{\tau_v(\alpha(z_v)\lambda(z_v))}=\sum_{\lambda(z_v)\in L_v}\zeta_p^{\tau'(\sum_{k=0}^{v-1}\alpha_k\lambda_{v-1-k})}\\ &= \sum_{\lambda(z_v)\in L_v}\zeta_p^{\sum_{k=0}^{v-1}\tau'(\alpha_k\lambda_{v-1-k})}\\ &= \sum_{\lambda(z_v)\in L_v}\zeta_p^{\tau'(\lambda_0\alpha_{v-1})}\cdots\zeta_p^{\tau'(\lambda_{v-1}\alpha_0)}\ .\end{aligned}$$

Esta última suma es igual a la suma sobre todas las v-plas $(\lambda_0,\lambda_1,\ldots,\lambda_{v-1})$ donde $\lambda_i\in L_v$. De aquí se sigue:

$$\begin{aligned}\sum_{\lambda(z_v)\in L_v}\zeta_p^{\tau'(\lambda_0\alpha_{v-1})}\cdots\zeta_p^{\tau'(\lambda_{v-1}\alpha_0)} &= \sum_{(\lambda_0,\lambda_1,\ldots,\lambda_{v-1})}\zeta_p^{\tau'(\lambda_0\alpha_{v-1})}\cdots\zeta_p^{\tau'(\lambda_{v-1}\alpha_0)}\\ &= \sum_{\lambda_0\in L}\zeta_p^{\tau'(\lambda_0\alpha_{v-1})}\cdots\sum_{\lambda_{v-1}\in L}\zeta_p^{\tau'(\lambda_{v-1}\alpha_0)}\\ &= \sum_{\lambda_0\in L}e(\lambda_0\alpha_{v-1})\cdots\sum_{\lambda_{v-1}\in L}e(\lambda_{v-1}\alpha_0)=q^{vd}\end{aligned}$$

cuando $\alpha_0=\cdots=\alpha_{v-1}=0$, y 0 en caso contrario usando la proposición 9. □

A continuación extendemos las funciones τ_v y ψ_v a la $\mathbb{F}_q$-álgebra Λ. Definimos la funcion τ^* de la siguiente manera:

$$\tau^*(\boldsymbol{\lambda}(z_v)):=\sum_{i=1}^{r}\tau_{v_i}(\lambda(z_{v_i}))\,, \tag{10}$$

donde $\lambda(z_{v_i})\in L_{v_i}$ y τ_{v_i} es la correspondiente función τ sobre cada L_i-álgebra L_{v_i} para $i=1,\ldots,r$. De manera que tenemos la siguiente proposición análoga a la proposición 8.

Proposición 11. *La función τ^* es una aplicación $\mathbb{F}_p-$lineal sobreyectiva del álgebra Λ en $\mathbb{F}_p$.*

Extendamos ahora la función ψ_v para ello definimos la función $\psi^* : \bigoplus_{i=1}^{r} L_{v_i} \to \boldsymbol{\mu}_p$ mediante la relación:

$$\begin{aligned} \psi^*(\boldsymbol{\lambda}(z_v)) :&= \zeta_p^{\tau^*(\boldsymbol{\lambda}(z_v))} = \zeta_p^{\sum_{i=1}^{r} \tau_{v_i}(\lambda(z_{v_i}))} \\ &= \zeta_p^{\tau_{v_1}(\lambda(z_{v_1}))} \zeta_p^{\tau_{v_r}(\lambda(z_{v_r}))} \\ &= \psi_{v_1}(\lambda(z_{v_1})) \cdots \psi_{v_r}(\lambda(z_{v_r})) \end{aligned} \tag{11}$$

En la siguiente proposición presentamos algunas propiedades de esta función:

Proposición 12. i) $\psi^*(0, \ldots, 0) = 1$.

ii) *ψ^* es un epimorfismo del grupo aditivo de la $\mathbb{F}_q$–álgebra Λ en el grupo multiplicativo $\boldsymbol{\mu}_p$.*

iii) *Existe $\boldsymbol{\lambda}(z_v) \in L_v$ tal que $\psi^*(\boldsymbol{\lambda}(z_v)) \neq 1$.*

iv) $\sum_{\boldsymbol{\lambda}(z_v)\in\Lambda} \psi^*(\boldsymbol{\lambda}(z_v)) = 0$.

v) $$\sum_{\boldsymbol{\lambda}(z_v)\in\Lambda} \psi^*(\boldsymbol{\lambda}(z_v)\boldsymbol{\alpha}(z_v)) = \begin{cases} q^m, & \text{si } \boldsymbol{\alpha}(z_v) = 0, \\ 0, & \text{en caso contrario.} \end{cases}$$

donde $m = d_1 v_1 + \cdots + d_r v_r$.

Demostración. La parte $i)$ es inmediata de la definición de ψ^*. Las partes $ii)$ y $iii)$ se sigue del hecho que la función τ_{v_1} es sobreyectiva de acuerdo a la proposición 8. Para probar $iv)$, utilice $iii)$. En $v)$, si $\boldsymbol{\alpha}(z_v) = 0$ la suma tiene el valor q^m. Consideremos el caso en que $\alpha(z_{v_i}) \neq 0$ para algún i.

$$\begin{aligned} &\sum_{\boldsymbol{\lambda}(z_v)\in\Lambda} \psi^*(\boldsymbol{\lambda}(z_v)\boldsymbol{\alpha}(z_v)) \\ &= \sum_{\boldsymbol{\lambda}(z_v)\in\Lambda} \psi_{v_1}(\lambda(z_{v_1})\alpha(z_{v_1})) \cdots \psi_{v_i}(\lambda(z_{v_i})\alpha(z_{v_i})) \cdots \psi_{v_r}(\lambda(z_{v_r})\alpha(z_{v_r})) \\ &= \sum_{(\lambda(z_{v_1}),\ldots,\lambda(z_{v_r}))\in\Lambda} \psi_{v_1}(\lambda(z_{v_1})\alpha(z_{v_1})) \cdots \psi_{v_i}(\lambda(z_{v_i})\alpha(z_{v_i})) \cdots \psi_{v_r}(\lambda(z_{v_r})\alpha(z_{v_r})) \\ &= \sum_{\lambda(z_{v_1})\in L_{v_1}} \psi_{v_1}(\lambda(z_{v_1})\alpha(z_{v_1})) \cdots \sum_{\lambda(z_{v_i})\in L_{v_i}} \psi_{v_i}(\lambda(z_{v_i})\alpha(z_{v_i})) \cdots \sum_{\lambda(z_{v_r})\in L_{v_r}} \psi_{v_r}(\lambda(z_{v_r})\alpha(z_{v_r})) \\ &= 0 \end{aligned}$$

donde hemos utilizado que $\alpha(z_{v_i}) \neq 0$ y la proposición 10,v). □

A continuación mostramos la existencia de una serie de Fourier finita para las funciones aritméticas modulares. Para empezar, para $\alpha(z_v) \in L_v$, definimos

$$\varepsilon_{\sigma(z_v)}(\alpha(z_v)) := \psi_v(\alpha(z_v)\sigma(z_v)) .$$

Proposición 13. *Si $\alpha(z_v)$, $\beta(z_v)$, $\gamma(z_v)$, $\sigma(z_v)$ y $\sigma_1(z_v) \in L_v$, tenemos:*

i) $\varepsilon_{\sigma(z_v)}(\alpha(z_v)) = \varepsilon_{\alpha(z_v)}(\sigma(z_v))$.

ii) $\varepsilon_{\sigma(z_v)}(\alpha(z_v) + \beta(z_v)) = \varepsilon_{\sigma(z_v)}(\alpha(z_v))\varepsilon_{\sigma(z_v)}(\beta(z_v))$.

iii) $\varepsilon_{\sigma(z_v)+\sigma_1(z_v)}(\alpha(z_v)) = \varepsilon_{\sigma(z_v)}(\alpha(z_v))\varepsilon_{\sigma_1(z_v)}(\alpha(z_v))$.

iv) $\varepsilon_{\sigma(z_v)}(\alpha(z_v)) = \varepsilon_{\sigma_1(z_v)}(\alpha(z_v))$ *si, y sólo si,* $\sigma(z_v) = \sigma_1(z_v)$.

v)

$$
\begin{aligned}
(\varepsilon_{\sigma(z_v)} \cdot \varepsilon_{\sigma_1(z_v)})(\alpha(z_v)) &:= \sum_{\alpha(z_v)=\beta(z_v)+\gamma(z_v)} \varepsilon_{\sigma(z_v)}(\beta(z_v))\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&= \begin{cases} q^{vd}\varepsilon_{\sigma(z_v)}(\alpha(z_v)), & \textit{si } \sigma(z_v)=\sigma_1(z_v), \\ 0, & \textit{en otro caso.} \end{cases}
\end{aligned}
$$

Demostración. Las afirmaciones dadas en i), ii) y iii), se deducen de manera inmediata de las propiedades de la función ψ_v consignadas en la proposición 10. Para iv), utilizamos que $\psi_v(-\alpha(z_v)) = \psi_v(\alpha(z_v))^{-1}$. Para v), observe que

$$
\begin{aligned}
&\sum_{\alpha(z_v)=\beta(z_v)+\gamma(z_v)} \varepsilon_{\sigma(z_v)}(\beta(z_v))\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&= \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v)-\gamma(z_v))\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&= \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v))\varepsilon_{\sigma(z_v)}(-\gamma(z_v))\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&= \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v))\varepsilon_{\sigma_1(z_v)-\sigma(z_v)}(\gamma(z_v)) \\
&= \varepsilon_{\sigma(z_v)}(\alpha(z_v)) \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma_1(z_v)-\sigma(z_v)}(\gamma(z_v)) \\
&= \varepsilon_{\sigma(z_v)}(\alpha(z_v)) \sum_{\gamma(z_v)\in L_v} \psi_v[(\sigma_1(z_v)-\sigma(z_v))\gamma(z_v)] = \varepsilon_{\sigma(z_v)}(\alpha(z_v))q^{vd},
\end{aligned}
$$

cuando $\sigma_1(z_v) = \sigma(z_v)$ y 0 en caso contrario, de acuerdo a la proposición 10,v. □

Como $\varepsilon_{\sigma(z_v)}$ depende de $\sigma(z_v)$, cuando éste varía en L_v tenemos que hay a lo más q^{vd} funciones de este tipo. La siguiente proposición nos dice que hay exactamente q^{vd} funciones.

Proposición 14. *Las q^{vd} funciones $\varepsilon_{\sigma(z_v)}$ son linealmente independientes.*

Demostración. Tomemos $g = \sum_{\sigma(z_v)\in L_v} a_{\sigma(z_v)}\varepsilon_{\sigma(z_v)} = 0$ con $a_{\sigma(z_v)} \in \mathbb{C}$. Usando la parte v) de la proposición anterior, tenemos

$$
g\varepsilon_{\sigma_1(z_v)} = \sum_{\sigma(z_v)\in L_v} a_{\sigma(z_v)}(\varepsilon_{\sigma(z_v)} \cdot \varepsilon_{\sigma_1(z_v)}) = a_{\sigma_1(z_v)}q^{vd}\varepsilon_{\sigma_1(z_v)} = 0
$$

lo cual exige que $a_{\sigma_1(z_v)} = 0$ pues $\varepsilon_{\sigma_1(z_v)} \neq 0$(por definición). □

Proposición 15. *Si F es una función aritmética sobre L_v, entonces de manera única*

$$
F = \sum_{\sigma(z_v)\in L_v} f_{\sigma(z_v)}\varepsilon_{\sigma(z_v)},
$$

donde

$$f_{\sigma(z_v)} = \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v))\varepsilon_{\sigma(z_v)}(-\gamma(z_v)).$$

Demostración. Tomemos un $\alpha(z_v) \in L_v$, tenemos:

$$\begin{aligned}
\sum_{\sigma(z_v)\in L_v} & f_{\sigma(z_v)}\varepsilon_{\sigma(z_v)}(\alpha(z_v)) \\
&= \sum_{\sigma(z_v)\in L_v} \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v))\varepsilon_{\sigma(z_v)}(-\gamma(z_v))\varepsilon_{\sigma(z_v)}(\alpha(z_v)) \\
&= \frac{1}{q^{vd}} \sum_{\sigma(z_v)\in L_v} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v))\varepsilon_{\sigma(z_v)}(\alpha(z_v)-\gamma(z_v)) \\
&= \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v)) \sum_{\sigma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v)-\gamma(z_v)) \\
&= \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v)) \sum_{\sigma(z_v)\in L_v} \psi_v(\sigma(z_v)(\alpha(z_v)-\gamma(z_v)) \\
&= F(\alpha(z_v)),
\end{aligned}$$

de acuerdo a la proposición 10,v). □

Este resultado muestra que para cada función aritmética F de L_v, existe un desarrollo en serie de Fourier finita con respecto a la $\mathbb{C}$-base $\varepsilon_{\sigma(z_v)}$, de la $\mathbb{C}$–álgebra de las funciones aritméticas definidas sobre L_v, donde

$$(F\cdot G)(\alpha(z_v)) := \sum_{\alpha(z_v)=\beta(z_v)+\gamma(z_v)} F(\beta(z_v))G(\gamma(z_v)).$$

Si para $\boldsymbol{\alpha}(z_v) \in \Lambda$ definimos

$$\varepsilon_{\boldsymbol{\sigma}(z_v)}(\boldsymbol{\alpha}(z_v)) := \psi^*(\boldsymbol{\alpha}(z_v)\boldsymbol{\sigma}(z_v))\,,$$

obtenemos proposiciones para el caso del álgebra Λ análogas a las proposiciones 13, 14 y 15 con demostraciones similares, las cuales omitimos.

De esta manera tenemos que para cada función aritmética F del álgebra Λ, existe un desarrollo en serie de Fourier finita con respecto a la $\mathbb{C}$-base $\varepsilon_{\boldsymbol{\sigma(z_v)}}$ de la $\mathbb{C}$–álgebra de las funciones aritméticas definidas sobre Λ, donde

$$(F\cdot G)(\boldsymbol{\alpha}(z_v)) := \sum_{\boldsymbol{\alpha}(z_v)=\boldsymbol{\beta}(z_v)+\boldsymbol{\gamma}(z_v)} F(\boldsymbol{\beta}(z_v))G(\boldsymbol{\gamma}(z_v)).$$

2. Sumas de Gauss y Ramanujan en la L–álgebra L_v

Definimos una *suma de Gauss* de la siguiente manera:

$$g_v(\beta(z_v));\chi) := \sum_{\alpha(z_v)\in L_v^\times} \chi(\alpha(z_v))\psi_v(\alpha(z_v)\beta(z_v))\ ,$$

donde χ es un carácter de la L–álgebra L_v. De la definición de carácter vemos que esta suma se hace sobre los elementos invertibles del álgebra L_v. A continuación demostramos algunas propiedades básicas de estas sumas.

Proposición 16. *Sean χ un carácter de L_v y $\beta(z_v) \in L_v^\times$. Entonces*

$$g_v(\beta(z_v); \chi) = \overline{\chi}(\beta(z_v))g_v(1; \chi) \ .$$

Demostración. Para χ un carácter de L_v, $\chi(\beta(z_v))\overline{\chi}(\beta(z_v)) = 1,$ si $\beta(z_v) \in L_v^\times$. En consecuencia,

$$\chi(\alpha(z_v)) = \chi(\alpha(z_v))\chi(\beta(z_v))\overline{\chi}(\beta(z_v)) = \chi(\alpha(z_v)\beta(z_v))\overline{\chi}(\beta(z_v)) \ ,$$

de aquí se sigue fácilmente el resultado. □

Una suma de Gauss se dice *separable* si

$$g_v(\beta(z_v); \chi) = \overline{\chi}(\beta(z_v))g_v(1; \chi) \ .$$

La proposición anterior nos muestra que $g_v(\beta(z_v); \chi)$ es separable si $\beta(z_v) \in L_v^\times$. Cuando $\beta(z_v) \notin L_v^\times$, tenemos la siguiente

Proposición 17. *Si χ es un carácter de L_v y $\beta(z_v) \notin L_v^\times$, la suma de $g_v(\beta(z_v); \chi)$ es separable si, y sólo si, $g_v(\beta(z_v); \chi) = 0$*

Demostración. Por definición, $\overline{\chi}(\beta(z_v)) = 0$ si $\beta(z_v) \notin L_v^\times$. En consecuencia, $g_v(\beta(z_v); \chi)$ $= 0$ si y sólo si $g_v(\beta(z_v); \chi) = \overline{\chi}(\beta(z_v))g_v(1; \chi)$, es decir, si, y sólo si, $g_v(\beta(z_v); \chi)$ es separable. □

Proposición 18. *Para una suma de Gauss g_v y χ un carácter de L_v, tenemos lo siguiente*

$$g_v(\beta(z_v); \chi) = \begin{cases} q^{d(v-1)}(q^d - 1), & \text{si } \chi = \chi_0 \text{ y } \beta(z_v) = 0, \\ 0, & \text{si } \chi = \chi_0 \text{ y } \beta(z_v) \neq 0, \\ 0, & \text{si } \chi \neq \chi_0 \text{ y } \beta(z_v) = 0, \\ \overline{\chi}(\beta(z_v))g_v(1, \chi), & \chi \neq \chi_0 \text{ y } \beta(z_v) \in L_v^\times \ . \end{cases}$$

Demostración. Se sigue de la definición de carácter principal, de la proposición 10, la proposición 5 y la proposición 16 respectivamente. □

Observe que los casos interesantes se presentan cuando consideramos $\chi \neq \chi_0$ y $\beta(z_v) \notin L_v^\times$.

Proposición 19. *Si $g_v(\alpha(z_v); \chi)$ es separable y $\chi \neq \chi_0$, entonces*

$$|g_v(1; \chi)|^2 = \text{Card } L_v = q^{vd} \ .$$

Demostración. Tenemos que

$$
\begin{aligned}
|g_v(1;\chi)|^2 &= g_v(1;\chi)\overline{g_v(1;\chi)} = g_v(1;\chi) \sum_{\alpha(z_v)\in L_v} \overline{\chi}(\alpha(z_v))\overline{\psi_v(\alpha(z_v))} \\
&= g_v(1;\chi) \sum_{\alpha(z_v)\in L_v} \overline{\chi}(\alpha(z_v))\psi_v(-\alpha(z_v)) \\
&= \sum_{\alpha(z_v)\in L_v} g_v(1;\chi)\overline{\chi}(\alpha(z_v))\psi_v(-\alpha(z_v)) \\
&= \sum_{\alpha(z_v)\in L_v} g_v(\alpha(z_v);\chi)\psi_v(-\alpha(z_v)) \\
&= \sum_{\alpha(z_v)\in L_v} \sum_{\beta(z_v)\in L_v} \chi(\beta(z_v))\psi_v(\alpha(z_v)\beta(z_v))\psi_v(-\alpha(z_v)) \\
&= \sum_{\alpha(z_v)\in L_v} \sum_{\beta(z_v)\in L_v} \chi(\beta(z_v))\psi_v(\alpha(z_v)(\beta(z_v)-1)) \\
&= \sum_{\beta(z_v)\in L_v} \chi(\beta(z_v)) \sum_{\alpha(z_v)\in L_v} \psi_v(\alpha(z_v))(\beta(z_v)-1)) = \chi(1)q^{vd} = \text{Card } L_v,
\end{aligned}
$$

si $\beta(z_v) = 1$, de acuerdo a la proposición 10,v. □

Ejemplo: Para $\chi \neq \chi_0$, tomemos $\gamma(z_v) \in L_v^\times$. De la definición de suma de Gauss es facíl ver que en cada sumando podemos reemplazar a $\alpha(z_v)$ por $\gamma(z_v)\alpha(z_v)$ sin que la suma se altere. Así tenemos que

$$
\begin{aligned}
\overline{g_v(1;\chi)} &= \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\alpha(z_v)\gamma(z_v))\overline{\psi_v}(\gamma(z_v)\alpha(z_v)) \\
&= \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\alpha(z_v))\overline{\chi}(\gamma(z_v))\overline{\psi_v}(\gamma(z_v)\alpha(z_v)) \\
&= \overline{\chi}(\alpha(z_v)) \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\overline{\psi_v}(\gamma(z_v)\alpha(z_v)) \ .
\end{aligned}
$$

Utilizando la proposición 19, tenemos

$$
\begin{aligned}
\chi(\alpha(z_v))q^{vd} &= \chi(\alpha(z_v))g_v(1;\chi)\overline{g_v(1;\chi)} \\
&= \chi(\alpha(z_v))g_v(1;\chi)\overline{\chi}(\alpha(z_v)) \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\overline{\psi_v}(\gamma(z_v)\alpha(z_v)) \\
&= g_v(1;\chi) \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\overline{\psi_v}(\gamma(z_v)\alpha(z_v)) \ .
\end{aligned}
$$

De aquí resulta

$$
\chi(\alpha(z_v)) = \frac{g_v(1;\chi)}{q^{vd}} \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\overline{\psi_v}(\gamma(z_v)\alpha(z_v)).
$$

Si $\alpha(z_v) = 0$, como $\chi(\alpha(z_v)) = 0$ y $\sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v)) = 0$ se conserva la igualdad. La anterior expresión es el desarrollo en *serie de Fourier finita* de $\chi(\alpha(z_v))$ sobre $\mathbb{C}$ (véase la sección anterior).

Definimos una suma de Ramanujan por medio de la siguiente expresión

$$c_v(\beta(z_v)) = \sum_{\alpha(z_v)\in L_v^{\times}} \psi_v[\alpha(z_v)\beta(z_v)].$$

Observemos que si tomamos $\chi = \chi_0$ en la definición de suma de Gauss, vemos que una suma de Ramanujan es un caso especial de una suma de Gauss y tenemos fácilmente la siguiente

Proposición 20.

i) $c_v(0) = \text{Card } L_v^{\times}$.
ii) $c_v(\alpha(z_v)\beta(z_v)) = c_v(\beta(z_v))$ *si* $\alpha(z_v) \in L_v^{\times}$.

Ahora pasamos a definir sumas de Gauss y de Ramanujan en el álgebra Λ. Definimos una suma de Gauss de la siguiente manera:

$$g_h(\boldsymbol{\beta}(z_v)); \chi) = \sum_{\boldsymbol{\alpha}(z_v)\in\Lambda^{\times}} \chi(\boldsymbol{\alpha}(z_v))\psi^*(\boldsymbol{\alpha}(z_v)\boldsymbol{\beta}(z_v)),$$

donde χ es un carácter de la $\mathbb{F}_q$–álgebra Λ.

De la caracterización realizada en la proposición 3, tenemos:

$$\begin{aligned} g_h(\boldsymbol{\beta}(z_v)); \chi) &= \sum_{\boldsymbol{\alpha}(z_v)\in\Lambda^{\times}} \chi(\boldsymbol{\alpha}(z_v))\psi^*(\boldsymbol{\alpha}(z_v)\boldsymbol{\beta}(z_v)) \\ &= g_{v_1}(\beta(z_{v_1})); \chi_1) \cdots g_{v_i}(\beta(z_{v_i})); \chi_i) \cdots g_{v_r}(\beta(z_{v_r})); \chi_r) \end{aligned}$$

en donde hemos tomado $\chi = \prod_{i=1}^{r} \chi_i$.

Tomando $\chi = \chi_0$ en la definición anterior de suma de Gauss en el álgebra Λ obtenemos la suma de Ramanujan:

$$c_h(\boldsymbol{\beta}(z_v)) = \sum_{\boldsymbol{\alpha}(z_v)\in\Lambda^{\times}} \psi^*(\boldsymbol{\alpha}(z_v)\boldsymbol{\beta}(z_v)).$$

3. **Aplicaciones**

En esta sección mostraremos, en primer lugar, cómo se aplican estas sumas para hallar el número de soluciones de algunas ecuaciones algebraicas en las álgebras L_v y Λ. Para tal fin extendemos un resultado clásico en el anillo de los enteros debido a **Libri**(veánse [2], [18], [19] y [13]). En segundo lugar presentamos la versión en el álgebra L_v de un resultado sobre particiones obtenido por **Nageswara Rao** en el anillo de polinomios (véase [21]). Antes de continuar, recordemos que si N_v designa al número de soluciones en L_v^n de la ecuación

$$f(t_1, \dots, t_n) = 0$$

donde $f(t_1,\ldots,t_n)\in L[[Z]][t_1,\ldots,t_n]$, la expresión

$$1+\sum_{v=1}^{\infty} N_v T^v$$

se dice la *serie de Poincaré del polinomio* $f(t_1,\ldots,t_n)$. Se ha conjeturado, tal como el caso racional (demostrado por **Igusa** [1], [3]), que esta serie es siempre el cociente de $\dfrac{R(T)}{Q(R)}$ de dos polinomios $R(T)$, $Q(T)\in\mathbb{Z}[T]$. Como consecuencia de los resultados que siguen, se puede verificar que en los casos que consideramos este es el caso.

3.1. Un análogo de un viejo resultado de Libri ([18], [19] y [13])**.** El análogo, que nos permite calcular en teoría N_v para cada v, es el siguiente:

Proposición 21. *Sean* $F(t_1,\ldots,t_n)\in L_v[t_1,\ldots,t_n]$ *y* N_v *el número de soluciones de la ecuación* $F(t_1,\ldots,t_n)=0$, *entonces*

$$N_v=\frac{1}{q^{vd}}\sum_{\alpha(z_v)\in L_v}\sum_{t_1\in L_v}\cdots\sum_{t_n\in L_v}\psi_v[\alpha(z_v)F(t_1,\ldots,t_n)]$$
$$\frac{1}{q^{vd}}\sum_{\alpha(z_v)\in L_v}\sum_{(t_1,t_2,\ldots,t_n)\in L_v^n}\psi_v[\alpha(z_v)F(t_1,\ldots,t_n)]\,.$$

Demostración. El lado derecho de la anterior igualdad lo podemos escribir de la siguiente manera

$$\frac{1}{q^{vd}}\sum_{\alpha(z_v)\in L_v}\left\{\sum_{\substack{(t_1,\ldots,t_n)\in L_v^n\\ F(t_1,\ldots,t_n)=0}}\psi_v[\alpha(z_v)F(t_1,\ldots,t_n)]\right.$$
$$\left.+\sum_{\substack{(t_1,\ldots,t_n)\in L_v^n\\ F(t_1,\ldots,t_n)\neq 0}}\psi_v[\alpha(z_v)F(t_1,\ldots,t_n)]\right\}$$
$$=\frac{1}{q^{vd}}\sum_{\alpha(z_v)\in L_v}N_v+\left\{\sum_{\substack{(t_1,\ldots,t_n)\in L_v^n\\ F(t_1,\ldots,t_n)\neq 0}}\sum_{\alpha(z_v)\in L_v}\psi_v[\alpha(z_v)F(t_1,\ldots,t_n)]\right\}=N_v$$

donde hemos usado la proposición 10, v). □

Para cada $\alpha(z_v)\in L_v$ definimos $w(\alpha(z_v))$ como el menor exponente de las potencias de z_v que aparecen en $\alpha(z_v)\neq 0$ y $w(0)=0$. De manera que $0\leqslant w(\alpha(z_v))\leqslant v-1$. De la definición tenemos que, si $\alpha(z_v)\in L_v^{\times}$, $w(\alpha(z_v))=0$ ya que $\alpha_0\neq 0$; por otro lado si $w(\alpha(z_v))\neq 0$ tenemos que $\alpha(z_v)\notin L_v^{\times}$ y $\alpha(z_v)\neq 0$.

Proposición 22. *Sean* $\alpha(z_v)\in L_v$ *con* $f(\alpha(z_v))=j$ *y* $\gamma(z_v)=\gamma_0+\gamma_1 z_v+\cdots+\gamma_{v-j}z_v^{v-j}+\cdots+\gamma_{v-1}z_v^{v-1}$ *tal que* $\alpha(z_v)\gamma(z_v)=0$. *Entonces* $\gamma_0=\gamma_1=\cdots=\gamma_{v-j-1}=0$. *Es decir,* $\gamma(z_v)=\gamma_{v-j}z_v^{v-j}+\cdots+\gamma_{v-1}z_v^{v-1}$.

Demostración. Como $w(\alpha(z_v)) = j$ se tiene que $\alpha(z_v) = \alpha_j z_v^j + \cdots + \alpha_{v-1} z_v^{v-1}$ donde los $\alpha_i \in L$ para $i = j, \ldots, v-1$ y $\alpha_j \neq 0$. Realizando el producto e igualando a cero tenemos:

$$\begin{aligned} \gamma_0 \alpha_j &= 0 \\ \gamma_0 \alpha_{j+1} + \gamma_1 \alpha_j &= 0 \\ &\vdots \\ \gamma_0 \alpha_{v-1} + \gamma_1 \alpha_{v-2} + \cdots + \gamma_{v-j-1} \alpha_j &= 0 \end{aligned}$$

recuerde que $z_v^t = 0$ si $t \geqslant v$. Como $\alpha_j \neq 0$, de la primera ecuación se sigue $\gamma_0 = 0$. De la segunda ecuación tenemos $\gamma_1 = 0$ ya que $\gamma_0 = 0$ y $\alpha_j \neq 0$. De manera sucesiva se llega a que $\gamma_0 = \gamma_1 = \cdots = \gamma_{v-j-1} = 0$. Observe que no importa los valores que tomen γ_k para $k \geqslant v - j$ y cuando estos son no nulos muestran que el álgebra L_v tiene divisores de cero. □

A continuación aplicamos la proposición 21 al caso de ecuaciones lineales.

Proposición 23. *Sean $F(t) = \alpha(z_v)t + \beta(z_v) \in L_v[t]$, $\alpha(z_v) \neq 0$, $f(\alpha(z_v)) = j$ y N_v el número de soluciones de la ecuación $F(t) = 0$, entonces*

$$N_v = \begin{cases} q^{dj}, & \text{si } j > 0 \text{ y } \beta(z_v) = 0, \\ q^{dj}, & \text{si } j \geqslant 0 \text{ y } w(\beta(z_v)) \geqslant j, \\ 0, & \text{en otro caso.} \end{cases}$$

Demostración. Sabemos por la proposición anterior que

$$\begin{aligned} q^{vd} N_v &= \sum_{\gamma(z_v) \in L_v} \sum_{t \in L_v} \psi_v[\gamma(z_v) F(t)] = \sum_{\gamma(z_v) \in L_v} \sum_{t \in L_v} \psi_v[\gamma(z_v)(\alpha(z_v)t + \beta(z_v))] \\ &= \sum_{\gamma(z_v) \in L_v} \sum_{t \in L_v} \psi_v[\gamma(z_v)\alpha(z_v)t] \psi_v[\gamma(z_v)\beta(z_v)] \\ &= \sum_{\gamma(z_v) \in L_v} \psi_v[\gamma(z_v)\beta(z_v)] \sum_{t \in L_v} \psi_v[\gamma(z_v)\alpha(z_v)t] \\ &= \sum_{\substack{\gamma(z_v) \in L_v \\ \gamma(z_v)\alpha(z_v) = 0}} \psi_v[\gamma(z_v)\beta(z_v)] q^{vd} \end{aligned} \tag{12}$$

Como $w(\alpha(z_v)) = j$ se tiene que $\alpha(z_v) = \alpha_j z_v^j + \cdots + \alpha_{v-1} z_v^{v-1}$ donde los $\alpha_i \in L$ para $i = j, \ldots, v-1$ y $\alpha_j \neq 0$. De la proposición 22 tenemos $\gamma(z_v) = \gamma_{v-j} z_v^{v-j} + \cdots + \gamma_{v-1} z_v^{v-1}$ y por un simple conteo, tenemos que hay q^{dj} de estos $\gamma(z_v)$, es decir, la suma (12) tiene q^{dj} sumandos.

Si $F(t) = 0$ tiene solución, existe $\sigma(z_v) \in L_v$ tal que $\alpha(z_v)\sigma(z_v) + \beta(z_v) = 0$ de donde $\beta(z_v) = -\alpha(z_v)\sigma(z_v)$, en consecuencia, $w(\beta(z_v)) = w(\alpha(z_v)\sigma(z_v))$. Si tomamos $w(\sigma(z_v)) = k$, como $w(\alpha(z_v)) = j$ se tiene $\beta(z_v) = 0$ ó $w(\beta(z_v)) \geqslant j$. En efecto, $\alpha(z_v)\sigma(z_v) = 0$ si $k + j \geqslant v$ pues $z_v^t = 0$ para todo $t \geqslant v$; en caso contrario

$z_v^{k+j} \neq 0$ y $w(\beta(z_v)) = k + j \geqslant j$. Reemplazando el valor de $\beta(z_v)$ en la suma (12) tenemos:

$$\begin{aligned}
\sum_{\substack{\gamma(z_v)\in L_v\\ \gamma(z_v)\alpha(z_v)=0}} \psi_v[\gamma(z_v)\beta(z_v)]q^{vd} &= \sum_{\substack{\gamma(z_v)\in L_v\\ \gamma(z_v)\alpha(z_v)=0}} \psi_v[\gamma(z_v)(-\alpha(z_v)\sigma(z_v))]q^{vd}\\
&= \sum_{\substack{\gamma(z_v)\in L_v\\ \gamma(z_v)\alpha(z_v)=0}} \psi_v[-(\gamma(z_v)\alpha(z_v))\sigma(z_v)]q^{vd}\\
&= q^{vd}q^{dj}
\end{aligned}$$

de donde $N_v = q^{dj}$.

□

Proposición 24. *Sean* $F(t_1,\dots,t_n) = \beta(z_v)+\alpha_1(z_v)t_1+\dots+\alpha_n(z_v)t_n \in L_v[t_1,\dots,t_n]$, $w(\alpha_i(z_v)) = j_i$, $j = \text{mín}\{j_i\}$ *para* $i = 1,\dots,n$ *y* N_v *el número de soluciones de la ecuación* $F(t_1,\dots,t_n) = 0$*. Entonces*

$$N_v = \begin{cases} q^{dj}(q^{vd})^{n-1}, & \text{si } j > 0 \text{ y } \beta(z_v) = 0,\\ q^{dj}(q^{vd})^{n-1}, & \text{si } j \geqslant 0 \text{ y } w(\beta(z_v)) \geqslant j\ ,\\ 0, & \text{en otro caso.}\end{cases}$$

Demostración. Por la proposición 21 se tiene

$$\begin{aligned}
q^{vd}N_v &= \sum_{\gamma(z_v)\in L_v}\sum_{t_1\in L_v}\cdots\sum_{t_n\in L_v}\psi_v[\gamma(z_v)F(t_1,\dots,t_n)]\\
&= \sum_{\gamma(z_v)\in L_v}\sum_{t_1\in L_v}\cdots\sum_{t_n\in L_v}\psi_v[\gamma(z_v)(\beta(z_v)+\alpha_1(z_v)t_1+\dots+\alpha_n(z_v)t_n)]\\
&= \sum_{\gamma(z_v)\in L_v}\sum_{t_1\in L_v}\cdots\sum_{t_n\in L_v}\psi_v[\gamma(z_v)\beta(z_v)]\psi_v[\gamma(z_v)\alpha_1(z_v)t_1]\dots\psi_v[\gamma(z_v)\alpha_n(z_v)t_n]\\
&= \sum_{\gamma(z_v)\in L_v}\psi_v[\gamma(z_v)\beta(z_v)]\sum_{t_1\in L_v}\psi_v[\gamma(z_v)\alpha_1(z_v)t_1]\cdots\sum_{t_n\in L_v}\psi_v[\gamma(z_v)\alpha_n(z_v)t_n]
\end{aligned}$$

$$\begin{aligned}
&= \sum_{\gamma(z_v)\in L_v}\psi_v[\gamma(z_v)\beta(z_v)]\cdots\sum_{\substack{t_{n-1}\in L_v\\ \alpha_n(z_v)\gamma(z_v)=0}}\psi_v[\gamma(z_v)\alpha_{n-1}(z_v)t_{n-1}]q^{vd}\\
&= \sum_{\substack{\gamma(z_v)\in L_v\\ \alpha_1(z_v)\gamma(z_v)=0,\cdots,\alpha_n(z_v)\gamma(z_v)=0}}\psi_v[\gamma(z_v)\beta(z_v)](q^{vd})^n. \qquad (13)
\end{aligned}$$

Haciendo uso reiterado de la proposición 10,v. Por la proposición 22, $w(\gamma(z_v)) = v - j$ y como $j = \text{mín}\{j_i\}$, es claro que $\alpha_i(z_v)\gamma(z_v) = 0$, para $i = 1,\dots,n$, y la suma (13) tiene q^{dj} sumandos.

Si $F(t_1,\dots,t_n) = 0$ tiene solución existen $\sigma_1(z_v),\dots,\sigma_n(z_v) \in L_v$ tales que

$$\beta(z_v) = -(\alpha_1(z_v)\sigma_1(z_v)+\dots+\alpha_n(z_v)\sigma_n(z_v)). \qquad (14)$$

Por consiguiente, $w(\beta(z_v)) = w(\alpha_1(z_v)\sigma_1(z_v)+\cdots+\alpha_n(z_v)\sigma_n(z_v))$. Tomemos $w(\sigma_i(z_v)) = k_i$ y $k = \text{mín}\{k_i\}$, para $i = 1, \ldots, n$. Dado que $w(\alpha_i(z_v)) \geq j$, tenemos que $\beta(z_v) = 0$ ó $w(\beta(z_v)) \geq j$. En efecto, $\alpha_i(z_v)\sigma_i(z_v) = 0$, para $i = 1, \ldots, n$ si $k + j \geq v$ pues $z_v^t = 0$ para todo $t \geq v$ y por tanto $\beta(z_v) = 0$; también puede suceder que al hacer todas las sumas en (14) de 0 y así $\beta(z_v) = 0$. De lo contrario, existe un $z_v^r \neq 0$ con $k + j <= r < v$ y por tanto $w(\beta(z_v)) = r \geq j$. Reemplazando el valor de $\beta(z_v)$ en (13) se tiene que $N_v = (q^{vd})^{n-1}q^{dj}$. $\square$

Proposición 25. *Sean* $F(t_1, \ldots, t_n) = \beta(z_v) + t_1 + \alpha_2(z_v)t_2^{k_2} + \cdots + \alpha_n(z_v)t_n^{k_n} \in L_v[t_1, \ldots, t_n]$, k_i *enteros positivos para* $i = 2, \ldots, n$ *y* N_v *el número de soluciones de la ecuación* $F(t_1, \ldots, t_n) = 0$. *Entonces*

$$N_v = (q^{vd})^{n-1}$$

Demostración. Nuevamente por la proposición 21 se tiene

$$\begin{aligned}
&q^{vd}N_v = \\
&\sum_{\gamma(z_v)\in L_v}\sum_{t_1\in L_v}\cdots\sum_{t_n\in L_v}\psi_v[\gamma(z_v)(\beta(z_v) + t_1 + \alpha_2(z_v)t_2^{k_2} + \cdots + \alpha_n(z_v)t_n^{k_n})] \\
&= \sum_{\gamma(z_v)\in L_v}\psi_v[\gamma(z_v)\beta(z_v)]\sum_{t_n\in L_v}\psi_v[\gamma(z_v)\alpha_n(z_v)t_n^{k_n}]\cdots\sum_{t_1\in L_v}\psi_v[\gamma(z_v)t_1] \\
&= (q^{vd})^n \ \text{ si } \gamma(z_v) = 0 \text{ de acuerdo a la proposición 10,v.}
\end{aligned}$$

$\square$

3.2. Un resultado de Nageswara Rao. Sea n un entero mayor que cero y $n_1, \ldots, n_v$ enteros mayores o iguales que cero que satisfacen la condición $n = n_1 + \cdots + n_v$. Tome $m_k = n_1 + \cdots + n_k$ con $k = 1, \ldots, v$. Para $\alpha(z_v) \in L_v$ designamos con $N_v(\alpha(z_v))$ al número de soluciones $(\gamma_1(z_v), \ldots, \gamma_n(z_v))$ de la ecuación:

$$\gamma_1(z_v) + \cdots + \gamma_n(z_v) = \alpha(z_v),$$

que satisfacen las condiciones:

$$\begin{aligned}
&w(\gamma_{j_1}(z_v)) = 0\ ,\ j_1 = 1, \ldots, m_1, \text{con } \gamma_{j_1}(z_v) \neq 0, \\
&w(\gamma_{j_2}(z_v)) = 1\ ,\ j_2 = m_1 + 1, \ldots, m_2, \\
&\qquad\vdots \\
&w(\gamma_{j_v}(z_v)) = v - 1\ ,\ j_v = m_{v-1} + 1, \ldots, m_v = n.
\end{aligned}$$

Proposición 26. *Con las anteriores notaciones, tenemos*

$$N_v(\alpha(z_v)) = \frac{1}{q^{vd}}\sum_{l=0}^{v-1}\left\{\prod_{i=1}^{v}c_{v-i+1}^{n_i}(\tau_l^*(z_{v-i+1}))\right\}c_{v-l}(\alpha^*(z_{v-l})).$$

Demostración. Es claro que $N_v(\cdot)$ es una función aritmética. Luego en virtud de la proposición 15 se tiene:

$$N_v(\alpha(z_v)) = \sum_{\tau(z_v)\in L_v} f_{\tau(z_v)}\varepsilon_{\tau(z_v)}(\alpha(z_v)), \tag{15}$$

donde $f_{\tau(z_v)} = \frac{1}{q^{vd}} \sum_{\beta(z_v)\in L_v} N(\beta(z_v))\varepsilon_{\tau(z_v)}(-\beta(z_v))$, es decir,

$$\begin{aligned} f_{\tau(z_v)} &= \frac{1}{q^{vd}} \sum_{\beta(z_v)\in L_v} N_v(\beta(z_v))\psi_v[-\tau(z_v)\beta(z_v)] \\ &= \frac{1}{q^{vd}} \sum_{\beta(z_v)\in L_v} \sum_{\substack{(\beta_1(z_v),\ldots,\beta_n(z_v)) \\ w(\beta_{ji}(z_v))=i-1}} \psi_v[-\tau(z_v)(\beta_1 z_v) + \beta_2(z_v) + \cdots + \beta_n(z_v))] \end{aligned}$$

donde la suma se hace sobre las n-plas $(\beta_1(z_v), \ldots, \beta_n(z_v))$ que satisfacen

$$\beta(z_v) = \beta_1(z_v) + \beta_2(z_v) + \cdots + \beta_n(z_v),$$

y

$$\begin{aligned} w(\beta_{j_1}(z_v)) &= 0\ ,\ j_1 = 1, \ldots, m_1, \text{con } \beta_{j_1}(z_v) \neq 0, \\ w(\beta_{j_2}(z_v)) &= 1\ ,\ j_2 = m_1 + 1, \ldots, m_2, \\ &\vdots \\ w(\beta_{j_v}(z_v)) &= v - 1\ ,\ j_v = m_{v-1} + 1, \ldots, m_v = n \end{aligned}$$

cuyo número es precisamente $N_v(\beta(z_v))$. Utilizando la proposición 10 tenemos:

$$f_{\tau(z_v)} = \frac{1}{q^{vd}} \sum_{\beta(z_v)\in L_v} \sum_{\substack{(\beta_1(z_v),\ldots,\beta_n(z_v)) \\ w(\beta_{ji}(z_v))=i-1}} \prod_{k=1}^{n} \psi_v[-\tau(z_v)\beta_k(z_v)]$$

Haciendo $\beta_{j_i}(z_v) = \beta_{ji}(z_v)$ podemos escribir

$$f_{\tau(z_v)} = \frac{1}{q^{vd}} \sum_{\substack{\beta_{ji}(z_v) \\ w(\beta_{ji}(z_v))=i-1}} \prod_{i=1}^{v}\prod_{j=1}^{n_i} \psi_v[-\tau(z_v)\beta_{ji}(z_v)],$$

reemplazando $\beta_{ji}(z_v)$ por $\sigma(z_v) \in L_v$ tal que $w(\sigma(z_v)) = i - 1$ obtenemos

$$\begin{aligned} f_{\tau(z_v)} &= \frac{1}{q^{vd}} \sum_{\substack{\sigma(z_v) \\ w(\sigma(z_v))=i-1}} \prod_{i=1}^{v}\prod_{j=1}^{n_i} \psi_v[-\tau(z_v)\sigma(z_v)] \\ &= \frac{1}{q^{vd}} \prod_{i=1}^{v}\prod_{j=1}^{n_i} \sum_{\substack{\sigma(z_v) \\ w(\sigma(z_v))=i-1}} \psi_v[-\tau(z_v)\sigma(z_v)] \end{aligned} \tag{16}$$

Como $w(\sigma(z_v)) = i-1$, se tiene que $\sigma(z_v) = \sigma_{i-1} z_v^{i-1} + \cdots + \sigma_{v-1} z_v^{v-1}$ donde $\sigma_{i-1} \neq 0$ y $\sigma_i, \ldots, \sigma_{v-1} \in L$ son arbitrarios. Si tomamos $\tau(z_v) = \tau_0 + \tau_1 z_v + \cdots + \tau_{v-1} z_v^{v-1}$ tenemos

$$\sigma(z_v)\tau(z_v) = \tau_0\sigma_{i-1} z_v^{i-1} + \cdots + (\sum_{k=0}^{v-i} \sigma_{v-k-1}\tau_k) z_v^{v-1}, \tag{17}$$

y aplicando ψ_v se llega a

$$\psi_v[-\sigma(z_v)\tau(z_v)] = \zeta_p^{\operatorname{tr}_{L/\mathbb{F}_p}(-\sum_{k=0}^{v-i} \sigma_{v-k-1}\tau_k)}.$$

De aquí es claro que para hallar el valor de $\psi_v[-\sigma(z_v)\tau(z_v)]$ sólo tienen relevancia los $v - i + 1$ valores $\tau_0, \tau_1, \ldots, \tau_{v-i}$ en la expresión de $\tau(z_v)$ y los $v - i + 1$ valores

$\sigma_{i-1}, \ldots, \sigma_{v-1}$ en la expresión de $\sigma(z_v)$. Además todos estos valores son arbitrarios, a excepción de σ_{i-1}. Debido a esto, consideremos los siguientes elementos sobre el álgebra L_{v-i+1},

$$\begin{aligned}\sigma^*(z_{v-i+1}) &= \sigma_{i-1} + \sigma_i z_{v-i+1} \cdots + \sigma_{v-1} z_{v-i+1}^{v-i},\\ \tau^*(z_{v-i+1}) &= \tau_0 + \tau_1 z_{v-i+1} + \cdots + \tau_{v-i} z_{v-i+1}^{v-i},\end{aligned}$$

de manera que,

$$\psi_{v-i+1}[-\sigma^*(z_{v-i+1})\tau^*(z_{v-i+1})] = \zeta_p^{tr_{L/\mathbb{F}_p}(-\sum_{k=0}^{v-i} \sigma_{v-k-1}\tau_k)} = \psi_v[-\sigma(z_v)\tau(z_v)],$$

es decir, podemos reemplazar la suma

$$\sum_{w(\sigma(z_v))=i-1} \psi_v[-\tau(z_v)\sigma(z_v)],$$

de (16) por la suma

$$\sum_{w(\sigma^*(z_{v-i+1}))=0} \psi_{v-i+1}[-\tau^*(z_{v-i+1})\sigma^*(z_{v-i+1})],$$

que corresponde a la suma de Ramanujan $c_{v-i+1}(\tau^*(z_{v-i+1}))$. De lo anterior tenemos,

$$\begin{aligned}f_{\tau(z_v)} &= \frac{1}{q^{vd}} \prod_{i=1}^{v} \prod_{j=1}^{n_i} \sum_{w(\sigma^*(z_{v-i+1}))=0} \psi_{v-i+1}[-\tau^*(z_{v-i+1})\sigma^*(z_{v-i+1})]\\ &= \frac{1}{q^{vd}} \prod_{i=1}^{v} \prod_{j=1}^{n_i} c_{v-i+1}(\tau^*(z_{v-i+1}))\\ &= \frac{1}{q^{vd}} \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1})). \qquad (18)\end{aligned}$$

Reemplazando (18) en (15) obtenemos,

$$\begin{aligned}N_v(\alpha(z_v)) &= \frac{1}{q^{vd}} \sum_{\tau(z_v)\in L_v} \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1}))\varepsilon_{\tau(z_v)}(-\alpha(z_v))\\ &= \frac{1}{q^{vd}} \sum_{\tau(z_v)\in L_v} \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1}))\psi_v[-\tau(z_v)\alpha(z_v)]\\ &= \frac{1}{q^{vd}} \sum_{j=0}^{v-1} \left\{ \sum_{w(\tau(z_v))=j} \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1}))\psi_v[-\tau(z_v)\alpha(z_v)] \right\}. \qquad (19)\end{aligned}$$

Teníamos que $\tau^*(z_{v-i+1}) = \tau_0 + \tau_1 z_{v-i+1} + \cdots + \tau_{v-i} z_{v-i+1}^{v-i}$. Si $w(\tau(z_v)) = j$ definimos

$$\tau_j^*(z_{v-i+1}) := \begin{cases} \tau_j z_{v-i+1}^{j} + \cdots + \tau_{v-i} z_{v-i+1}^{v-i}, & \text{si } j < v-i+1,\\ 0, & \text{si } j \geq v-i+1, \end{cases} \qquad (20)$$

aplicando (20) a (19) obtenemos,

$$N_v(\alpha(z_v)) = \frac{1}{q^{vd}} \sum_{j=0}^{v-1} \left\{ \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau_j^*(z_{v-i+1})) \sum_{w(\tau(z_v))=j} \psi_v[-\tau(z_v)\alpha(z_v)] \right\},$$

Como $w(\tau(z_v)) = j$ siguiendo el mismo razonamiento realizado en (17) tenemos:

$$N_v(\alpha(z_v)) = \frac{1}{q^{vd}} \sum_{j=0}^{v-1} \left\{ \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau_j^*(z_{v-i+1})) \right\} c_{v-j}(\alpha^*(z_{v-j}))$$

tal como se quería. □

Referencias

[1] **V. S. Albis & R. Chaparro**. *On a conjecture of Borevich and Shafarevich.* Rev. Acad. Colomb. Cienc. **21** (1997), 313–319. [MR:98g:11130]

[2] **Albis, V. S.**, *Lecciones sobre la aritmética de polinomios.* Notas de clase, Departamento de Matemáticas y Estadística, Universidad Nacional de Colombia, Santafé de Bogotá, 1999, capítulos I, II, VI, VII.

[3] **Albis, V. S. & Zúñiga, Wilson**, *Una introducción elemental a la teoría de las funciones zeta locales de Igusa*, Lecturas Matemáticas, **20** (1999), 5–33.

[4] **Apostol, Tom**, *Introduction to Analytic Number Theory*, Springer Verlag, New York, 1976, capítulos 6 y 8.

[5] **Carlitz, L.** *The arithmetic of polynomials in a Galois field.* Am. J. Math. **54** (1932), 39–50.

[6] **Carlitz, L.** *The singular series form sums of squares of polynomials.* Duke Math. J. **14** (1947), 1105–1120.

[7] **Carlitz, L.** *Representation of arithmetic functions in* $GF[p^n, x]$*. I.* Duke Math. J. **14** (1947), 1121–1137.

[8] **Carlitz, L.** *Representation of arithmetic functions in* $GF[p^n, x]$*. II.* Duke Math. J. **15** (1948), 795–801.

[9] **Cohen, E.**, *Arithmetic functions of polynomials*, Proc. Amer. Math. Soc. **3** (1953), 352–358.

[10] **Cohen, E.**, *An extension of Ramanujan sums. II. Additive properties*, Duke Math. J. **22** (1955), 534–550.

[11] **Cohen, E.**, *An extension of Ramanujan sums. III. Connections with totien functions*, Duke Math. J. **22** (1956), 623–650.

[12] **Cohen, E.**, *Representations of even functions* $(\bmod\ r)$*. I. Arithmetical identies*, Duke Math. J. **25** (1958), 401–421.

[13] **Dickson, L. E.**, *History of Number Theory.* 3 vols. Chelsea, New York, 1919.

[14] **Ireland, K. y Rosen, M.**, *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1982, capítulo 8.

[15] **Knopfmacher, John**. *Abstract Analytical Number Theory*, Dover Pub., New York, 1990.

[16] **Kummer, E.**, *Note sur une expression analogue a la resolvante de Lagrange por l'équation* $z^p = 1$, Atti dell'Academia Pontifica de Nouvi Lincei **6** (1852–1853), 237–241.

[17] Lamprecht, E., *Algemeine Theorie der Gaussschien Summen in endliche kommutativen Ringen.*, Math. Nachr. **9** (1953), 149–196.

[18] **G. (conde de) Libri Carucci dalla Sommaia**. *Mémoirs de divers savants.* Acad. Sci. de l'Insitut de France (Math.) **5** (1838), 32. [Leído en 1825]

[19] **G. (conde de) Libri Carucci dalla Sommaia**. *...* . J. für angew. reine Math. **9** (1832), 54.

[20] **Moreno, Carlos J.**, *Exponential sums over finite fields. A report.* Preprint.

[21] **Nageswara Rao, K.**, *Some applications of Carlitz's* η*–sum*, Acta Arithmetica **12** (1967), 213-221.

[22] **Nageswara Rao, K.**, *On a congruence equation and related arithmetical identities*, Monatsh. Math **xx**, 19xx, xxx-xxx.

[23] **Niederreiter, H.** *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. **46** No. 9 (1970), 1001–1005. [MR: 44#5298].

[24] **Niederreiter, H.** *Orthogonal systems of polynomials in finite fields*, Proc. Amer. Math. Soc. **28** (1971), 415–422. [MR:45# 230].

[25] **Smits, T. H. .** *On the group of units of* $GF(q)[X]/(a(X))$. Indag. Math. **44** (1982), 355-358.