ON A CONJECTURE OF BOREVICH AND SHAFAREVICH

por

Víctor Samuel Albis González* & Raúl Chaparro

Resumen

Albis González, V. S. & R. Chaparro: On a conjecture of Borevich and Shafarevich. Rev. Acad. Colomb. Cienc. **21**(80): 313-319, 1997. ISSN 0370-3908.

Z. I. Borevich & I. R. Shafarevich conjeturaron la racionalidad de la serie de Poincaré $\Sigma_{n\geq 0}c_nU^n$, donde $c_0= 1$ y c_n $(n\geq 1)$ designa al número de soluciones de la reducción módulo ℓ^n, ℓ primo racional, de un polinomio $H(t) \in Z_\ell[t]$, $t= (t_1,...,t_r)$. Esta conjetura fue confirmada por J. Igusa, usando el profundo teorema de resolución de singularidades de Hironaka. Más tarde, J. Denef dio una nueva demostración usando esencialmente el hecho de que $\mathbf{Q}_\ell$ admite eliminación de cuantificadores, evitando así el teorema de Hironaka. La misma conjetura está aún sin resolver en el caso de característica > 0, anotándose que ninguna de las técnicas usadas en el caso de característica 0 parece ser apropiada en característica > 0. En esta corta comunicación demostramos la conjetura en característica > 0 para algunos tipos de polinomios, usando métodos elementales.

Palabras claves: Geometría algebraica, cuerpos aritméticos de funciones, series de Poincaré.

Abstract

Z. I. Borevich & I. R. Shafarevich conjectured the rationality of the Poincaré series $\Sigma_{n\geq 0}c_nU^n$, where $c_0= 1$ and c_n $(n\geq 1)$ denotes the number of solutions of the reduction modulo ℓ^n, ℓ a rational prime, of a polynomial $H(t) \in Z_\ell[t]$, $t= (t_1,...,t_r)$. This conjecture was settled in the affirmative by J. Igusa, using Hironaka's deep resolution of singularities teorem. Later on, J. Denef produced a new proof of this result, essentially using the fact that $\mathbf{Q}_\ell$ admits elimination of quantifiers, avoiding thus Hironaka's result. The same conjecture for characteristic > 0 is still an open problem, and none of the techniques used in characteristic 0 seem to help in characteristic > 0. In this short note we prove the conjecture in characteristic > 0 for some special cases of polynomials, using elementary methods.

Key words: Algebraic geometry, arithmetic function fields, Poincaré series.

* Departamento de Matemáticas y Estadística, Universidad Nacional de Colombia, Santafé de Bogotá. Apartado aéreo 91480, Santafé de Bogotá, D.C., 8, Colombia.
Email: valbis@ciencias.ciencias.unal.edu.co; albisf@inter.net.co

§1. Introduction

In [5], Problem 9, page 47, Borevich and Shafarevich asked the following question: given a fixed rational prime ℓ, let $\mathbb{Q}_\ell$ be the field of ℓ-adic numbers and let $\mathbb{Z}_\ell$ be the ring of ℓ-adic integers. For a polynomial $H(t_1,\cdots,t_s) \in \mathbb{Z}_\ell[t_1,\cdots,t_s]$, let $c(n;H)$ (or simply $c(n)$ if there is no possible confusion) denote the number of zeroes of the reduction $H_n(t_1,\cdots,t_s)$ of $H(t_1,\cdots,t_s)$ in the residue ring $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$. Is then the Poincaré series of H

$$P(U;H) := \sum_{n=0}^{\infty} c(n;H)U^n \in \mathbb{Z}[[U]]\,, \qquad (1.1)$$

where $c(0;U) = 1$, a rational function of U ? Partial answers to this question were known before 1973 (for which we refer to [7]), when Igusa ([11], [12], [13]) gave a general affirmative answer, based on Hironaka's resolution of singularities theorem in characteristic zero. His results, however, did not show how to effectively compute (1.1) and thus how to express it as a quotient of two polynomials in U. Later on, in 1984, Denef [7] gave a new and elegant proof of the conjecture, essentially using the fact that $\mathbb{Q}_\ell$ admits elimination of quantifiers, avoiding thus Hironaka's result. Related to this conjecture is the following one by Hayes and Nutt [10]: $P(H;U) = Q(U)/R(U)$, where $Q(U)$ and $R(U)$ are polynomials in $\mathbb{Z}[U]$ satisfying the following conditions: $Q(0) = 1$, and $R(U)$ is a product of polynomials of the form $(1-\ell^m U^n)$, where $m \geq 0$ and $n \geq 1$ are integers for which the inequality $m \leq ns$ holds. They called this assertion the *Q-conjecture*.

Due to the existing analogy between arithmetic fields of characteristic zero and those of characteristic > 0 (*i.e.* arithmetic function fields), it is quite natural to propose the analogous question in this latter case. However, in this case we do not have a general resolution of singularities theorem ([1], [2]), nor the rings involved admit elimination of quantifiers ([3], [4], [6]). Because of these facts it seems that a direct approach to the conjecture in the arithmetic function field case, by means of elementary methods, *à la* Abhyankar ([1], [2]), would be of some interest. Indeed, in this paper we show for some special cases the validity of the conjecture, and compute explicitly some of the corresponding Poincaré series, in a rather elementary way using simple arithmetical properties of the field $L[[Z]]$ of formal meromorphic functions over a finite field L. Also, we show that the Q-conjecture of Hayes and Nutt is valid for these cases.

§2. Some preliminary results

We begin this section by recalling (see [14]) that a formal power series

$$d_0 + d_1U + \cdots + d_nU^n + \cdots \in \mathbb{Z}[[U]] \qquad (2.1)$$

is a rational function of U if, and only if, there is an index $m \geq 1$ such that all the numbers d_n, $n \geq m$, can be computed from $d_0, d_1, \cdots, d_m$ by means of a linear recurrence, say

$$u_{n+k} = a_1u_{n+k-1} + \cdots + a_ku_n \quad (n \geq m \geq 1) \qquad (2.2)$$

where

$$u_1 = d_0,\ u_2 = d_1\ ,\cdots,\ u_n = d_{n-1},\cdots,$$

k is the *order of the recurrrence* and $a_1,\cdots,a_k$ are called the *coefficients of the recurrence relation* (2.2). Moreover, (2.1) can be expressed as the quotient $Q(U)/R(U)$,

$$Q(U) := u_1 + (u_2 - a_1u_1)U + \cdots + \\ + (u_{k+m-1} - a_1u_{k+m-2} - \cdots - a_ku_{m-1})U^{k+m-2} \qquad (2.3)$$

and

$$R(U) := 1 - a_1U - \cdots - a_kU^k\ . \qquad (2.4)$$

Let now K be an arithmetic function field of characteristic $\ell > 1$, that is, a finite algebraic extension of $\mathbb{F}_q(X)$, $q = \ell^\nu$. Let $\mathfrak{p}$ be a prime divisor of K, and let us consider the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$. If $w_\mathfrak{p}$ represents the corresponding discrete valuation, let us denote by $\mathcal{O}_\mathfrak{p} = \{\, x \in K_\mathfrak{p}\ ;\ w_\mathfrak{p}(x) \geq 0\,\}$ and $p\mathcal{O}_\mathfrak{p} = \{\, x \in K_\mathfrak{p}\ ;\ w_\mathfrak{p}(x) > 0\,\}$, $w_\mathfrak{p}(p) = 1$, the ring of $\mathfrak{p}$-adic integers and the prime ideal of $\mathcal{O}_\mathfrak{p}$, respectively. Then $L_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}$ is a finite extension of $\mathbb{F}_\ell$, with, say, q elements. With this notation our conjecture can be stated thus:

Let $H(t_1,\cdots,t_s) \in \mathcal{O}_\mathfrak{p}[t_1,\cdots,t_s]$ and let $c(n;H)$ denote the number of zeroes of the reduction of H in the residue ring $\mathcal{O}_\mathfrak{p}/p^n\mathcal{O}_\mathfrak{p}$ $(n = 1,2,\cdots)$. Then (1.1) is a rational function of U.

Since $\mathcal{O}_\mathfrak{p} = L_\mathfrak{p}[[Z]]$, where $L_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}$, $p\mathcal{O}_\mathfrak{p} = (Z)$, it suffices to prove the conjecture when $H(t_1,\cdots,t_s)$ has coefficients in the ring $L[[Z]]$, where L is a finite field of characteristic ℓ and q elements. More precisely, it is enough to prove that if $c(n;H)$ denotes the number of zeroes of H in the residue field $L[[Z]]/(Z^n)$, then (1.1) is a rational function of U.

The Q-conjecture takes now the following form: $Q(0) = 1$ and $R(U)$ is the product of polynomials of the form $(1 - q^mU^n)$, where $m \geq 0$, $n \geq 1$, and $m \leq ns$.

If $\pi_n : L[[Z]] \to L[[Z]]/(Z^n)$, defined by

$$\pi_n(\sum_{i=0}^{\infty} \alpha_i Z^i) := \sum_{i=0}^{n-1} \alpha_i z_n^i,$$

where $\pi_n(Z) = z_n$, is the canonical epimorphism onto the residue ring, then $1, z_n, \cdots, z_n^{n-1}$ is a basis over L of the algebra $L[[Z]]/(Z^n)$. Clearly, $z_n^k \neq 0$ for $k = 0, \cdots, n-1$, and $z_n^k = 0$ for $k \geq n$. Let us denote by L_n the n-dimensional L-algebra $L[[Z]]/(Z^n)$. The canonical epimorphisms $\pi_{n,m} : L_m \to L_n$, $m \geq n$, given by

$$\pi_{n,m}(\sum_{i=o}^{m-1} \alpha_i z_m^i) = \sum_{i=0}^{n-1} \alpha_i z_n^i ,$$

are L-algebra morphisms.

We write

$$\tau_n := \left(\sum_{i=0}^{n-1} \tau_{1,i} z_n^i, \cdots, \sum_{i=0}^{n-1} \tau_{s,i} z_n^i\right) \quad (\tau_{i,j} \in L) \quad (2.5)$$

for an element of L_n^s. If $H(t_1, \cdots, t_s) \in L[[Z]][t_1, \cdots, t_s]$, its reduction $H_n(t_1, \cdots, t_s)$ is just the polynomial in $L_n[t_1, \cdots, t_s]$ whose coefficients are the coefficients of $H(t_1, \cdots, t_s)$ taken modulo (Z^n). Also, with the obvious meaning,

$$\pi_{n,m}(H_m(t_1, \cdots, t_s)) = H_n(t_1, \cdots, t_s)$$

if $n \leq m$.

If $\tau_m \in L_m^s$ is a zero of $H_m(t_1, \cdots, t_s)$ and $m \geq n$, we say that τ_m is a *descendant* of τ_m if $\pi_{n,m}(\tau_m) = \tau_n$; obviously, if such is the case, $H_n(\tau_n) = 0$, and we also say that τ_n is an *ascendant* of τ_m. Conversely, if $\tau_n \in L_n^s$ is a zero of $H_n(t_1, \cdots, t_s)$, then in L_m^s, $m \geq n$, τ_n has at most $q^{s(m-n)}$ descendants, if any.

A zero $\tau_n \in L_n^s$ of $H_n(t_1, \cdots, t_s)$ is said to be *non-singular* if

$$\frac{\partial H_1(\pi_{1,n}(\tau_n))}{\partial t_j} = \frac{\partial H_1(\tau_{1,0}, \cdots, \tau_{s,0})}{\partial t_j} \neq 0$$

for some $j = 1, \cdots, s$. Otherwise τ_n is called a *singular zero*.

Proposition 2.1. *Any descendant (resp. ascendant) of a non-singular zero is a non-singular zero.*

Proof. Obvious.

The group of units of a ring A will be denoted here by $A^\times$.

Proposition 2.2. (a)

$$L_m^\times = \{ \upsilon_0 + \upsilon_1 z_m + \cdots + \upsilon_{m-1} z_m^{m-1} \ ; \ \upsilon_0 \neq 0 \}.$$

(b) *If $\upsilon \in L_m^\times$, then $\pi_{n,m}(\upsilon) \in L_n^\times$ for all $n \leq m$. Also, $\pi_{m,m+k}^{-1}(\upsilon) \subseteq L_{m+k}^\times$ for all $k \geq 0$.*

(c) *If $\tau_n \in L_n^s$ is a non-singular zero of $H_n(t_1, \cdots, t_s)$, then for all its descendants and ascendants τ_m we have $\partial(H_m(\tau_m))/\partial t_j \in L_m^\times$ for all $j = 1, \cdots, s$ satisfying $\partial H_1(\tau_1)/\partial t_j \neq 0$.*

Proof. (a) The equation

$$(\upsilon_0 + \upsilon_1 z_m + \cdots + \upsilon_{m-1} z_m^{m-1}) \times (\beta_0 + \beta_1 z_m + \cdots + \beta_{m-1} z_m^{m-1}) = 1$$

leads to a finite system of linear equations: $\upsilon_0 \beta_0 = 1, \cdots$, from which the result follows readily.

(b) Follows easily from (a) and the fact that

$$\pi_{m,m+k}^{-1}(\upsilon) = \{\upsilon_0 + \upsilon_1 z_{m+k} + \cdots + \upsilon_{m+k-1} z_m^{m+k-1} \ ; \ \upsilon_j \in L\}$$

if $\upsilon = \upsilon_0 + \upsilon_1 z_m + \cdots + \upsilon_{m-1} z_m^{m-1}$.

(c) This follows from (a), (b), and proposition 2.1.

If τ_n is given by (2.5), let us denote by $\hat{\tau}_n$ the element in L_n^s given by

$$\hat{\tau}_n := \left(\sum_{i=0}^{n-2} \tau_{1,i} z_n^i, \cdots, \sum_{i=0}^{n-2} \tau_{s,i} z_n^i\right) .$$

This notation enables us to state the following version of Taylor's formula:

Proposition 2.3. *If $H(t_1, \cdots, t_s)$ is a polynomial with coefficients in $L[[Z]]$, then for each $n = 1, 2, \cdots$ we have*

$$H_n(\tau_n) = H_n(\hat{\tau}_n) + z_n^{n-1} \sum_{j=1}^{s} \tau_{j,n-1} \frac{\partial H_n(\hat{\tau}_n)}{\partial t_j} . \quad (2.6)$$

Proof. By induction on s.

Proposition 2.4. *If $\alpha \in L_n$ and $e < n$, then $z_n^e \alpha = 0$ if, and only if, $\pi_{n-e,n}(\alpha) = 0$.*

Proof. Let $\alpha = \sum_{i=o}^{n-1} \alpha_i z_n^i$. Then $z_n^e \alpha = \sum_{i=0}^{n-1} \alpha_i z_n^{i+e} = \sum_{i=o}^{n-e-1} \alpha_i z_n^{i+e} = 0$ if, and only if, $\alpha_0 = \alpha_1 = \cdots = \alpha_{n-e-1} = 0$. The result follows then from $\pi_{n-e,n}(\alpha) = \sum_{i=0}^{n-e-1} \alpha_i z_{n-e}^i$.

Proposition 2.5. *Let $H(t_1,\cdots,t_s)$ be a polynomial with coefficients in $L[[Z]]$, and let $n>1$. Then:*

(a) *For each singular zero τ_n of $H_n(t_1,\cdots,t_s)$ we have*

$$H_n(\tau_n)=H_n(\hat{\tau}_n)\ . \tag{2.7}$$

Further, the zero

$$\overset{\vee}{\tau}_{n-1}:=\pi_{n-1,n}(\tau_n)=\left(\sum_{i=0}^{n-2}\tau_{1,i}z_{n-1}^i,\cdots,\sum_{i=0}^{n-2}\tau_{s,i}z_{n-1}^i\right) \tag{2.8}$$

of $H_{n-1}(t_1,\cdots,t_s)$ has always exactly q^s descendants in L_n^s.

(b) *If τ_n is a non-singular zero of $H_n(t_1,\cdots,t_s)$, then $\overset{\vee}{\tau}_{n-1}$ has always exactly q^{s-1} descendants in L_n^s.*

Proof. For $j=1,\cdots,s$, let

$$\frac{\partial H_n(\hat{\tau}_n)}{\partial t_j}=\beta_{j,0}(n)+\beta_{j,1}(n)z_n+\cdots+\beta_{j,n-1}(n)z_n^{n-1}$$

($\beta_{j,k}(n)\in L$). Replacing these expressions in (2.6), we obtain

$$H_n(\tau_n)=H_n(\hat{\tau}_n)+\left[\sum_{j=1}^{s}\tau_{j,n-1}\beta_{j,0}(n)\right]z_n^{n-1}\ . \tag{2.9}$$

If τ_n is a singular zero of $H_n(t_1,\cdots,t_s)$, then $\beta_{j,0}(n)=0$ for all $j=1,\cdots,s$. Thus we have (2.7). The rest of part (a) in the proposition is an inmediate consequence of (2.7). If now

$$H_n(\hat{\tau}_n)=\gamma_0(n)+\gamma_1(n)z_n+\cdots+\gamma_{n-1}(n)z_n^{n-1}\ ,$$

it follows from (2.9) that τ_n is a non-singular zero of $H_n(t_1,\cdots,t_s)$ if, and only if,

$$\gamma_0(n)=\gamma_1(n)=\cdots=\gamma_{n-2}(n)=0\ , \tag{2.10}$$

and

$$\gamma_{n-1}(n)+\sum_{j=1}^{s}\tau_{j,n-1}\beta_{j,0}(n)=0\ . \tag{2.11}$$

Let us remark that (2.10) is equivalent to $H_{n-1}(\overset{\vee}{\tau}_n)=0$. Thus $\overset{\vee}{\tau}_n$ has as many descendants in L_n^s as solutions has the linear equation (2.11). But, by hypothesis, there is an index k ($k=1,\cdots,s$) such that $\beta_{k,0}(n)\neq 0$; therefore, for any choice of the coefficients $\tau_{j,n-1}$, $j\neq k$, the equation (2.11) is solvable for $\tau_{k,n-1}$. But there are exactly q^{s-1} choices for the $\tau_{j,n-1}$ ($j\neq k$) and hence q^{s-1} descendants of $\overset{\vee}{\tau}_n$. Finally, let us notice that the foregoing argument also shows that (2.11) is always solvable.

The following well-known result can be found in [9].

Proposition 2.6. *Given a system*

$$H^1(t_1,\cdots,t_s),\cdots,H^r(t_1,\cdots,t_s)$$

of polynomials in $L[[Z]][t_1,\cdots,t_s]$, they have a common zero in $L[[Z]]^s$ if, and only if, for each $n=1,2,\cdots$, the polynomials $H_n^1(t_1,\cdots,t_s),\cdots,H_n^r(t_1,\cdots,t_s)$ have a common zero in L_n^s.

§3. Proof of the conjecture in some particular cases

Given $H(t_1,\cdots,t_s)$ with coefficients in $L[[Z]]$, let us consider a zero $\tau_1=(\tau_{1,0},\cdots,\tau_{s,0})$ of $H_1(t_1,\cdots,t_s)$ in L_1^s. The number of descendants of τ_1 in L_n^s ($n\geq 1$) will be denoted by $d(n;H;\tau_1)$ (or simply $d(n;\tau_1)$ if there is no possible confusion). Of course, $d(1;\tau_1)=1$. With this notation,

$$c(n;H)=\sum_{\{\tau_1\ ;\ H_1(\tau_1)=0\}}d(n;\tau_1)\ ,\quad n\geq 1\ .$$

The formal series

$$\sum_{n=1}^{\infty}d(n;\tau_1)U^n \tag{3.1}$$

is called *the contribution of τ_1 to the Poincaré series of* $H(t_1,\cdots,t_s)$. Therefore,

$$P(H;U)-1=\sum_{\{\tau_1\ ;\ H_1(\tau_1)=0\}}\ \sum_{n=1}^{\infty}d(n;\tau_1)U^n$$

will be a rational function of U if each of the series (3.1) is a rational function of U. For example, if τ_1 is a non-singular zero of $H_1(t_1,\cdots,t_s)$, it follows from (b), Proposition 2.5, that $d(n;\tau_1)=d(n-1;\tau_1)q^{s-1}\neq 0$ for $n\geq 2$, and thus the contribution of τ_1 to the Poincaré series of $H(t_1,\cdots,t_s)$ is given by

$$U+q^{s-1}U^2+\cdots+q^{n(s-1)}U^{n+1}+\cdots=$$
$$=\frac{U}{1-q^{s-1}U}\ . \tag{3.2}$$

Consequently we have proved the conjecture in the following special case.

Proposition 3.1. *Let $H(t_1,\cdots,t_s)$ be a polynomial with coefficients in $L[[Z]]$. If all the zeroes of $H_1(t_1,...,t_s)$ are non-singular, then*

$$P(H;U)=1+c(1;H)\frac{U}{1-q^{s-1}U}\ , \tag{3.3}$$

where $c(1;H)$ is the number of zeroes of $H_1(t_1,\cdots,t_s)$ in L_1^s.

Corollary. *In the conditions of Proposition 3.1, the Poincaré series of $H(t_1,\cdots,t_s)$ satisfies the Q-conjecture.*

Another case that we can handle inmediately is the following: A form $H(t_1,\cdots,t_s)$ is called *strongly non-degenerate* if $(0,\cdots,0)\in L_1^s$ is the only singular zero of $H_1(t_1,\cdots,t_s)$. For this particular type of forms we prove the following result, analogous to the one to be found in Goldman [8].

Proposition 3.2. *Let $H(t_1,\cdots,t_s)$ be a strongly non-degenerate form of degree e and coefficients in $L[[Z]]$. Then the Poincaré series of H is a rational function given by*

$$P(H;U)=1+\frac{U\left\{c(1;H)(1-q^sU)+\left[1-q^{s-1}U\right]\left[1-(q^sU)^e\right]\right\}}{(1-q^{se}U^e)(1-q^{s-1}U)(1-q^sU)}$$

Proof. Let τ_n be a descendant of $\tau_1=(0,\cdots,0)\in L^s$. Then

$$\tau_n=(z_n\sum_{i=1}^{n-1}\tau_{1,i}z_n^{i-1},\cdots,z_n\sum_{i=1}^{n-1}\tau_{s,i}z_n^{i-1}),$$

so that

$$H_n(\tau_n)=z_n^eH_n\left(\sum_{i=1}^{n-1}\tau_{1,i}z_n^{i-1},\cdots,\sum_{i=1}^{n-1}\tau_{s,i}z_n^{i-1}\right). \tag{3.4}$$

If $n\le e$, (3.9) is always equal to zero. Thus $d(n;\tau_1)=q^{s(n-1)}$. If $n>e$, (3.9) equals zero if, and only if,

$$H_{n-e}\left(\sum_{i=1}^{n-e}\tau_{1,i}z_{n-e}^{i-1},\cdots,\sum_{i=1}^{n-e}\tau_{s,i}z_{n-e}^{i-1}\right)=0,$$

because of proposition 2.4. Thus $d(n;\tau_1)=c(n-e)q^{se}$ and the contribution of $\tau_1=(0,\cdots,0)$ to the Poincaré series of $H(t_1,\cdots,t_s)$ is given by

$$\begin{aligned}&U+q^sU^2+\cdots+q^{s(e-1)}U^e+\sum_{n=e+1}^{\infty}c(n-e)q^{se}U^n\\&=\frac{U\left[1-(q^sU)^e\right]}{1-q^sU}+q^{se}U^e\sum_{n=e+1}^{\infty}c(n-e)U^{n-e}\\&=\frac{U\left[1-(q^sU)^e\right]}{1-q^sU}+q^{se}U^e[P(H;U)-1]\end{aligned} \tag{3.5}$$

The contribution of the other zeroes of $H_1(t_1,\cdots,t_s)$ is given by

$$[c(1:H)-1]\frac{U}{1-q^{s-1}U}, \tag{3.6}$$

using (3.2). From (3.5) and (3.6) the result follows readily.

Corollary. *The Poincaré series of a strongly non-degenerate form satisfies the Q-conjecture*

Examples of strongly non-degenerate forms are the following: quadratic forms if $\ell\neq 2$, and forms of the type

$$\alpha_1(Z)t_1^e+\cdots+\alpha_s(Z)t_s^e,$$

where $\ell\nmid e$ and the $\alpha_i(Z)$ are units.

In order to treat cases in which at least one of the zeroes of $H_1(t_1,\cdots,t_s)$ is singular, it is convenient to reduce ourselves to the case where the content of the polynomial $H(t_1,\cdots,t_s)$ is 1. In general, $H(t_1,\cdots,t_s)$ can be written as $v(Z)Z^rH^*(t_1,\cdots,t_s)$, where $v(Z)$ is a unit in $L[[Z]]$, $r\ge 0$, and $H^*(t_1,\cdots,t_s)$ is a polynomial of content 1. Since $\pi_n(v(Z))$ is a unit in L_n for all $n\ge 1$, it is evident that $z_n^rH_n^*(t_1,\cdots,t_s)$ and $H_n(t_1,\cdots,t_s)$ have the same number of zeroes in L_n^s. Therefore, without loss of generality, we may suppose that

$$H(t_1,\cdots,t_s)=Z^rH^*(t_1,\cdots,t_s).$$

Now, if $r\ge 1$, all the elements in L_n^s, for $n\le r$, are zeroes of $H_n(t_1,\cdots,t_s)$. Also, since $\partial H_n/\partial t_j=z_n^r\partial H_n^*/\partial t_j$, all of them are singular. That is,

$$H_n(\tau_n)=z_n^rH_n^*(\tau_n)=0, \tag{3.7}$$

for all $\tau\in L_n^s$ if $n\le r$. This means that $d(n;H;\tau_1)=d(n;H^*;\tau_1)=q^{s(n-1)}$ for $n=1,2,\cdots,r$. If $n>r$, then (3.7) holds if, and only if, $H_{n-r}^*(\pi_{n-r,n}(\tau_n))=H_{n-r}^*(\tau_{n-r})=0$, because of proposition 2.4. But this implies that $d(n;H;\tau_1)=d(n-r;H^*;\tau_1)$ for all $n>r$, by virtue of (a), proposition 2.5. Therefore the contribution of any $\tau_1\in L_1^s$ to the Poincaré series of $H(t_1,\cdots,t_s)$ is given by

$$\begin{aligned}&\textstyle\sum_{n=1}^{r}q^{s(n-1)}U^n+\sum_{n=r+1}^{\infty}d(n-r;H^*;\tau_1)U^n\\&=\frac{U[1-(q^sU)^r]}{1-q^sU}+U^r\textstyle\sum_{k=1}^{\infty}d(k;H^*;\tau_1)U^k.\end{aligned}$$

Therefore

$$P(H;U)=1+c(1:H)\frac{U[1-(q^sU)^r]}{1-q^sU}+U^r[P(H^*;U)-1], \tag{3.8}$$

which proves the following

Proposition 3.3. *If $r \geq 1$ and $H(t_1, \cdots, t_s) = Z^r H^*(t_1, \cdots, t_s)$, then $P(H;U)$ is a rational function of U if, and only if, $P(H^*;U)$ is a rational function of U.*

Thus from now on all polynomials under consideration will be supossed to have content 1.

Proposition 3.4. *The Poincaré series of the polynomial $H(t) = (t - \alpha(Z))^e$, where $\alpha(Z) = \alpha_0 + \alpha_1 Z + \cdots$, is a rational function.*

Proof. Let us consider $H_1(t) = (t - \alpha_0)^e$. If $e = 1$, we have $H_1'(t) = 1 \neq 0$, so that α_0 is a non-singular zero. Using (3.2) we see that in this case $P(H;U) = 1 + U/(1-U)$. Suppose now that $e > 1$, so that α_0 is a singular zero. A descendant τ_n of $\tau_1 = \alpha_0$, for $n > 1$, is given by $\tau_n = \alpha_0 + \tau_1 z_n + \cdots + \tau_{n-1} z_n^{n-1}$ and satisfies

$$\begin{aligned} H_n(\tau_n) &= (\tau_n - \pi_n(\alpha(Z)))^e \\ &= z_n^e[(\tau_1 - \alpha_1) + \cdots + (\tau_{n-1} - \alpha_{n-1}) z_n^{n-2}]^e \\ &= 0. \end{aligned} \tag{3.9}$$

If $n \leq e$, (3.9) is satisfied for all choices of $\tau_1, \cdots, \tau_{n-1}$. That is, $d(n;\tau_1) = q^{n-1}$. If $e < n \leq 2e$, then (3.6) is satisfied if, and only if,

$$[(\tau_1 - \alpha_1) + \cdots + (\tau_{n-e-1} - \alpha_{n-e-1}) z_{n-e}^{n-e-1}]^e = 0\,, \tag{3.10}$$

by proposition 2.4. But (3.10) holds if, and only if, $\tau_1 = \alpha_1$, since otherwise $(\tau_1 - \alpha_1) + \cdots + (\tau_{n-e-1} - \alpha_{n-e-1}) z_{n-e-1}^{n-e-1}$ would be a unit, which is not possible. But then (3.10) becomes

$$\begin{aligned} &z_{n-e}^e[(\tau_2 - \alpha_2) + \cdots + (\tau_{n-e-1} - \alpha_{n-e-1}) z_{n-e}^{n-e-2}]^e \\ &= 0, \end{aligned} \tag{3.11}$$

which holds for all possible choices of $\tau_2, \cdots, \tau_{n-e-1}$, if $1 < n - e \leq e$. Thus, for $e + 1 < n \leq 2e$, $d(n;\tau_1) = q^{n-e-2} q^e = q^{n-2}$, because of (a), proposition 2.5. Now $d(e;\tau_1) = q^{e-1} = d(e+1;\tau_1)$. An inductive reasoning on k will show the following: if $ke < n \leq (k+1)e$, then

$$\begin{aligned} d(n;\tau_1) &= q^{n-(k+1)} \\ d(ke;\tau_1) &= q^{k(e-1)} = d(ke+1;\tau_1). \end{aligned}$$

From these identities we get

$$d(n+e;\tau_1) = q^{e-1} d(n;\tau_1) \quad \text{for} \quad n \geq 1\,.$$

This last identity defines a recurrent sequence of order e with $a_1 = a_2 = \cdots = a_{e-1} = 0$ and $a_e = q^{e-1}$. By virtue of (2.3) and (2.4), the contribution of τ_1 to the Poincaré series of $H(t)$ is given by

$$\frac{U[1 + qU + \cdots + q^{e-1}U^{e-1}]}{1 - q^{e-1}U^e}$$

and thus

$$P(H;U) = 1 + \frac{U[1 + qU + \cdots + q^{e-1}U^{e-1}]}{1 - q^{e-1}U^e}\,.$$

Corollary. *The polynomial $H(t) = (t - \alpha(Z))^e$ satisfies the Q-conjecture.*

Proposition 3.5. *Let*

$$H(t) = \beta(0) + \beta(1)t + \cdots + \beta(m)t^m, \quad \beta(m) \neq 0,)$$

where $\beta(j) \in L[[Z]]$, $j = 1, \cdots, m$. Then $P(H;U)$ is a rational function of U.

Proof. If $H(t)$ has no roots in $L[[Z]]$, the contribution of any zero of $H_1(t)$ to the Poincaré series of $H(t)$ is a polynomial in U (because of proposition 2.6), so in this case there is nothing to prove. Let thus $\alpha(Z) = \sum_{k=0}^{\infty} \alpha_k Z^k$ be a zero of $H(t)$ in $L[[Z]]$, with multiplicity $e \geq 1$ so that

$$H(t) = (t - \alpha(Z))^e G(t),$$

where $G(t) \in L[[Z]][t]$, $G(\alpha(Z)) \neq 0$. Because of proposition 3.3, and since we may write

$$Z^r H(t) = (t - \alpha(Z))^e G^*(t),$$

with $G^*(t) \in L((Z))[t]$, for some $r \geq 0$, we may assume that $G(t) \in L[[Z]][t]$. Of course the multiplicity of $\pi_1(\alpha(Z)) = \alpha_0$ in the polynomial $H_1(t) = (t - \alpha_0)^e G_1(t)$ may happen to be $\geq e$, i.e. $G_1(\alpha_0) = 0$. However, there is an index v such that $G(\pi_v(\alpha)) \neq 0$, since otherwise $G(\alpha(X)) = 0$ (proposition 2.6), contrary to the hypothesis. Therefore, the contribution of $\pi_1(\alpha(Z)) = \alpha_0$ to the Poincaré series of $H(t)$ from $n > v$ on will be the same as that of α_0 to the Poincaré series of $(t - \alpha(Z))^e$, which we know, by proposition 3.3, is a rational function.

Corollary. *The Poincaré series of a polynomial in one variable and coefficients in $L[[Z]]$ satisfies the Q-conjecture.*

Another case which can be handled in this elementary way, but whose proof we do not include here, is the following:

Proposition 3.6. *Let $H(t_1, \cdots, t_s) = \alpha(Z) t_1^{e_1} \cdots t_s^{e_s}$ be a monomial. Then $P(H;U)$ is a rational function of U.*

Bibliografía

1. Abhyankar, S., *High-school algebra in algebraic geometry*, Historia Mathematica **2** (1975), 567–572.
2. Abhyankar, S., *Historical ramblings in algebraic geometry and related algebra*, Amer. Math. Monthly **83** (1976), 409–449.
3. Berline, C., *Rings which admit elimination of quantifiers*, J. of Symb. Logic **46** (1981), 56–58.
4. Berline, C., *QE rings in characteristic p^n*, J. of Symb. Logic **48** (1983), 140–162.
5. Borevich, Z. I. & Shafarevich, I. R., *Number Theory*, Academic Press, New York, 1966.
6. Cherlin, G. & Dickmann, M. A., *Real closed rings II. Model theory*, Annals of Pure and Applied Logic **25** (1983), 213–231.
7. Denef, J., *The rationality of the Poincaré series associated to the p-adic points on a variety*, Inv. Mathematicae **77** (1984), 1–23.
8. Goldman, J. R., *Number of solutions of congruences: Poincaré series for strongly non-degenerate forms*, Proceedings Amer. Math. Soc. **87** (1983), 586–590.
9. Greenberg, M. J., *Lectures on Forms in Many Variables*, W. A. Benjamin, New York, 1969.
10. Hayes, D. R. & Nutt, M. D., *Reflective functions on p-adic fields*, Acta Arithmetica **XL** (1982), 229–248.
11. Igusa, J.-I., *Complex powers and asymptotic expansions I.*, J. reine ange. Math. **268/269** (1974), 110–130.
12. Igusa, J.-I., *Complex powers and asymptotic expansions II.*, J. reine ange. Math. **278/279** (1975), 307–321.
13. Igusa, J.-I., *Some observations on higher degree characters*, Amer. J. Math. **99** (1977), 393–417.
14. Markushévich, A. I., *Sucesiones recurrentes*, Mir, Moscú, 1974.