Revista Colombiana de Matemáticas
Vol. XXI (1987), págs. 85-94

ON A THEOREM OF MÖBIUS: ELEMENTARY VARIATIONS ON THE POLYNOMIAL TONALITY

by

Víctor S. ALBIS-GONZALEZ

§1. Introduction. The following theorem which is due to Möbius in the case of the ring of rational integers $\mathbb{Z}$, is known to be versatile and general in its applications [**3**, 37; **2**, 93]:

Let $\{(d_j,\alpha_j);\ d_j \in \mathbb{N},\ \alpha_j \in \mathbb{C},\ 1 \leq j \leq n\}$, $S(m) = \sum_{d_j \equiv 0 (\mathrm{mod}\ m)} \alpha_j$ *and* $S' = \sum_{d_j=1}\alpha_j$. *Then* $S' = \sum_{m=1}^{\infty}\mu(m)S(m)$, *where* μ *is the Möbius function.*

With its help a good lot of number-theoretic identities and asymptotic formulae can be proved rather easily. Our porpuse in this paper is to prove its analog for the ring $\mathbb{F}[X]$ of polynomials in the indeterminate X and coefficients in a finite field $\mathbb{F}$, with $q = p^s$ $(s \geq 1)$ elements, and use it to establish in $\mathbb{F}[X]$ analogs of some known results in the case of the ring $\mathbb{Z}$.

Let $\mathcal{P}$ denote the set of all monic irreducible polynomials in $\mathbb{F}[X]$; since $\mathbb{F}[X]$ is a unique factorization domain, the set $\mathfrak{M}$ of all its monic polynomials is the free monoid generated by $\mathcal{P} \cup \{1\}$. An *arithmetical function of* $\mathbb{F}[X]$ is any function $f:\mathfrak{M} \to \mathbb{C}$. For example,

$$\mu(M) = \begin{cases} 1 & \text{if } M = 1 \text{ ;} \\ (-1)^k & \text{if } M = P_1 \ldots P_k,\ P_i \in \mathcal{P}, \text{ mutually distinct;} \\ 0 & \text{if } P^2 \mid M \text{ for some } P \in \mathcal{P}, \end{cases}$$

is an arithmetical function of $\mathbb{F}[X]$, called the *Möbius function of* $\mathbb{F}[X]$. An in the case of the rational integers, this function has a combinatorial character; more precisely, we have the following:

$$\sum_{D|M} \mu(D) = \begin{cases} 1 & \text{if } M = 1 \\ 0 & \text{if } M \neq 1. \end{cases} \tag{1}$$

Another example of an arithmetical function is the *(absolute) norm of a polynomial*: $n(M) = q^m$, where $m = \deg M$. Clearly n satisfies $n(MN) = n(M)\cdot n(N)$ for any $M,N \in \mathfrak{M}$. An arithmetical function f satisfying $f(MN) = f(M)\cdot f(N)$ whenever $(M,N) = 1$, is called *multiplicative,* and *completely multiplicative* if $f(MN) = f(M)\ f(N)$ for arbitrary $M,N \in \mathfrak{M}$. Thus n is completely multiplicative, while μ is just multiplicative. If $M = P_1^{e_1} \ldots P_k^{e_k}$ is the canonical decomposition of $M \in \mathfrak{M}$ in elements of $\mathcal{P}$, then the following formula is valid for any multiplicative arithmetical function f:

$$\sum_{D|M} f(D) = \sum_{j=1}^{k} \Big(\sum_{i=o}^{e_j} f(P_j^i) \Big) \tag{2}$$

(where the right-side member equals 1 if $M = 1$). In particular, we have the following identities:

$$\sum_{D|M} \mu(D) f(D) = \prod_{j=1}^{k} (1 - f(P_j)), \tag{3}$$

and

$$\sum_{D|M} \mu(D)/n(D) = \prod_{j=1}^{k} (1 - n(P_j)^{-1}), \tag{4}$$

or again

$$\emptyset(M) = \sum_{D|M} \mu(D)n(M/D) = n(M)\cdot \sum_{D|M} \mu(D)/n(D), \qquad (5)$$

where $\emptyset(M)$, the number of invertible elements of the ring $\mathbb{F}[X]/(M(X))$, is the analogous of the Euler $\emptyset$-function.

Another arithmetical function of interest is

$$\tau(M) = \sum_{D|M} 1 = \sum_{j=1}^{m} \sum_{\substack{D|M \\ \deg D=j}} 1 ,$$

the number of divisors in $\mathfrak{M}$ of the polynomial $M \in \mathfrak{M}$, $\deg M = m$.

If $M = P_1^{e_1} \dots P_k^{e_k}$, $e_i \geqslant 1$, is the canonical decomposition of M, we obtain from (2) the following identity:

$$\tau(M) = (e_1 + 1)\dots(e_k + 1), \qquad (6)$$

and from this the following inequality, for $\varepsilon \leqslant 1$:

$$\frac{\tau(M)}{n(M)^{\varepsilon}} = \frac{(e_1+1)}{q^{e_1 f_1 \varepsilon}} \cdots \frac{(e_k+1)}{q^{e_k f_k \varepsilon}} < C ,$$

for some constant C, where $f_i = \deg P_i$. Indeed, for each i $(e_i + 1)/q^{e_i f_i \varepsilon} \leqslant (e_i + 1)/2^{e_i f_i \varepsilon} \leqslant (e_i + 1)/2^{e_i \varepsilon} < 1/\varepsilon \log 2$ since $\varepsilon \log 2 < 1$. On the other hand, $f_i \varepsilon \geqslant 1$ implies that $q^{e_i f_i \varepsilon} \geqslant 2^{e_i}$, which in turn implies that $(e_i + 1)/q^{e_i f_i \varepsilon} \leqslant (e_i + 1)/2^{e_i} \leqslant 1$. But the number of primes P_i such that $f_i = \deg P_i < 1/\varepsilon$ is finite, say R. Thus

$$\frac{\tau(M)}{n(M)^{\varepsilon}} \leqslant \left(\frac{1}{\varepsilon \log 2}\right)^{R} = C.$$

Thus we have shown: *for any* $\varepsilon > 0$,

$$\tau(M) = O(n(M)^{\varepsilon}) \textit{ as } n(M) \to \infty \qquad (7)$$

(Cfr. [3, 44-45]).

In this paper we will make use of the ζ-function of the field $\mathbb{F}(X)$:

$$\zeta_{\mathbb{F}(X)}(s) = \sum_{M\in\mathfrak{M}} 1/n(M)^s = \sum_{k=o}^{\infty} q^k/q^{ks} = q^{s-1}/(q^{s-1}-1) \qquad (8)$$

which converges absolutely for all $s > 1$.

In §2, we will prove the analog of Möbius theorem in $\mathbb{F}[X]$ and some of its corollaries. In §3 we apply these results to obtain explicit and asymptotic formulae for the generalized $\emptyset$-functions introduced by Carlitz [1]; in particular, we are able to compute the average order of these $\emptyset$-functions. Also we present a result totally analogous to the case of integers about the probability that k monic polinomials, taken at random, are relatively prime [3, 49].

§2. Möbius's Theorem in $\mathbb{F}[X]$.

THEOREM. *Let* $\{(D_j,\alpha_j);\ D_j \in \mathfrak{M},\ \alpha_j \in \mathbb{C},\ 1 \leqslant j \leqslant n\}$, $S(M) = \sum_{M|D_j}\alpha_j$ *and* $S' = \sum_{D_j=1}\alpha_j$. *Then* $S' = \sum_{M\in\mathfrak{M}}\mu(M)S(M)$.

Proof. We have $\sum_{M\in\mathfrak{M}}\mu(M)S(M) = \sum_{M\in\mathfrak{M}}\mu(M)\sum_{M|D_j}\alpha_j = \sum_{j=1}^{n}\alpha_j(\sum_{M|D_j}\mu(M)) = \sum_{D_j=1}\alpha_j = S'$, by virtue of (1).

COROLLARY 1. *Let* $A_1,\ldots,A_n \in \mathfrak{M}$ *and let* $F:\{A_1,\ldots,A_n\}\to\mathbb{C}$ *be an arbitrary function. Then for a given* $M \in \mathfrak{M}$ *the following holds*:

$$\sum_{(A_j,M)=1}F(A_j) = \sum_{D|M}\mu(D)S(D), \qquad (9)$$

where $S(D) = \sum_{D|A_j}F(A_j)$.

Proof. Let us take $D_j = (A_j,M)$ and $\alpha_j = F(A_j)$; then $S' = \sum_{(A_j,M)=1}F(A_j)$ and $S(D) = \sum_{D|(A_j,M)}F(A_j)$; since $S(D) = 0$ if $D\nmid M$, the corollary follows.

A generalization of the above corollary is the following:

COROLLARY 2. *Let* k *be an integer greater than* 1, *and let* $\mathbf{A} = \{(A_1^{(j)},\dots,A_k^{(j)});\ A_1^{(j)},\dots,A_k^{(j)} \in \mathfrak{M},\ 1 \leq j \leq n\}$. *If* $F:\mathbf{A} \to \mathbb{C}$ *is an arbitrary function, then*

$$\sum_{\text{g.c.d.}(A_1^{(j)},\dots,A_k^{(j)})=1} F((A_1^{(j)},\dots,A_k^{(j)})) = \sum_{D\in\mathfrak{M}} \mu(D)S(D), \tag{10}$$

where $S(D) = \sum_{D|\text{g.c.d.}(A_1^{(j)},\dots,A_k^{(j)})} F((A_1^{(j)},\dots,A_k^{(j)}))$.

Proof. The corollary follows by taking $D_j =$ g.c.d.$(A_1^{(j)},\dots,A_k^{(j)})$ and $\alpha_j = F((A_1^{(j)},\dots,A_k^{(j)}))$ in the theorem.

§3. Some aplications of Möbius Theorem.

a) ***The generalized Ø-functions.*** Let r be a non-negative integer and $M \in \mathfrak{M}$. With Carlitz [1] let us define $\emptyset_r(M)$ to be the number of polynomials in $\mathfrak{M}$ that are prime to M and of degree r. It is clear that $\emptyset_o(M) = 1$ for any $M \in \mathfrak{M}$. Let us take $\{(D_j,\alpha_j)\}$ where $D_j = (A_j,M)$ and $\alpha_j = 1$, and A_j runs over the set of all polynomials in $\mathfrak{M}$ of degree $= r$. Thus $\emptyset_r(M) = S' = \sum_{D_j=1} 1$ and $S(D) = \sum_{D|D_j} 1 = 0$ if $D \nmid M$ and $S(D) = \sum_{D|A_j} 1$ if $D|M$. That is, if $D|M$ then $S(D)$ is the number of multiples of D whose degree is r; this number equals q^{r-d}, where $d = \deg D$. The foregoing argument and Möbius theorem establish thus the following property:

PROPOSITION 1. *Let* $\emptyset_r(M)$ *denote the number of monic polynomials that are prime to* M *and of degree* r. *Then*

$$\emptyset_r(M) = q^r \sum_{\substack{D|M \\ o\leq \deg D\leq r}} \mu(D)/n(D). \tag{11}$$

If $r \geqslant \deg M$ *we have* $\phi_r(M) = q^r\phi(M)/n(M)$. *In particular,* $\phi_r(M) = \phi(M)$ *if* $r = \deg M$.

The last part of the proposition follows from (5) and the fact that $S(D) = 0$ if $\deg D > r \geqslant \deg M$.

COROLLARY. *We have for any* $\varepsilon > 0$,

$$\phi_r(M) = q^r\phi(M)/n(M) + O(n(M)^{\varepsilon}) \tag{12}$$

as $n(M) \to \infty$.

The proof of this statement is as follows: (11) can be written as

$$\phi_r(M) = q^r\phi(M)/n(M) - A(r;M),$$

where

$$A(r;M) = q^r \cdot \sum_{\substack{D|M \\ r<\deg D\leqslant m}} \mu(D)/n(D) \quad \text{and} \quad m = \deg M.$$

Consequently, using (7), we have

$$|A(r;M)| \leqslant q^r \cdot \sum_{\substack{D|M \\ r<\deg D\leqslant m}} |\mu(D)| \leqslant q^r \cdot \sum_{D|M} |\mu(D)| \leqslant q^r\tau(M) \leqslant q^r C(n(M)^{\varepsilon})$$

which proves the corollary.

As a consequence of (4) the function $\phi_r(M)$ can also be expressed as

$$\phi_r(M) = q^r \cdot \prod_{\substack{P\in\mathcal{P} \\ P|M}} \left(1 - \frac{1}{n(P)}\right) + O(n(M)^{\varepsilon})$$

or

$$\phi_r(M) = q^r \cdot \prod_{\substack{P\in\mathcal{P} \\ P|M}} \left(1 - \frac{1}{n(P)}\right) \text{ if } \deg M \leqslant r,$$

formulae which shed some light on that proposed by Carlitz in [1, 44,(9)], whose meaning is quite difficult to grasp.

If now $\pi(r;M)$ is the number of monic polynomials that are prime to $M \in \mathfrak{M}$ and are of degree $\leqslant r$, it is clear that

$$\pi(r;M) = \phi_o(M) + \phi_1(M) + \ldots + \phi_r(M),$$

and, therefore,

$$\pi(r;M) = \sum_{j=o}^{r} q^j \sum_{\substack{D|M \\ o\leqslant \deg D\leqslant j}} \mu(D)/n(D)$$

$$= \sum_{j=o}^{r} \sum_{\substack{D|M \\ \deg D=j}} \left\{\frac{q^{r+1-j}-1}{q-1}\right\} \mu(D).$$

This last expression can be rewritten as follows

$$\frac{q^{r+1}}{q-1} \cdot \sum_{\substack{D|M \\ o\leqslant \deg D\leqslant r}} \frac{\mu(D)}{n(D)} - \frac{1}{q-1} \cdot \sum_{\substack{D|M \\ o\leqslant \deg D\leqslant r}} \mu(D),$$

which, in particular, implies that

$$\pi(r;1) = \frac{q^{r+1}-1}{q-1} = q^r + q^{r-1} + \ldots + q + 1,$$

and

$$\pi(r;M) = \frac{q^{r+1}\phi(M)}{(q-1)n(M)} = \frac{q^{r+1}}{q-1} \prod_{P|M} \left(1 - \frac{1}{n(P)}\right) \text{ if } r \geqslant m = \deg M.$$

More generally,

$$\pi(r;M) = \frac{q^{r+1}\phi(M)}{(q-1)n(M)} - B(r;M),$$

where

$$B(r;M) = \frac{1}{q-1} \sum_{j=r+1} \sum_{\substack{D|M \\ \deg D=j}} (q^{r+1-j}-1)\mu(D).$$

Since $|q^{r+1-j} - 1| < 1$ if $j \geqslant r+1$, we see that

$$|B(r;M)| \leqslant \frac{1}{q-1} \sum_{j=r+1}^{m} \sum_{\substack{D|M \\ \deg D=1}} |\mu(D)| \leqslant \frac{1}{q-1} \sum_{D|M} |\mu(D)| \leqslant \frac{1}{q-1} \tau(M).$$

Thus, using again (7), we obtain the following property:

PROPOSITION 2. *If* $\pi(r;M)$ *denotes the number of monic polynomials of degree* $\leqslant r$ *that are prime to* M, *and if* $\varepsilon > 0$, *then the following formula holds*

$$\pi(r;M) = \frac{q^{r+1}\emptyset(M)}{(q-1)n(M)} + 0(n(M)^{\varepsilon}) = \frac{q^{r+1}}{(q-1)} \prod_{\substack{P\in\mathcal{P} \\ P|M}} \left(1 - \frac{1}{n(P)}\right) + 0(n(M)^{\varepsilon}) \quad (13)$$

when $n(M) \to \infty$.

Next we investigate the average order of $\emptyset_r(M)$. To begin with, let us suppose that $\deg M \leqslant t$, so that for $\varepsilon > 0$ (12) can be written as

$$\emptyset_r(M) = q^r\emptyset(M)/n(M) + 0(q^{t\varepsilon}).$$

From this it follows that

$$\sum_{\substack{M \\ o\leqslant \deg M\leqslant t}} \emptyset_r(M) = q^r \sum_{\substack{M \\ o\leqslant \deg M\leqslant t}} \frac{\emptyset(M)}{n(M)} + 0(q^{t\varepsilon}).$$

But

$$\sum_{\substack{M \\ o\leqslant \deg M\leqslant t}} \emptyset(M)/n(M) = \sum_{j=o}^{t} \sum_{\substack{M \\ \deg M=j}} \emptyset(M)/n(M) = \sum_{j=o}^{t} q^{-j} \sum_{\deg M=j} \emptyset(M)$$

Since $\sum_{\deg M=j} \emptyset(M) = q^j(q^j - q^{j-1})$ [1, 44,(10)], this equation becomes

$$\sum_{\substack{M \\ o\leqslant \deg M\leqslant t}} \emptyset(M)/n(M) = (q^{t+1}-1)/q .$$

Combining (14) and (15) we have

PROPOSITION 3. *For any* $\varepsilon > 0$ *the following formula* *holds*

$$\sum_{\substack{M \\ 0\leq \deg M\leq t}} \phi_r(M) = q^{r-1}(q^{t+1}-1) + O(q^{t\varepsilon}) \qquad (16)$$

as $t \to \infty$.

Finally, if $\varepsilon < 1$,

$$\frac{1}{q^t} \sum_{\substack{M \\ 0\leq \deg M\leq t}} \phi_r(M) = q^r\left(1 - \frac{1}{q^{t+1}}\right) + O(q^{t(\varepsilon-1)})$$

tends to q^r as $t \to \infty$, which shows that *the average order of* $\phi_r(M)$ *is* q^r. If $r > 1$, we also can say that the average order of $\phi_r(M)$ is $\zeta(r)(q^r-q)$ where ζ is the ζ-function of the field $\mathbb{F}(X)$.

b) ***A probabilistic result.*** Let $\mathbf{A}_{r,k} = \{(A_1^{(j)},\ldots,A_k^{(j)});\ A_i^{(j)} \in \mathfrak{M},\ n(A_i^{(j)}) \leq q^r\}$; $k \geq 2$; this set has $((q^{r+1}-1)/(q-1))^k$ elements. Let $\mathbf{A}^*_{r,k}$ denote the set of elements of $\mathbf{A}_{r,k}$ satisfying $\text{g.c.d.}(A_1^{(j)},\ldots,A_k^{(j)}) = 1$, and let S' be its number. It is clear then that

$$\text{Prob } \mathbf{A}^*_{r,k} = S'/((q^{r+1}-1)/(q-1))^k \qquad (17)$$

represents the probability that k polynomials of degree $\leq r$ are relatively primer. Defining the probability that k elements of $\mathfrak{M}$ taken at random are relatively prime as the limit of (17) as $r \to \infty$, we are able to prove the following:

PROPOSITION 4. *The probability that* k $(k \geq 2)$ *monic polynomials taken at random are relatively prime is given by*

$$1/\zeta(k)$$

where $\zeta(k)$ *is the* ζ-*function of the field* $\mathbb{F}(X)$.

Proof. The value S' can be computed by means of corollary 2 of the theorem, by taking $D_j = \text{g.c.d.}(A_1^{(j)},\ldots,A_k^{(j)}))$, and $F((A_1^{(j)},\ldots,A_k^{(j)})) = 1$, so that $S' = \sum_{M\in\mathfrak{M}} \mu(D)S(D)$, where

$$S(D) = \sum_{D|g.c.d.(A_1^{(j)},\dots,A_n^{(j)})} 1 = (q^{r-d})^k$$

if $d = \deg D \leqslant r$ and $S(D) = 0$ if $\deg D > r$. Thus

$$S' = \sum_{\substack{D \\ 0\leqslant \deg D\leqslant r}} \mu(D)(q^{r-d})^k = q^{rk} \sum_{j=0}^{r} \sum_{\substack{D \\ \deg D=j}} \frac{\mu(D)}{n(D)^k}$$

which in turn, using the relations $\sum_{\deg D=j}\mu(D) = 0$ if $j \geqslant 2$ and $= -q$ if $j = 1$ [1,43], becomes

$$S' = q^{rk}\left(1 - \frac{q}{q^k}\right) = q^{rk}(q^{k-1}-1)/q^{k-1}.$$

Therefore,

$$\text{Prob } A^*_{r,k} = \frac{q^{k-1}-1}{q^{k-1}} \left(\frac{q^r(q-1)}{q^{r+1}-1}\right)^k$$

which tends to $(q^{k-1}-1)/q^{k-1} = \zeta(k)^{-1}$ as $r \to \infty$, since $k > 2$.

This result is completely analogous to the one obtained in the case of rational integers (cf. [3, 49]).

The author wishes to express his gratitude to the referee for some helpful suggestions which inproved the contents and presentation of this paper.

REFERENCES

[1] Carlitz, L., *The arithmetic of polynomials in a Galois field*, Amer. J. Math. **54** (1932), 39-50.
[2] Grosswald, E., *Topics from the Theory of Numbers*, 2nd ed. MacMillan (New York).
[3] Vinográdov, I.M., *Fundamentos de la teoría de los números*, Mir (Moscú), 1971.

Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia
Ciudad Universitaria
Bogotá, D.E. Colombia.

(Recibido en septiembre de 1986)