A GENERALIZATION OF A THEOREM OF CARLITZ

Mireille Car

Abstract: Extending Carlitz’s theorem on sums of two squares, we study the number of representations of a polynomial in $\mathbb{F}_q[T]$ as a norm in the extension $\mathbb{F}_{q^k}[T]$ of $\mathbb{F}_q[T]$ of a polynomial in $\mathbb{F}_{q^k}[T]$.

Généralisant un théorème de Carlitz sur les sommes de deux carrés, nous étudions le nombre de représentations d’un polynôme de $\mathbb{F}_q[T]$ comme norme dans l’extension $\mathbb{F}_{q^k}[T]$ de $\mathbb{F}_q[T]$ d’un polynôme de $\mathbb{F}_{q^k}[T]$.

1 – Introduction

Let $\mathbb{F}_q$ be the finite field with $q$ elements. If $q$ is odd, sums of squares in $\mathbb{F}_q[T]$ are well known, cf. [2], [3], [4], [5], [6], [7], [8]. In these papers, one can find formulas which give the number $r_k(M)$ of representations of a polynomial $M \in \mathbb{F}_q[T]$ as a sum of $k$ squares. As a corollary to the general result proved by Carlitz in [1], one may deduce that

$$r_2(M) = (q + 1) \sum_{D|\deg M} (-1)^{\deg D},$$

if $-1$ is not a square in $\mathbb{F}_q$, the symbol $\ast$ being used to indicate that all polynomials $D$ in the sum are monic. This is not true if $-1$ is a square in $\mathbb{F}_q$. When $-1$ is not a square in $\mathbb{F}_q$, a sum of two squares in $\mathbb{F}_q[T]$ is a norm of a polynomial of the extension $\mathbb{F}_{q^2}[T]$ of $\mathbb{F}_q[T]$. We shall prove that the above formula is true in all cases if $r_2(M)$ is defined as the number $\Omega_2(M)$ of polynomials $B \in \mathbb{F}_q[T]$, such that $M$ is the norm of $B$ in the extension $\mathbb{F}_{q^2}[T]$ of $\mathbb{F}_q[T]$ and that the number $\Omega_h(M)$ of polynomials $B \in \mathbb{F}_{q^h}[T]$, such that $M$ is the norm of a polynomial

Received: April 24, 1992; Revised: November 13, 1992.
\[ B \text{ in the extension } \mathbb{F}_q^h[T] \text{ of } \mathbb{F}_q[T] \text{ is given by a formula of the same type:} \]

\[ \Omega_h(M) = \frac{q^h - 1}{q - 1} \sum_{D|\mu} \epsilon(D), \]

where \( \epsilon \) is a multiplicative function to be defined later on.

2 – Notation

If \( F \) is any field, we denote by \( F^* \) the set of the non zero elements of \( F \).

Let \( h \) be an integer such that \( h \geq 2 \). We denote by \( N \) the norm of the extension \( \mathbb{F}_q^h[T] \) of \( \mathbb{F}_q[T] \). Let \( \theta \in \mathbb{F}_q^h \) such that \( \mathbb{F}_q^h = \mathbb{F}_q(\theta) \). We denote by \( \theta_1 = \theta, \ldots, \theta_h \) all the roots of the minimal polynomial of \( \theta \) over \( F \). Obviously, every polynomial \( A \in \mathbb{F}_q^h[T] \) admits an unique representation as a sum

\[ A = A_0 + A_1 \theta + \ldots + A_{h-1} \theta^{h-1}, \]

and the \( h \) conjugates of \( A \) are the polynomials

\[ A_i = A_0 + A_1 \theta_i + \ldots + A_{h-1} \theta_i^{h-1}, \quad 1 \leq i \leq h. \]

Since

\[ N(A) = A_1 \times A_2 \times \ldots \times A_h, \]

there is an homogeneous polynomial \( \Phi \in \mathbb{F}_q[Y_0, \ldots, Y_{h-1}] \), only depending on \( h \), such for every \( A = A_0 + A_1 \theta + \ldots + A_{h-1} \theta^{h-1} \) belonging to \( \mathbb{F}_q^h[T] \),

\[ N(A) = \Phi(A_0, \ldots, A_{h-1}), \]

and the number \( \Omega_h(A) \) may be seen as the number of solutions \( (A_0, \ldots, A_{h-1}) \in \mathbb{F}_q^h \) of the equation

\[ A = \Phi(A_0, \ldots, A_{h-1}), \]

Let \( A \in \mathbb{F}_q[T] \). If there exists \( A \in \mathbb{F}_q^h[T] \) such that \( A = N(A) \), we shall say simply that \( A \) is a norm.

Let \( A \in \mathbb{F}_Q[T] \), resp. \( A \in \mathbb{F}_q^h[T] \) be different from \( 0 \). We denote by \( \text{sgn}(A) \), resp. \( \text{sgn}(A) \), the coefficient of the highest degree term in \( A \), resp. in \( A \).

If \( E \) is a finite set, we denote by \( \#(E) \) the number of elements of \( E \).
3 – The set of norms

**Proposition 3.1.** If $A \in \mathbb{F}_{q^h}[T]$ is monic, then $N(A)$ is monic and $\text{deg}(N(A)) = h \text{deg} A$.

**Proof:** Since $N(1) = 1$, it suffices to prove the proposition for a monic polynomial $A \in \mathbb{F}_{q^h}[T]$ whose degree is positive. Let

$$A = T^n + \sum_{i=1}^{n} \alpha_i T^{n-i}, \quad \alpha_i \in \mathbb{F}_{q^h}, \quad n \geq 1,$$

be such a polynomial. For every $i = 1, \ldots, n$, let $a_{i,0}, \ldots, a_{i,h-1} \in \mathbb{F}_q$, such that

$$\alpha_i = \sum_{k=0}^{h-1} a_{i,k} \theta^k.$$

If we write $A$ as a sum

(3.1) $$A = A_0 + A_1 \theta + \ldots + A_{h-1} \theta^{h-1},$$

then

$$A_0 = T^n + \sum_{i=1}^{n} a_{i,0} T^{n-i},$$

and, for $k = 1, \ldots, h-1$,

$$A_k = \sum_{i=1}^{n} a_{i,k} T^{n-i}.$$

From (3.1), we get that

$$N(A) = A_0^h + \psi(A_0, \ldots, A_{h-1})$$

where $\psi$ is a polynomial in $\mathbb{F}_q[Y_0, \ldots, Y_{h-1}]$ which does not contain the monomial $Y_0^h$. Whence,

$$\deg\left(\psi(A_0, \ldots, A_{h-1})\right) < h n = \deg(A_0^h),$$

$$\deg(N(A)) = h n$$

and the leading term in $N(A)$ is the leading term in $A_0^h$, that is to say $T^{hn}$. \(\blacksquare\)

**Proposition 3.2.** Let $A \in \mathbb{F}_q[T]$ be different from $0$. Then, $A$ is a norm if and only if $\text{sgn}(A)^{-1} A$ is a norm. In that case, $h$ divides $\text{deg} A$.

**Proof:** According to Hilbert’s theorem, every non-zero element in $\mathbb{F}_q$ is the norm of an element of $\mathbb{F}_{q^h}$, (cf. [1], §11). There exists $\alpha \in \mathbb{F}_{q^h}$ such that
\text{sgn}(A) = N(\alpha)$. If $\text{sgn}(A)^{-1}A$ is a norm, then $A$ is a norm, and conversely. Let $A \in \mathbb{F}_{q^h}[T]$, $A = N(A)$, $H \in \mathbb{F}_{q^h}[T]$ and $\mathcal{H} \in \mathbb{F}_{q^h}[T]$ monic such that $A = \text{sgn}(A)H$ and $A = \text{sgn}(A)\mathcal{H}$. Then, $\text{sgn}(A)H = N(A) = N(\text{sgn}(A))N(\mathcal{H})$.

Since $N(\mathcal{H})$ is monic, $H = N(\mathcal{H})$ and $\deg A = \deg H = h \deg \mathcal{H}$. 

\textbf{Proposition 3.3.} Let $P \in \mathbb{F}_q[T]$ be monic and irreducible. Then, $P$ is the norm of a monic polynomial $\mathcal{P} \in \mathbb{F}_{q^h}[T]$ if and only if $h$ divides $\deg P$. In that case, $\mathcal{P}$ is irreducible and its degree is $\frac{\deg P}{h}$.

\textbf{Proof:} We suppose $P = N(\mathcal{P})$, where $\mathcal{P} \in \mathbb{F}_{q^h}[T]$ is monic. Proposition 3.1 says that $\deg P = h \deg \mathcal{P}$. It remains to prove that $\mathcal{P}$ is irreducible. We suppose that there exists an integer $r \geq 1$, monic irreducible polynomials $\mathcal{P}_1, \ldots, \mathcal{P}_r$ in $\mathbb{F}_{q^h}[T]$, positive integers $e_1, \ldots, e_r$, such that

$$P = \mathcal{P}_1^{e_1} \times \cdots \times \mathcal{P}_r^{e_r}.$$ 

Then,

$$P = N(\mathcal{P}) = N(\mathcal{P}_1^{e_1} \times \cdots \times \mathcal{P}_r^{e_r}) = N(\mathcal{P}_1)^{e_1} \times \cdots \times N(\mathcal{P}_r)^{e_r}.$$

Then, $r = 1$, $e_1 = 1$ and $\mathcal{P} = \mathcal{P}_1$ is irreducible.

We suppose that $h$ divides $\deg P$. Let

$$m = \frac{\deg P}{h}.$$

Let $\mathcal{L} \in \mathbb{F}_{q^h}[T]$ be monic, irreducible, and such that $\deg(\mathcal{L}) = m$. It is well known that such $\mathcal{L}$ exists. A proof of this may be provided by theorem 3.25 of [9]. Then,

$$\mathbb{F}_{q^h}[T]/(\mathcal{L}) = \mathbb{F}_{q^{h \deg(\mathcal{L})}} = \mathbb{F}_{q^{\deg P}} = \mathbb{F}_q[T]/(P),$$

where $(\mathcal{L})$ denotes the ideal generated by $\mathcal{L}$ in $\mathbb{F}_{q^h}[T]$, and $(P)$ the ideal generated by $P$ in $\mathbb{F}_q[T]$. In the ring $\mathbb{F}_{q^h}[T]$, $\mathcal{L}$ divides $P$. We put

$$P = \mathcal{L} \mathcal{H},$$

with $\mathcal{L} \in \mathbb{F}_{q^h}[T]$.

Let $d$ be the least integer such that $\mathcal{L} \in \mathbb{F}_{q^d}[T]$. Then $d$ divides $h$ and $\mathcal{H} \in \mathbb{F}_{q^d}[T]$. Let $\mathcal{L}_1, \ldots, \mathcal{L}_d$ be the $d$ different conjugates of $\mathcal{L}$ in the extension $\mathbb{F}_{q^d}[T]$ of $\mathbb{F}_q[T]$, and $\mathcal{H}_1, \ldots, \mathcal{H}_d$ be the $d$ conjugates of $\mathcal{H}$ in the same extension. Then, for each index $i$,

$$P = \mathcal{L}_i \mathcal{H}_i.$$
Since \( L_1, \ldots, L_d \) are distinct irreducible polynomials, the product \( L_1 \times \ldots \times L_d \) divides \( P \). Since \( P \) is irreducible

\[
P = L_1 \times \ldots \times L_d ,
\]
\[
\deg P = d \deg L_1 = d \deg L .
\]

With (i) we get that \( h = d \) and (ii) shows that \( P \) is the norm of \( L_1 = L \).

**Proposition 3.4.** Let \( P \in \mathbb{F}_q[T] \) be monic and irreducible, let

\[
d = \text{G.C.D.}(h, \deg P) ,
\]

and let \( a \) be a non negative integer. Then

1. There exist \( d \) monic irreducible polynomials \( P_1, \ldots, P_d \) in \( \mathbb{F}_q[T] \) which remain irreducible in \( \mathbb{F}_{q^h}[T] \) such that
   \[
P = P_1 \times \ldots \times P_d ;
   \]

2. \( P^a \) is a norm if and only if \( \frac{h}{d} \) divides \( a \);

3. If \( P^a \) is norm of a polynomial \( \mathcal{H} \in \mathbb{F}_{q^h}[T] \), then,
   - If \( d = 1 \), \( \mathcal{H} \in \mathbb{F}_q[T] \),
   - If \( d > 1 \), there exist non negative integers \( a_1, \ldots, a_d \) such that
     \[
     \mathcal{H} = P_{a_1}^1 \times \ldots \times P_d^{a_d} \quad \text{and} \quad \frac{ad}{h} = a_1 + \ldots + a_d .
     \]

**Proof:** Let

\[
k = \frac{h}{d}, \quad m = \frac{\deg P}{d} .
\]

Then, \( k \) and \( m \) are coprime. According to proposition 3.3, there exist \( d \) monic irreducible polynomials \( P_1, \ldots, P_d \) in \( \mathbb{F}_{q^d}[T] \) such that

\[
P = P_1 \times \ldots \times P_d .
\]

Let \( N_1 \) be the norm of the extension \( \mathbb{F}_{q^d}[T] \) of \( \mathbb{F}_q[T] \). Let \( P = P_1 \). Then,

\[
P = N_1(P) .
\]

If \( P \) is not irreducible in \( \mathbb{F}_{q^h}[T] \), then \( P \) admits in \( \mathbb{F}_{q^h}[T] \) an irreducible factor \( L \). Since \( P \) is irreducible in \( \mathbb{F}_{q^d}[T] \), we prove as in proposition 3.3, that \( P \) is the product of the \( k \) conjugates of \( L \) in the extension \( \mathbb{F}_{q^h}[T] \) of \( \mathbb{F}_{q^d}[T] \). Then, \( k \) divides \( \deg(P) \), so, \( h \) divides \( \deg P \) and \( h = d \). If \( h \neq d \), all the \( P_i \) remain
irreducible in $\mathbb{F}_{q^h}[T]$, if $h = d$, all the $P_i$ are irreducible polynomials in $\mathbb{F}_{q^h}[T]$, whence (1) is proved.

If $P^a$ is a norm, $h = kd$ divides $\deg(P^a) = a \deg P = a m d$, so $k$ divides $a$ and the “if” part of (2) is proved. Let $N_1$ be the norm of the extension $\mathbb{F}_{q^d}[T]$ of $\mathbb{F}_q[T]$. Let $N_2$ be the norm of the extension $\mathbb{F}_{q^h}[T]$ of $\mathbb{F}_{q^d}[T]$. Since $P$ remains irreducible in $\mathbb{F}_{q^h}[T]$, 

$$N_2(P) = P^k,$$

whence, 

$$P^k = N_1(P)^k = N_1(P^k) = N_1(N_2(P)) = N(P).$$

Since $P^k$ is a norm, every power of $P^k$ is a norm, and the “only if” part of (2) is proved.

Theorem 3.5. Let $P_1, \ldots, P_r$, be monic irreducible pairwise distinct polynomials in $\mathbb{F}_q[T]$, let $a_1, \ldots, a_r$ be positive integers, and let

$$A = P_1^{a_1} \times \ldots \times P_r^{a_r}.$$ 

Then, $A$ is a norm in the extension $\mathbb{F}_{q^h}[T]$ of $\mathbb{F}_{q^d}[T]$ if and only if for every $i \in \{1, \ldots, r\}$, $h$ divides $a_i \deg P_i$.

Proof: The above results prove that the condition is sufficient. Let $A \in \mathbb{F}_{q^h}[T]$ be monic, such that

$$A = N(A).$$
We write
\[ A = \prod_{d|h} A_d, \]
where \( A_d \) is the product of all monic irreducible divisors \( L \) of \( A \) such that \( L \in \mathbb{F}_{q^d}[T] \) and \( L \notin \mathbb{F}_{q^d}[T] \) for any \( \delta \) smaller than \( d \), these divisors being counted with multiplicity. Let \( \mathcal{L} \) be an irreducible factor of \( A_d \). Let \( v_{\mathcal{L}} \) be the \( \mathcal{L} \)-adic valuation of \( A \). Let \( N_1 \) be the norm of the extension \( \mathbb{F}_{q^h}[T] \) of \( \mathbb{F}_{q^d}[T] \), and \( N_2 \) be the norm of the extension \( \mathbb{F}_{q^h}[T] \) of \( \mathbb{F}_{q^d}[T] \). Then, \( N_1(\mathcal{L}) \) is an irreducible polynomial in \( \mathbb{F}_q[T] \), and
\[ N_1(L) = N_1(N_2(L)) = N_1(L^{h/d}) = N_1(L)^{h/d}. \]
So \( N_1(L) \) is an irreducible divisor of \( A \) and it occurs in \( A \) with the exponent \( h \cdot v_{\mathcal{L}} \).

Each term \( P_{a_i} \) is equal to one of the terms \( N_1(L)^{v_{\mathcal{L}} h/d} \) occurring in \( A \), and
\[ a_i \deg P_i = v_{\mathcal{L}} h/d \deg(N_1(\mathcal{L})). \]
Since \( d \) divides \( \deg(N_1(\mathcal{L})) \), \( h \) divides \( a_i \deg P_i \).

4 - The functions \( \Pi_h \) and \( U \)

**Definition.** For every monic polynomial \( A \in \mathbb{F}_q[T] \), we denote by \( U(h, A) \) the number of monic polynomials \( A \in \mathbb{F}_q[T] \) such that \( A = N(A) \).

We notice that \( U(h, A) \) is the number of principal ideals \( (A) \) of \( \mathbb{F}_q[T] \) whose norm is the principal ideal \( (A) \).

**Proposition 4.1.** Let \( A \in \mathbb{F}_q[T] \), different from 0. Then
\[ \Pi_h(A) = \frac{q^h - 1}{q - 1} U \left( h, \frac{A}{\text{sgn}(A)} \right). \]

**Proof:** Let \( Y(A) \), resp. \( V(A) \), be the set of polynomials \( A \in \mathbb{F}_q[T] \) such that \( A = N(A) \), resp. the set of monic polynomials \( A \in \mathbb{F}_q[T] \) such that \( \frac{A}{\text{sgn}(A)} = N(A) \). Then
\[ \Pi_h(A) = \#Y(A), \quad U \left( h, \frac{A}{\text{sgn}(A)} \right) = \#V(A). \]
Let \( A \in Y(A) \). Then
\[ \text{sgn}(A) \frac{A}{\text{sgn}(A)} = A = N \left( \text{sgn}(A) \frac{A}{\text{sgn}(A)} \right) = N(\text{sgn}(A)) N \left( \frac{A}{\text{sgn}(A)} \right). \]
Since $\frac{A}{\text{sgn}(A)}$ and $N\left(\frac{A}{\text{sgn}(A)}\right)$ are monic polynomials in $\mathbb{F}_q[T]$, 
\[
\text{sgn}(A) = N\left(\frac{A}{\text{sgn}(A)}\right), \quad \frac{A}{\text{sgn}(A)} = N\left(\frac{A}{\text{sgn}(A)}\right),
\]
and $\text{sgn}(A) \in Y(\text{sgn}(A))$, $\frac{A}{\text{sgn}(A)} \in V(\frac{A}{\text{sgn}(A)})$. Conversely, if $H \in V\left(\frac{A}{\text{sgn}(A)}\right)$, and if $\alpha \in \mathbb{F}_{q^h}$ is such that $N(\alpha) = \text{sgn}(A)$, then $\alpha H \in Y(A)$. Whence, 
\[
(ii) \quad \#Y(A) = \#Y(\text{sgn}(A)) \#V\left(\frac{A}{\text{sgn}(A)}\right).
\]
According to Hilbert’s theorem, every $b \in \mathbb{F}_q^*$ is norm of an element of $\mathbb{F}_{q^h}^*$ (cf. [1], §11). So, when $b$ runs through $\mathbb{F}_q^*$, all the sets $Y(b)$ have the same cardinality equal to $\frac{q^h - 1}{q - 1}$. We may conclude with $(i)$ and $(ii)$. 

**Proposition 4.2.** The function $A \mapsto U(h, A)$ is a multiplicative.

**Proof:** Let $A$ and $B$ be monic and coprime polynomials.

- If $U(h, A) = 0$, $A$ is not a norm, and, according to theorem 3.5, there exists an irreducible polynomial $P$ dividing $A$ with an exponent $a$ such that $h$ does not divide $a \deg P$. Since $A$ and $B$ are coprime, $P$ does not divide $B$, and $P$ divides $AB$ with the same exponent $a$, $AB$ is not a norm, and $U(h, AB) = 0$.
- We suppose $U(h, A) = r > 0$ and $U(h, B) = s > 0$. Let $A_1, \ldots, A_r$, $B_1, \ldots, B_s$, be the different polynomials in $\mathbb{F}_q[T]$ such that 
\[
A = N(A_1) = \ldots = N(A_r),
\]
\[
B = N(B_1) = \ldots = N(B_s),
\]
then, 
\[
AB = N(A_i B_j), \quad 1 \leq i \leq r, \quad 1 \leq j \leq s.
\]
Since $A$ and $B$ are coprime, for every $i = 1, \ldots, r$, every $j = 1, \ldots, s$, $A_i$ and $B_j$ are coprime. Let $i \in \{1, \ldots, r\}$, $k \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s\}$, $\ell \in \{1, \ldots, s\}$ with $k \neq i$. We may suppose that there exists an irreducible polynomial $P$ dividing $A_i$ such that $v_P(A_i) \neq v_P(A_k)$, $v_P$ being the $P$-adic valuation. Then, $P$ does not divide $B_j$ or $B_\ell$, $v_P(A_i B_j) = v_P(A_i)$, $v_P(A_k B_\ell) = v_P(A_k)$ and $A_i B_j \neq A_k B_\ell$.

Conversely, if $H \in \mathbb{F}_q[T]$ is such that $N(H) = AB$, every irreducible divisor of $H$ divides $AB$. Since $A$ and $B$ are coprime, we may write $H$ as a product 
\[
H = H_A H_B,
\]
where the irreducible factors of $H_A$, resp. $H_B$ are those of $A$, resp. $B$, 
\[
A = N(H_A), \quad B = N(H_B),
\]
and \( \mathcal{H}_A \), resp. \( \mathcal{H}_B \) is one of the \( A_i \)'s, resp. one of the \( B_i \)'s. Whence,

\[ U(h, AB) = rs . \]

**Proposition 4.3.** Let \( P \) be monic and irreducible. Let \( m \) be a positive integer. Then,

1. If \( \frac{h}{\gcd(h, \deg P)} \) does not divide \( m \), \( U(h, P^m) = 0 \),
2. If \( \frac{h}{\gcd(h, \deg P)} \) divides \( m \), \( U(h, P^m) = p_d \left( \frac{\gcd(h, \deg P)}{h} \right) \),

where \( p_d(b) \) denotes the number of partitions of the integer \( b \) in \( d \) parts, that is to say the number of solutions \( (b_1, \ldots, b_d) \) in non negative integers of the equation

\[ b = b_1 + \ldots + b_d . \]

**Proof:** This is a corollary to proposition 3.4. \( \blacksquare \)

We define the multiplicative function \( \epsilon \) which will be used to generalize Carlitz’s theorem.

**Definition.** Let \( \epsilon \) be the multiplicative function defined on the set of monic polynomials by the following conditions. Let \( P \) be a monic and irreducible polynomial. Let \( b, s, r \) be positive integers. Then,

1. If \( \gcd(h, \deg P) = 1 \),
   \[
   \epsilon(P^h) = 1 ,
   \]
   \[
   \epsilon(P^{hb+1}) = -1 ,
   \]
   \[
   \epsilon(P^{hb+r}) = 0 \quad \text{if} \quad 1 < r < b ,
   \]
2. If \( \gcd(h, \deg P) = h \),
   \[
   \epsilon(P^h) = \left( \begin{array}{c}
   b + h - 2 \\
   h - 2
   \end{array} \right) ,
   \]
3. If \( \gcd(h, \deg P) = d > 1 \), if \( \frac{h}{d} = k > 1 \),
   \[
   \epsilon(P^{kb}) = \left( \begin{array}{c}
   b + d - 1 \\
   d - 1
   \end{array} \right) ,
   \]
   \[
   \epsilon(P^{kb+1}) = - \left( \begin{array}{c}
   b + d - 1 \\
   d - 1
   \end{array} \right) ,
   \]
   \[
   \epsilon(P^{kb+r}) = 0 \quad \text{if} \quad 1 < r < k .
   \]
**Theorem 4.4.** For any non zero polynomial $A$, one has

$$\zeta_h(A) = \frac{q^n h^q - 1}{q^n - 1} \sum_{\alpha | A} \epsilon(D).$$

**Proof:** Let

\[(i)\] \[S(A) = \sum_{\alpha | A} \epsilon(D).\]

According to proposition 4.1, we have to prove that

\[(ii)\] \[S(A) = U(h, A),\]

for every monic polynomial $A$. Since the functions $A \mapsto S(A)$ and $A \mapsto U(h, A)$ are multiplicative, it is sufficient to prove (2) when $A$ is the power $P^m$ of a monic irreducible polynomial $P$, i.e., to prove that

\[(iii)\] \[\epsilon(P^m) = U(h, P^m) - U(h, P^{m-1}).\]

We notice that $\mathcal{P}_1(b) = 1$ for every integer $b$. From the identity

\[(1 - x)^{-d} = \sum_{j=0}^{\infty} \mathcal{P}_d(j) x^j,\]

we deduce that $\mathcal{P}_d(j) = \left( \begin{array}{c} j + d - 1 \\ d - 1 \end{array} \right)$. The above proposition gives the following results:

- If $h$ and $\deg P$ are coprime,

  \[U(h, P^m) - U(h, P^{m-1}) = \begin{cases} 1 & \text{if } h \text{ divides } m, \\ -1 & \text{if } h \text{ divides } m - 1, \\ 0 & \text{otherwise}; \end{cases}\]

- If $h$ divides $\deg P$,

  \[U(h, P^m) - U(h, P^{m-1}) = \mathcal{P}_h(m) - \mathcal{P}_h(m - 1) = \left( \begin{array}{c} m + h - 1 \\ h - 1 \end{array} \right) - \left( \begin{array}{c} m + h - 2 \\ h - 1 \end{array} \right),\]

  \[U(h, P^m) - U(h, P^{m-1}) = \left( \begin{array}{c} m + h - 2 \\ h - 2 \end{array} \right);\]
A GENERALIZATION OF A THEOREM OF CARLITZ 581

If \( G \colon C \colon D \) : \( (h; \deg P) = d > 1 \), if \( k = h \), \( d > 1 \),

\[
U(h, P^m) - U(h, P^{m-1}) = \begin{cases} 
  P_d \left( \frac{m}{k} \right) = \left( \frac{m+d-1}{d-1} \right) & \text{if } k \text{ divides } m, \\
  -P_d \left( \frac{m-1}{k} \right) = - \left( \frac{m+d-1}{d-1} \right) & \text{if } k \text{ divides } m-1, \\
  0 & \text{otherwise}. 
\end{cases}
\]

In both cases (iii) is true.

We notice that, if \( h = 2 \), \( \epsilon(H) = (-1)^{\deg H} \) for every monic polynomial \( H \), so theorem 4.4 contains Carlitz’s formula. \( \blacksquare \)

REFERENCES


Mireille Car,
Laboratoire de Mathématiques, Faculté de Saint-Jérôme
Avenue Escadrille Normandie-Niemen, 13397 Marseille Cedex 13 – FRANCE