PORTUGALIAE MATHEMATICA
Vol. 51 Fasc. 4 – 1994

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 $\mathbb{F}_{q^h}[T]$ of $\mathbb{F}_q[T]$ of a polynomial in $\mathbb{F}_{q^h}[T]$.

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 $\mathbb{F}_{q^h}[T]$ de $\mathbb{F}_q[T]$ d'un polynôme de $\mathbb{F}_{q^h}[T]$.

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

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

if -1 is not a square in $\mathbb{F}_Q$, the symbol $*$ 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 $\mathfrak{n}_2(M)$ of polynomials $\mathcal{B} \in \mathbb{F}_{q^2}[T]$, such that M is the norm of $\mathcal{B}$ in the extension $\mathbb{F}_{q^2}[T]$ of $\mathbb{F}_q[T]$ and that the number $\mathfrak{n}_h(M)$ of polynomials $\mathcal{B} \in \mathbb{F}_{q^h}[T]$, such that M is the norm of a polynomial

Received: April 24, 1992; *Revised*: November 13, 1992.

$\mathcal{B}$ in the extension $\mathbb{F}_{q^h}[T]$ of $\mathbb{F}_q[T]$ is given by a formula of the same type:

$$\mathrm{n}_h(M) = \frac{q^h - 1}{q - 1} \sum_{D|M}^{*} \epsilon(D) ,$$

where ϵ is a multiplicative function to be defined later on.

2 – Notation

If $\mathbf{F}$ is any field, we denote by $\mathbf{F}^*$ the set of the non zero elements of $\mathbf{F}$.

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 θ over $\mathbb{F}$. Obviously, every polynomial $\mathcal{A} \in \mathbb{F}_{q^h}[T]$ admits an unique representation as a sum

$$\mathcal{A} = A_0 + A_1\theta + \ldots + A_{h-1}\theta^{h-1} , \tag{2.1}$$

and the h conjugates of $\mathcal{A}$ are the polynomials

$$\mathcal{A}_i = A_0 + A_1\theta_i + \ldots + A_{h-1}\theta_i^{h-1} , \quad 1 \leq i \leq h .$$

Since

$$N\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2 \times \ldots \times \mathcal{A}_h ,$$

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

$$N(\mathcal{A}) = \Phi(A_0, \ldots, A_{h-1}) , \tag{2.2}$$

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

$$A = \Phi(A_0, \ldots, A_{h-1}) , \tag{2.3}$$

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

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

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

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

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

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 $\mathcal{A}$ as a sum

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

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

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

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

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

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

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

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

$\mathrm{sgn}(A) = N(\alpha)$. If $\mathrm{sgn}(A)^{-1}A$ is a norm, then A is a norm, and conversely. Let $\mathcal{A} \in \mathbb{F}_{q^h}[T]$, $A = N(\mathcal{A})$, $H \in \mathbb{F}_q[T]$ and $\mathcal{H} \in \mathbb{F}_{q^h}[T]$ monic such that $A = \mathrm{sgn}(A)H$ and $\mathcal{A} = \mathrm{sgn}(\mathcal{A})\mathcal{H}$. Then, $\mathrm{sgn}(A)H = N(\mathcal{A}) = N(\mathrm{sgn}(\mathcal{A}))N(\mathcal{H})$. Since $N(\mathcal{H})$ is monic, $H = N(\mathcal{H})$ and $\deg A = \deg H = h \deg \mathcal{H}$. ∎

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 $\frac{\deg P}{h}$.*

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

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

Then,

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

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

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

$$(i) \qquad m = \frac{\deg P}{h} \ .$$

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 $\mathbb{F}_{q^h}[T]$, $\mathcal{L}$ divises 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 $\mathcal{F}_{q^d}[T]$ 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 $\mathcal{L}_1, \ldots, \mathcal{L}_d$ are distinct irreducible polynomials, the product $\mathcal{L}_1 \times \ldots \times \mathcal{L}_d$ divides P. Since P is irreducible

$$(ii) \qquad \begin{gathered} P = \mathcal{L}_1 \times \ldots \times \mathcal{L}_d \ , \\ \deg P = d \deg \mathcal{L}_1 = d \deg \mathcal{L} \ . \end{gathered}$$

With (i) we get that $h = d$ and (ii) shows that P is the norm of $\mathcal{L}_1 = \mathcal{L}$. ∎

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 $\mathcal{P}_1, \ldots, \mathcal{P}_d$ in $\mathbb{F}_{q^d}[T]$ which remain irreducible in $\mathbb{F}_{q^h}[T]$ such that*

$$P = \mathcal{P}_1 \times \ldots \times \mathcal{P}_d \ ;$$

(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*

$$\mathcal{H} = \mathcal{P}_1^{a_1} \times \ldots \times \mathcal{P}_d^{a_d} \quad \text{and} \quad \frac{ad}{h} = a_1 + \ldots + a_d \ .$$

Proof: Let

$$k = \frac{h}{d} \ , \qquad m = \frac{\deg P}{d} \ .$$

Then, k and m are coprime. According to proposition 3.3, there exist d monic irreducible polynomials $\mathcal{P}_1, \ldots, \mathcal{P}_d$ in $\mathbb{F}_{q^d}[T]$ such that

$$(i) \qquad P = \mathcal{P}_1 \times \ldots \times \mathcal{P}_d \ .$$

Let N_1 be the norm of the extension $\mathbb{F}_{q^d}[T]$ of $\mathbb{F}_q[T]$. Let $\mathcal{P} = \mathcal{P}_1$. Then,

$$P = N_1(\mathcal{P}) \ .$$

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

$$N_2(\mathcal{P}) = \mathcal{P}^k \ ,$$

whence,

$$P^k = N_1(\mathcal{P})^k = N_1(\mathcal{P}^k) = N_1(N_2(\mathcal{P})) = N(\mathcal{P}) \ .$$

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

Suppose that $P^a = N(\mathcal{H})$, with $\mathcal{H} \in \mathbb{F}_{q^h}[T]$, then $a = hb$. Let $\mathcal{L}$ be an irreducible factor of $\mathcal{H}$ in $\mathbb{F}_{q^h}[T]$ which does not belong to $\mathbb{F}_q[T]$, let δ be the least integer such that $\mathcal{L} \in \mathbb{F}_{q^\delta}[T]$ and let $\mathcal{L}_1, \ldots, \mathcal{L}_\delta$ be the conjugates of $\mathcal{L}$ in the extension $\mathcal{F}_{q^\delta}[T]$ of $\mathcal{F}_q[T]$. They are irreducible in $\mathbb{F}_{q^h}[T]$ and $\mathcal{L}_1 \times \ldots \times \mathcal{L}_\delta$ is an irreducible polynomial in $\mathbb{F}_q[T]$ dividing P^a, so,

$$(ii) \qquad P = \mathcal{L}_1 \times \ldots \times \mathcal{L}_\delta \ .$$

Since the factorizations (i) and (ii) of P must be the same, $d = \delta$, and the set $\{\mathcal{L}_1, \ldots \mathcal{L}_d\}$ is equal to the set $\{\mathcal{P}_1, \ldots, \mathcal{P}_d\}$. There exist non negative integers $a_1, \ldots, a_d$ such that $\mathcal{H} = \mathcal{P}_1^{a_1} \times \ldots \times \mathcal{P}_d^{a_d}$. We have

$$P^a = N(\mathcal{H}) = (P^k)^{a_1} \times \ldots \times (P^k)^{a_d} \ ,$$

and

$$\frac{a}{k} = a_1 + \ldots + a_d \ .$$

If $d = 1$, P remains irreducible in $\mathbb{F}_{q^h}[T]$ and is the only irreducible divisor of $\mathcal{H}$, then, $\mathcal{H} = P^b$. ∎

Theorem 3.5. *Let $P_1, \ldots, P_r$, be monic irreducible paiwise 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 $\mathcal{A} \in \mathbb{F}_{q^h}[T]$ be monic, such that

$$A = N(\mathcal{A}) \ .$$

We write

$$\mathcal{A} = \prod_{d|h} \mathcal{A}_d \ ,$$

where $\mathcal{A}_d$ is the product of all monic irreducible divisors $\mathcal{L}$ of $\mathcal{A}$ such that $\mathcal{L} \in \mathbb{F}_{q^d}[T]$ and $\mathcal{L} \notin \mathbb{F}_{q^\delta}[T]$ for any δ smaller than d, these divisors being counted with multiplicity. Let $\mathcal{L}$ be an irreducible factor of $\mathcal{A}_d$. Let $v_{\mathcal{L}}$ be the $\mathcal{L}$-adic valuation of $\mathcal{A}$. Let N_1 be the norm of the extension $\mathbb{F}_{q^d}[T]$ of $\mathbb{F}_q[T]$, 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

$$N(\mathcal{L}) = N_1(N_2(\mathcal{L})) = N_1(\mathcal{L}^{h/d}) = N_1(\mathcal{L})^{h/d} \ .$$

So $N_1(\mathcal{L})$ is an irreducible divisor of A and it occurs in A with the exponent $\frac{h}{d} v_{\mathcal{L}}$. Each term $P_i^{a_i}$ is equal to one of the terms $N_1(\mathcal{L})^{v_{\mathcal{L}} h/d}$ occuring 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 n_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 $\mathcal{A} \in \mathbb{F}_{q^h}[T]$ such that $A = N(\mathcal{A})$.

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

Proposition 4.1. *Let $A \in \mathbb{F}_q[T]$, different from 0. Then*

$$\mathrm{n}_h(A) = \frac{q^h - 1}{q - 1} \, U\left(U, \frac{A}{\mathrm{sign}(A)}\right) \ .$$

Proof: Let $Y(A)$, resp. $V(A)$, be the set of polynomials $\mathcal{A} \in \mathbb{F}_{q^h}[T]$ such that $A = N(\mathcal{A})$, resp. the set of monic polynomials $\mathcal{A} \in \mathbb{F}_{q^h}[T]$ such that $\frac{A}{\mathrm{sgn}(A)} = N(\mathcal{A})$. Then

$$(i) \qquad \mathrm{n}_h(A) = \#Y(A) \, , \qquad U\left(h, \frac{A}{\mathrm{sgn}(A)}\right) = \#V(A) \ .$$

Let $\mathcal{A} \in Y(A)$. Then

$$\mathrm{sgn}(A) \frac{A}{\mathrm{sgn}(A)} = A = N\left(\mathrm{sgn}(\mathcal{A}) \, \frac{\mathcal{A}}{\mathrm{sgn}(\mathcal{A})}\right) = N(\mathrm{sgn}(\mathcal{A})) \, N\left(\frac{\mathcal{A}}{\mathrm{sgn}(\mathcal{A})}\right) \ .$$

Since $\frac{A}{\operatorname{sgn}(A)}$ and $N(\frac{\mathcal{A}}{\operatorname{sgn}(\mathcal{A})})$ are monic polynomials in $\mathbb{F}_q[T]$,

$$\operatorname{sgn}(A) = N(\operatorname{sgn}(\mathcal{A}))\,, \qquad \frac{A}{\operatorname{sgn}(A)} = N\left(\frac{\mathcal{A}}{\operatorname{sgn}(\mathcal{A})}\right)\,,$$

and $\operatorname{sgn}(\mathcal{A}) \in Y(\operatorname{sgn}(A))$, $\frac{\mathcal{A}}{\operatorname{sgn}(\mathcal{A})} \in V(\frac{A}{\operatorname{sgn}(A)})$. Conversely, if $\mathcal{H} \in V(\frac{A}{\operatorname{sgn}(A)})$, and if $\alpha \in \mathbb{F}_{q^h}$ is such that $N(\alpha) = \operatorname{sgn}(A)$, then $\alpha\mathcal{H} \in Y(A)$. Whence,

$$(ii) \qquad \#Y(A) = \#Y(\operatorname{sgn}(A))\,\#V\left(\frac{A}{\operatorname{sgn}(A)}\right)\,.$$

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 $\mathcal{A}_1, \ldots, \mathcal{A}_r$, $\mathcal{B}_1, \ldots, \mathcal{B}_s$, be the different polynomials in $\mathbb{F}_{q^h}[T]$ such that

$$A = N(\mathcal{A}_1) = \ldots = N(\mathcal{A}_r)\,,$$

$$B = N(\mathcal{B}_1) = \ldots = N(\mathcal{B}_s)\,,$$

then,

$$AB = N(\mathcal{A}_i\mathcal{B}_j)\,, \qquad 1 \le i \le r, \;\; 1 \le j \le s\,.$$

Since A and B are coprime, for every $i = 1, \ldots, r$, every $j = 1, \ldots, s$, $\mathcal{A}_i$ and $\mathcal{B}_j$ 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 $\mathcal{P}$ dividing $\mathcal{A}_i$ such that $v_{\mathcal{P}}(\mathcal{A}_i) \neq v_{\mathcal{P}}(\mathcal{A}_k)$, $v_{\mathcal{P}}$ being the $\mathcal{P}$-adic valuation. Then, $\mathcal{P}$ does not divide $\mathcal{B}_j$ or $\mathcal{B}_\ell$, $v_{\mathcal{P}}(\mathcal{A}_i\mathcal{B}_j) = v_{\mathcal{P}}(\mathcal{A}_i)$, $v_{\mathcal{P}}(\mathcal{A}_k\mathcal{B}_\ell) = v_{\mathcal{P}}(\mathcal{A}_k)$ and $\mathcal{A}_i\mathcal{B}_j \neq \mathcal{A}_k\mathcal{B}_\ell$.

Conversely, if $\mathcal{H} \in \mathbb{F}_{q^h}[T]$ is such that $N(\mathcal{H}) = AB$, every irreducible divisor of $\mathcal{H}$ divides AB. Since A and B are coprime, we may write $\mathcal{H}$ as a product

$$\mathcal{H} = \mathcal{H}_A\,\mathcal{H}_B\,,$$

where the irreducible factors of $\mathcal{H}_A$, resp. $\mathcal{H}_B$ are those of A, resp. B,

$$A = N(\mathcal{H}_A)\,, \qquad B = N(\mathcal{H}_B)\,,$$

and $\mathcal{H}_A$, resp. $\mathcal{H}_B$ is one of the $\mathcal{A}_i$'s, resp. one of the $\mathcal{B}_i$'s. Whence,

$$U(h, AB) = r\, s\ . \blacksquare$$

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

(1) *If $\frac{h}{\text{G.C.D.}(h, \deg P)}$ does not divide m, $U(h, P^m) = 0$,*

(2) *If $\frac{h}{\text{G.C.D.}(h, \deg P)}$ divides m, $U(h, P^m) = \mathrm{p}_d\left(m \frac{\text{G.C.D.}(h, \deg P)}{h}\right)$,*

where $\mathrm{p}_d(b)$ 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 ϵ which will be used to generalize Carlitz's theorem.

Definition. Let ϵ 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 G.C.D.$(h \deg P) = 1$,

$$\epsilon(P^{hb}) = 1\ ,$$

$$\epsilon(P^{hb+1}) = -1\ ,$$

$$\epsilon(P^{hb+r}) = 0 \quad \text{if} \ \ 1 < r < b\ ,$$

(2) If G.C.D.$(h, \deg P) = h$,

$$\epsilon(P^b) = \left(\begin{array}{c} b+h-2 \\ h-2 \end{array} \right)\ ,$$

(3) If G.C.D.$(h, \deg P) = d > 1$, if $\frac{h}{d} = k > 1$,

$$\epsilon(P^{kb}) = \left(\begin{array}{c} b+d-1 \\ d-1 \end{array} \right)\ ,$$

$$\epsilon(P^{kb+1}) = -\left(\begin{array}{c} b+d-1 \\ d-1 \end{array} \right)\ ,$$

$$\epsilon(P^{kb+r}) = 0 \quad \text{if} \ \ 1 < r < k\ .$$

Theorem 4.4. *For any non zero polynomial A, one has*

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

Proof: Let

$$(i) \qquad S(A) = \sum_{D|A}^{*} \epsilon(D) \ .$$

According to proposition 4.1, we have to prove that

$$(ii) \qquad S(A) = U(h, A) \ ,$$

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

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

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

$$(1 - x)^{-d} = \sum_{j=0}^{\infty} \mathrm{p}_d(j)\, x^j \ ,$$

we deduce that $\mathrm{p}_d(j) = \begin{pmatrix} j + d - 1 \\ d - 1 \end{pmatrix}$. 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 $\deg P$,

$$\begin{aligned} U(h, P^m) - U(h, P^{m-1}) &= \mathrm{p}_h(m) - \mathrm{p}_h(m - 1) \\ &= \begin{pmatrix} m + h - 1 \\ h - 1 \end{pmatrix} - \begin{pmatrix} m + h - 2 \\ h - 1 \end{pmatrix} \ , \end{aligned}$$

$$U(h, P^m) - U(h, P^{m-1}) = \begin{pmatrix} m + h - 2 \\ h - 2 \end{pmatrix} \ ;$$

• If G.C.D.$(h, \deg P) = d > 1$, if $k = \frac{h}{d} > 1$,

$$U(h,P^m)-U(h,P^{m-1}) = \begin{cases} \mathrm{p}_d\left(\dfrac{m}{k}\right) = \begin{pmatrix} m+d-1 \\ d-1 \end{pmatrix} & \text{if } k \text{ divides } m, \\ -\mathrm{p}_d\left(\dfrac{m-1}{k}\right) = -\begin{pmatrix} m+d-1 \\ d-1 \end{pmatrix} & \text{if } k \text{ divides } m-1, \\ 0 & \text{otherwise .} \end{cases}$$

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. ∎

REFERENCES

[1] Bourbaki, N. – *Algèbre*, Chapitre 5, Hermann, France.

[2] Carlitz, L. – On the representations of a polynomial on a Galois field as the sum of an even number of squares, *Trans. Amer. Math. Soc.*, 35 (1933), 397–410.

[3] Carlitz, L. – On the representations of a polynomial on a Galois field as the sum of an odd number of squares, *Duke Math. Jour.*, 1 (1935), 298–315.

[4] Carlitz, L. – Sums of squares of polynomials, *Duke Math. Jour.*, 3 (1937), 1–7.

[5] Carlitz, L. – The singular series for sums of squares of polynomials, *Duke Math. Jour.*, 14 (1947), 1105–1120.

[6] Cohen, E. – Sums of an even number of squares on $GF[p^n, x]$, I, *Duke Math. Jour.*, 14, 251–267.

[7] Cohen, E. – Sums of an even number of squares on $GF[p^n, x]$, II, *Duke Math. Jour.*, 14, 543–557.

[8] Cohen, E. – Sums of an odd number of squares on $GF[p^n, x]$, I, *Duke Math. Jour.*, 15, 501–511.

[9] Lidl, R. and Niederreiter, H. – *Introduction to Finite Fields and their Applications*, Cambridge University Press.

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