ACTA ARITHMETICA
190.4 (2019)

Polynomials defining many units in function fields

by

Mohamed El Kati and Hassan Oukhaba (Besançon)

1. Introduction. Recently Osnel Broche and Ángel del Río [1] succeeded in classifying the polynomials with integral coefficients which give units when evaluated on nth roots of a fixed integer a for infinitely many integers n. The proof uses, among other things, the result proved in [3] that if K is a number field and S is a finite set of places of K containing the archimedean places, then the Diophantine equation $X + Y = 1$ has only finitely many solutions (u, v) such that u and v are S-units in K.

The purpose of this article is to study the same question in the case of global function fields, by using the Carlitz cyclotomic theory developed in [2]. More precisely, we fix a finite field $\mathbb{F}_q$, where q is the power of some prime number p. Let $k = \mathbb{F}_q(T)$ be the field of rational functions in the variable T over $\mathbb{F}_q$. Let k^{ac} be an algebraic closure of k. Let $\mathbb{F}_q[T]$ be the subring of polynomials in T. Let us briefly recall the Carlitz action of $\mathbb{F}_q[T]$ on k^{ac}. Let $\mathbb{F}_q[T]\{\varphi\}$ be the $\mathbb{F}_q$-algebra generated by $\mathbb{F}_q[T]$ together with another element φ satisfying

$$\varphi \cdot M = M^q \cdot \varphi \quad \text{for all } M \in \mathbb{F}_q[T]. \tag{1}$$

Any element of $\mathbb{F}_q[T]\{\varphi\}$ is uniquely written as a polynomial in φ with coefficients in $\mathbb{F}_q[T]$. Addition in $\mathbb{F}_q[T]\{\varphi\}$ is done in the usual way. For multiplication we use the above rule (1). Here we should mention that $\mathbb{F}_q[T]\{\varphi\}$ is the non-commutative ring denoted by $\mathbb{F}_q[T][t, S]$ by Nathan Jacobson in [6, Chap. 3, §1, p. 29] where t is an indeterminate and S is the Frobenius automorphism $x \mapsto x^q$ of k^{ac}. Let $D : \mathbb{F}_q[T]\{\varphi\} \to \mathbb{F}_q[T]$ be the homomorphism of rings that assigns to an element $f = \sum_{i=0}^{m} b_i\varphi^i$ its constant term b_0. Then

2010 *Mathematics Subject Classification*: Primary 16U60; Secondary 11R60.
Key words and phrases: Carlitz modules, polynomials defining units, cyclotomic polynomials.
Received 10 October 2017; revised 13 August 2018.
Published online 23 July 2019.

DOI: 10.4064/aa171010-8-10

there exists a unique injective homomorphism of rings

$$\rho : \mathbb{F}_q[T] \to \mathbb{F}_q[T]\{\varphi\}$$

such that if we denote by ρ_M the image of $M \in \mathbb{F}_q[T]$ then

- $D(\rho_a) = a$ for all $a \in \mathbb{F}_q[T]$.
- $\rho_T = \varphi + T$.

In particular, $\rho_a = a$ for all $a \in \mathbb{F}_q$. If $M \in \mathbb{F}_q[T]$, then it is proved in [4, Proposition 1.1] that

$$\rho_M = \sum_{i=0}^{d} \left[\begin{smallmatrix} M \\ i \end{smallmatrix}\right] \varphi^i, \tag{2}$$

where d is the degree of M, $\left[\begin{smallmatrix} M \\ 0 \end{smallmatrix}\right] = M$, $\left[\begin{smallmatrix} M \\ d \end{smallmatrix}\right]$ is the leading coefficient of M and in general each $\left[\begin{smallmatrix} M \\ i \end{smallmatrix}\right]$ is a polynomial in $\mathbb{F}_q[T]$ of degree $(d-i)q^i$.

The polynomial in X with coefficients in $\mathbb{F}_q[T]$ defined by

$$\rho_M(X) = \sum_{i=0}^{d} \left[\begin{smallmatrix} M \\ i \end{smallmatrix}\right] X^{q^i}$$

is called the *Carlitz polynomial* associated to M. We will also denote it by X^M. For instance $X^T = \rho_T(X) = X^q + TX$ and $X^a = aX$ for $a \in \mathbb{F}_q$. One may use Carlitz polynomials to define an action of $\mathbb{F}_q[T]$ on k^{ac}: if $u \in k^{\mathrm{ac}}$ then the action of M on u, denoted by u^M, is defined by

$$u^M = \rho_M(u).$$

This action has been intensively studied in the literature and is referred to as the *Carlitz module*, which is a special case of the general theory of Drinfeld modules. It was applied by David Hayes [4] to obtain an explicit description of the maximal abelian extension of k. Let Λ_M be the set of roots of the polynomial $X^M = \rho_M(X)$ in k^{ac}. It is proved in [4, Theorem 1.6] that Λ_M is an $\mathbb{F}_q[T]$-module isomorphic to $\mathbb{F}_q[T]/M\mathbb{F}_q[T]$. From [4, Section 2] we deduce that if λ is a generator of that module then the other generators are λ^A, where $A \in \mathbb{F}_q[T]$ is prime to M. Moreover, the irreducible polynomial of λ over k is

$$\Phi_M(X) = \prod_{A \in S} (X - \lambda^A),$$

where S is any complete system of representatives of the invertible classes of the ring $\mathbb{F}_q[T]/M\mathbb{F}_q[T]$. We recall that $\Phi_M(X) \in \mathbb{F}_q[T][X]$. It is the analogue of the classical cyclotomic polynomials.

Since $\rho_{T+a} = \varphi + T + a$ for any $a \in \mathbb{F}_q$ we deduce that $\rho_{T+a}(X) = X^q + (T+a)X$. This implies in particular that

$$\Phi_{T+a}(X) = X^{q-1} + T + a.$$

Let us come back to our task. Let $a, N \in \mathbb{F}_q[T]$ with $N \neq 0$, and let $f \in \mathbb{F}_q[T][X]$. If $f \neq 0$ then the following properties are obviously equivalent:

(1) The image of f in $\mathbb{F}_q[T][X]/(X^N - a)\mathbb{F}_q[T][X]$ is invertible.
(2) There exist $p, q \in \mathbb{F}_q[T][X]$ such that $f(X)p(X) + (X^N - a)q(X) = 1$.
(3) $f(\lambda)$ is a unit in $\mathbb{F}_q[T][\lambda]$ for any root λ of $X^N - a$.

Moreover, if f is irreducible then the above three properties are also equivalent to

(4) $\alpha^N - a$ is a unit in $\mathbb{F}_q[T][\alpha]$ for any root α of f.

When (1) is satisfied we say that f *defines units on roots of* $\rho_N(X) - a$.

For any distinct $a, b \in \mathbb{F}_q[T]$ we define the subset $\Delta_{a,b}$ of $\mathbb{F}_q[T][X]$ by declaring that $f \in \Delta_{a,b}$ if and only if f is irreducible in $\mathbb{F}_q[T][X]$ and there exists an infinite sequence $(N_i)_{i\in\mathbb{N}}$ of monic polynomials of strictly increasing degrees and a strictly increasing sequence $(d_i)_{i\in\mathbb{N}^*}$ of positive integers such that f divides all the polynomials

$$\frac{X^{N_i} - a}{b - a} - \left(\frac{X^{N_0} - a}{b - a}\right)^{p^{d_i}}, \qquad i \geq 1.$$

In this article we prove

THEOREM 1.1 (Theorem 3.1). *Let $f \in \mathbb{F}_q[T][X]$ and let $a, b \in \mathbb{F}_q[T]$ be distinct. Let $\Gamma \subset \mathbb{F}_q[T]$ be an infinite set of monic polynomials. Suppose that f defines units on roots of $\rho_N(X) - a$ and on roots of $\rho_N(X) - b$, for all $N \in \Gamma$. Let $g \in \mathbb{F}_q[T][X]$ be an irreducible factor of f. Then g satisfies one of the following two conditions.*

(1) *There exist $\varepsilon \in \mathbb{F}_q^*$ and a monic $M \in \mathbb{F}_q[T]$ such that $g = \varepsilon\Phi_M$. Moreover, if $q > 2$ then $a, b \in \mathbb{F}_q^*$ and M divides all $N \in \Gamma$. If $q = 2$ then a and b have degree at most 1 and M is explicitly described in Propositions 2.7 and 2.9.*
(2) *$g \in \Delta_{a,b}$.*

Our crucial argument in the proof of Theorem 1.1 is the following. Let L be a global function field and let $\mathbb{F}$ be the field of constants of L. Let S be a finite set of primes of L. Then the Diophantine equation $X + Y = 1$ has only finitely many solutions (u, v) such that u and v are nonconstant S-units in L and the extension $L/\mathbb{F}(u)$ is separable. See for instance [7, Theorem 7.19]. But as one may easily check, the couples (u^{p^n}, v^{p^n}) also satisfy the above equation, are nonconstant S-units in L, but the extensions $L/\mathbb{F}(u^{p^n})$ are not separable. This phenomenon leads us to conclude that a polynomial f as in Theorem 1.1 may have irreducible factors which are not necessarily cyclotomic polynomials, the elements of $\Delta_{a,b}$. At this stage this set seems mysterious. Nevertheless, the study of the converse of Theorem 1.1 requires the study of the behavior of the elements of $\Delta_{a,b}$. We hope to be able in the future to completely describe these elements.

In another direction we point out that in Corollary 2.2 we prove that a cyclotomic polynomial Φ_M defines units on roots of $\rho_N(X) - a$ for any $a \in \mathbb{F}_q^*$ and for any monic polynomial $N \in \mathbb{F}_q[T]$ divisible by M.

2. When does a polynomial Φ_M define many units? In this section we give a complete description of the pairs $\{a, \Phi_M\}$ such that $a \in \mathbb{F}_q[T]$ and Φ_M defines units on roots of $\rho_N(X) - a$ for infinitely many monic polynomials $N \in \mathbb{F}_q[T]$. We will use the following properties of the cyclotomic polynomials Φ_M, where M is assumed to be monic. The set of monic divisors of M will be denoted by $\mathrm{Div}(M)$, and as usual we denote the Möbius function on $\mathbb{F}_q[T]$ by μ.

1. We have

$$X^M = \prod_{D \in \mathrm{Div}(M)} \Phi_D(u). \tag{3}$$

2. By Möbius inversion we obtain

$$\Phi_M(X) = \prod_{D \in \mathrm{Div}(M)} (X^D)^{\mu(M/D)}. \tag{4}$$

3. For any irreducible distinct and monic polynomials $P_1, \ldots, P_r$ in R_T, and positive integers $\alpha_1, \ldots, \alpha_r$, we have

$$\Phi_{P_1^{\alpha_1} \cdots P_r^{\alpha_r}}(X) = \Phi_{P_1 \cdots P_r}(X^{P_1^{\alpha_1 - 1} \cdots P_r^{\alpha_r - 1}}). \tag{5}$$

4. If M and L are relatively prime in $\mathbb{F}_q[T]$ and monic, we have

$$\Phi_{ML}(X) = \prod_{D \in \mathrm{Div}(M)} \Phi_L(X^D)^{\mu(M/D)}. \tag{6}$$

5. For $M \neq 1$ in $\mathbb{F}_q[T]$ and monic, we have

$$\sum_{D \in \mathrm{Div}(M)} \mu(D) = 0. \tag{7}$$

For any nonzero $M \in \mathbb{F}_q[T]$ we denote by λ_M a fixed root of $\Phi_M(X)$.

Lemma 2.1. *Let $M, N, a \in \mathbb{F}_q[T]$ be such that M and N are nonzero monic polynomials. Let $D = M/\gcd(M, N)$. Then the following properties are equivalent:*

(a) *Φ_M defines units on roots of $\rho_N(X) - a$.*
(b) *$\lambda_D - a$ is a unit in $\mathbb{F}_q[T][\lambda_M]$.*
(c) *$\lambda_D - a$ is a unit in $\mathbb{F}_q[T][\lambda_D]$.*
(d) *$\Phi_D(a) \in \mathbb{F}_q^*$.*

Proof. See the proof of [1, Proposition 3]. ∎

Corollary 2.2. *Let $a \in \mathbb{F}_q^*$ and let $M_1, \ldots, M_s \in \mathbb{F}_q[T]$ be monic. Then the polynomial $f = \Phi_{M_1} \cdots \Phi_{M_s}$ defines units on roots of $\rho_N(X) - a$ for any N divisible by all the polynomials M_i, $i = 1, \ldots, s$.*

Proof. Let $N \in \mathbb{F}_q[T]$ be monic and divisible by all M_i, $i = 1, \ldots, s$. By definition $f = \Phi_{M_1} \cdots \Phi_{M_s}$ defines units on roots of $\rho_N(X) - a$ if and only if for all $i \in \{1, \ldots, s\}$ the polynomial Φ_{M_i} defines units on roots of $\rho_N(X) - a$. By Lemma 2.1 this is equivalent to $\Phi_{D_i}(a) \in \mathbb{F}_q^*$ for all $i \in \{1, \ldots, s\}$, where $D_i = M_i/\gcd(M_i, N)$. But we have supposed that M_i divides N, thus $D_i = 1$ and then $\Phi_{D_i}(a) = a$. ■

Let us now study the condition $\Phi_M(a) \in \mathbb{F}_q^*$. To this end we let v_∞ be the unique valuation of $k = \mathbb{F}_q(T)$ such that $v_\infty(f) = -\deg(f)$ for any $f \in \mathbb{F}_q[T]$. In particular, $v_\infty(1/T) = 1$. The place of k defined by v_∞ will be called the *place at infinity*.

Lemma 2.3. *Let $M \in \mathbb{F}_q[T] \setminus \{0\}$. Let w be a normalized valuation of $k(\Lambda_M)$ above v_∞. Let $\lambda \in \Lambda_M \setminus \{0\}$. Then $w(\lambda) \geq 0$ or $w(\lambda) = -1$.*

Proof. We know that $(q-1)v_\infty = w$ on k. This result is proved in [4, Theorem 3.2] for those M that are a power of an irreducible polynomial in $\mathbb{F}_q[T]$. The proof in the most general context is given in [5, Proposition 4.15]. Denote $\deg(M)$ by d and the leading coefficient of M by a_d.

If $d = 1$ then by (2) we have $0 = \lambda^M = a_1\lambda^q + M\lambda$. Since $\lambda \neq 0$ we immediately obtain $w(\lambda) = -1$. If $d \geq 2$ and $w(\lambda) < 0$ then for any $i \in \{0, \ldots, d\}$ we have

$$w\left(\left[\begin{smallmatrix} M \\ i \end{smallmatrix}\right]\lambda^{q^i}\right) = f(i),$$

where $f(x) = -(q-1)(d-x)q^x + w(\lambda)q^x$ and $\left[\begin{smallmatrix} M \\ i \end{smallmatrix}\right]$ is defined in (2). But the function f is strictly decreasing on $[0, d-1]$. Therefore

$$w\Big(\sum_{i=0}^{d-1}\left[\begin{smallmatrix} M \\ i \end{smallmatrix}\right]\lambda^{q^i}\Big) = \min_{0 \leq i \leq d-1} w\left(\left[\begin{smallmatrix} M \\ i \end{smallmatrix}\right]\lambda^{q^i}\right) = w\left(\left[\begin{smallmatrix} M \\ d-1 \end{smallmatrix}\right]\lambda^{q^{d-1}}\right) = q^{d-1}(w(\lambda) - (q-1)).$$

The equation $\lambda^M = 0$ then implies $w(\lambda^{q^d}) = q^{d-1}(w(\lambda) - (q-1))$ and hence $w(\lambda) = -1$. ■

Proposition 2.4. *Let $M \in \mathbb{F}_q[T] \setminus \{0\}$ and $a \in \mathbb{F}_q[T]$. Then*

$$\Phi_M(a) \in \mathbb{F}_q^* \implies \begin{cases} a \in \mathbb{F}_q^* & \textit{if } \deg(M) = 0, \\ a \in \mathbb{F}_q & \textit{if } \deg(M) > 0 \textit{ and } q \geq 3, \\ a = M + 1 & \textit{if } \deg(M) = 1 \textit{ and } q = 2, \\ \deg(a) \leq 1 & \textit{if } \deg(M) \geq 2 \textit{ and } q = 2. \end{cases}$$

Proof. The case $\deg(M) = 0$ is trivial since if $M = a_0 \in \mathbb{F}_q^*$ then $X^M = a_0X$ and $\Phi_M(X) = X$. Assume that $\deg(M) \geq 1$ and let $\mathbb{U}_M$ be the set of roots of Φ_M. Let w be a normalized valuation of $k(\Lambda_M)$ above v_∞. Suppose we have $\deg(a) > 1$, or $q > 2$ and $\deg(a) = 1$. Then $w(a) = -(q-1)\deg(a) < -1 \leq w(\lambda)$ for any $\lambda \in \mathbb{U}_M$ thanks to Lemma 2.3. If $\Phi_M(a) \in \mathbb{F}_q^*$ then

$$0 = w(\Phi_M(a)) = \sum_{\lambda \in \mathbb{U}_M} w(a-\lambda) = \deg(\Phi_M) w(a).$$

This implies that $\deg(\Phi_M) = 0$, which is absurd. Therefore we must have $\deg(a) \leq 1$. Moreover if $q > 2$ then $a \in \mathbb{F}_q$. We still have to prove that if $q = 2$ and M and a have degree 1 then $a = M + 1$. But if $M = T + a_0 \in R_T$, then $\rho_{T+a_0}(X) = X^2 + (T + a_0)X$ and $\Phi_M(X) = X + T + a_0$. Hence $\Phi_M(a) \in \mathbb{F}_q^*$ if and only if $a = M + 1$. ∎

Proposition 2.5. *Suppose $q > 2$. Let M be a nonzero monic polynomial in $\mathbb{F}_q[T]$ and let $a \in \mathbb{F}_q[T]$. Then*

$$\Phi_M(a) \in \mathbb{F}_q^* \iff \begin{cases} a \in \mathbb{F}_q^* & \text{if } \deg(M) = 0 \ (M = 1), \\ a = 0 & \text{if } \deg(M) > 0 \text{ and } M \text{ is not a prime power.} \end{cases}$$

Proof. As already observed at the beginning of the proof of Proposition 2.4, if $\deg(M) = 0$ then $\Phi_M(a) \in \mathbb{F}_q^*$ if and only if $a \in \mathbb{F}_q^*$. Suppose that $\deg(M) \geq 1$. According to Proposition 2.4 we have to consider the following cases:

1. The case $a = 0$ and $M = P^n$, where P is a monic irreducible polynomial in $\mathbb{F}_q[T]$. But then by (4) we have $\Phi_M(X) = X^{P^n}/X^{P^{n-1}}$, and in particular $\Phi_M(0) = P \notin \mathbb{F}_q^*$.
2. The case $a = 0$ and $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, where $P_1, \ldots, P_r$ are distinct monic irreducible polynomials in $\mathbb{F}_q[T]$ and $\alpha_1, \ldots, \alpha_r$ are positive integers. Then by evaluating at 0 the polynomial equality $X^M/X = \prod_{D \in \mathrm{Div}(N),\, D \neq 1} \Phi_D(X)$, derived from (3), we obtain
$$M = \prod_{D \in \mathrm{Div}(N),\, D \neq 1} \Phi_D(0).$$
But since $\Phi_{P_i^e}(0) = P_i$ for any positive integer e we find the relation
$$\prod_{D \in \Xi} \Phi_D(0) = 1,$$
where Ξ is the set of the monic divisors of M that are not prime powers. This proves that $\Phi_M(0) \in \mathbb{F}_q^*$.
3. The case $a \in \mathbb{F}_q^*$ and $M = P^n$, where P is a monic irreducible polynomial in $\mathbb{F}_q[T]$. Here also we use the equality $\Phi_M(X) = X^{P^n}/X^{P^{n-1}}$. Since the sequence $(d-i)q^i$ is strictly increasing on $[0, d-1]$ for any $d \geq 1$, we see from (2) that the degree in T of a^{P^n} is $q^{n\deg(P)-1}$. Hence, if $n \geq 2$ then the degree of $\Phi_M(a)$ is $q^{n\deg(P)-1} - q^{(n-1)\deg(P)-1} \neq 0$. If $n = 1$ then the degree of $\Phi_M(a)$ is $q^{\deg(P)-1} \neq 0$.

4. The case $a \in \mathbb{F}_q^*$ and $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, where $P_1, \dots, P_r$ are distinct monic irreducible polynomials in $\mathbb{F}_q[T]$ and $\alpha_1, \dots, \alpha_r$ are positive integers. Set $N = P_1^{\alpha_1 - 1} \cdots P_r^{\alpha_r - 1}$ and $b = a^N$. If $N \neq 1$ then $\deg(b) = q^{\deg(N)-1}$. In particular $b \notin \mathbb{F}_q$. Since $\Phi_M(a) = \Phi_{P_1 \dots P_r}(b)$ by (5), we deduce that $\Phi_M(a) \notin \mathbb{F}_q^*$ thanks to Proposition 2.4. If $N = 1$ then by (4) we have $\Phi_M(a) = \prod_{D \in \mathrm{Div}(M)} (a^D)^{\mu(M/D)}$ and $q \deg(\Phi_M(a)) = \sum_{D \in \mathrm{Div}(M), D \neq 1} \mu(M/D) q^{\deg(D)}$. The assumption $\Phi_M(a) \in \mathbb{F}_q^*$ would imply $\sum_{D \in \mathrm{Div}(M),\, D \neq 1} \mu(M/D) q^{\deg(D)} = 0$. For $i \in \{1, 2\}$ we denote by Ω_i the set of $D \in \mathrm{Div}(M) \setminus \{1\}$ with $\mu(M/D) = (-1)^i$. Since $r \geq 2$ the sets Ω_1 and Ω_2 are not empty and the last equality may be written as
$$\sum_{D \in \Omega_1} q^{\deg(D)} = \sum_{D \in \Omega_2} q^{\deg(D)}.$$
In addition we note that
$$\prod_{i=1}^{r} (1 - q^{\deg(P_i)}) - 1 = \begin{cases} \sum_{D \in \Omega_2} q^{\deg(D)} - \sum_{D \in \Omega_1} q^{\deg(D)} & \text{if } r \text{ is even,} \\ \sum_{D \in \Omega_1} q^{\deg(D)} - \sum_{D \in \Omega_2} q^{\deg(D)} & \text{if } r \text{ is odd.} \end{cases} \tag{8}$$
This implies that $\prod_{i=1}^{r} (1 - q^{\deg(P_i)}) = 1$, which is impossible.

This concludes the proof of the proposition. ∎

Lemma 2.6. *Suppose $q = 2$. Then:*

(i) $\rho_{T^n}(1) = T + 1$ *and* $\rho_{(T+1)^n}(1) = T$ *for any nonzero integer n.*
(ii) $\Phi_{T^n}(1) = \Phi_{(T+1)^n}(1) = 1$ *for any nonzero integer $n > 1$.*
(iii) $\rho_D(1) = (D(0) - D(1))T + D(1)$ *for any $D \in \mathbb{F}_2[T]$. In particular, if $D(0) = D(1) = 1$ we have $\rho_D(1) = 1$.*

Proof. We can show (i) by induction. We deduce (ii) from (i) since we have $\Phi_{P^n}(X) = X^{P^n}/X^{P^{n-1}}$ for any prime P in $\mathbb{F}_q[T]$. As for (iii) it is sufficient to note that $D = D(0) + \sum_{k=1}^{d} T^{n_k}$, then apply (i). ∎

Proposition 2.7. *Suppose $q = 2$ and $a \in \mathbb{F}_2$. Let $M = T^\alpha (T+1)^\beta N$ with N monic and prime to $T(T+1)$. Then $\Phi_M(a) = 1$ if and only if one of the following conditions is satisfied:*

(1) $a = 0$ *and M is not a prime power,*
(2) $a = 1$ *and* $M = 1$,
(3) $a = 1$, $\deg(M) \geq 2$, $N \neq 1$ *and* $(\alpha, \beta) \neq (1, 1)$,
(4) $a = 1$, $\deg(M) \geq 2$, $N = 1$ *but* $\alpha \neq 1$ *and* $\beta \neq 1$,
(5) $a = 1$, $(\alpha, \beta) = (1, 1)$ *and N is not a prime power.*

Proof. Since the case $\deg(M) = 0$ is obvious and the case $\deg(M) = 1$ is impossible by Proposition 2.4, we suppose that $\deg(M) \geq 2$. Then by arguing as for $q > 2$ we may show that $\Phi_M(0) = 1 \Leftrightarrow M$ is not a prime power. If $a = 1$ we obtain the following results.

1. If $M = T^\alpha$ or $M = (T+1)^\alpha$ with $\alpha \geq 2$, then $\Phi_M(1) = 1$ thanks to Lemma 2.6.
2. If $M = T(T+1)$ then $\Phi_M(1) = 0$ since obviously $\Phi_{T(T+1)}(X) = X + 1$.
3. If $M = T^\alpha(T+1)^\beta$ with $\alpha, \beta > 1$, then $1^{T^{\alpha-1}(T+1)^{\beta-1}} = 0$ thanks to Lemma 2.6. Thus $\Phi_M(1) = \Phi_{T(T+1)}(1^{T^{\alpha-1}(T+1)^{\beta-1}}) = \Phi_{T(T+1)}(0) = 1$.
4. If $M = T(T+1)^\beta$ with $\beta > 1$, then $\Phi_M(1) = \Phi_{T(T+1)}(1^{(T+1)^{\beta-1}}) = \Phi_{T(T+1)}(T) = T + 1$.
5. If $M = T^\alpha(T+1)$ with $\alpha > 1$, then $\Phi_M(1) = \Phi_{T(T+1)}(1^{T^{\alpha-1}}) = \Phi_{T(T+1)}(T+1) = T$.
6. If $M = T^\alpha(T+1)^\beta N$ with $(\alpha, \beta) \neq (1,1)$ and $N \neq 1$ monic and prime to $T(T+1)$, then on the one hand $\Phi_{T^\alpha(T+1)^\beta}(1) \neq 0$ by the previous study. On the other hand by Lemma 2.6(iii) we have $1^D = 1$ for any monic divisor D of N. Formulas (6) and (7) then imply
$$\begin{aligned}\Phi_M(1) &= \prod_{D \in \mathrm{Div}(N)} (\Phi_{T^\alpha(T+1)^\beta}(1^D))^{\mu(N/D)} \\ &= (\Phi_{T^\alpha(T+1)^\beta}(1))^{\sum_{D\in\mathrm{Div}(N)} \mu(N/D)} = 1.\end{aligned}$$
7. If $M = T(T+1)N$ with N monic and prime to $T(T+1)$, then by using (6) and the fact that $\Phi_{T(T+1)}(X) = X+1$ we obtain
$$\begin{aligned}\Phi_M(X) &= \prod_{D \in \mathrm{Div}(N)} (\Phi_{T(T+1)}(X^D))^{\mu(N/D)} = \prod_{D \in \mathrm{Div}(N)} (X^D + 1)^{\mu(N/D)} \\ &= \prod_{D \in \mathrm{Div}(N)} ((X+1)^D)^{\mu(N/D)} = \Phi_N(X+1).\end{aligned}$$
Hence $\Phi_M(1) = \Phi_N(0)$. Therefore $\Phi_M(1) = 1$ if and only if N is not a prime power.

This completes the proof of the lemma. ∎

Lemma 2.8. *Suppose $q = 2$. Then:*

(i) $T^{T^n} = 0$ *and* $(T+1)^{(T+1)^n} = 0$*, for any positive integer* n.
(ii) $T^D = D(0).T$ *and* $(T+1)^D = D(1).(T+1)$*, for any* $D \in \mathbb{F}_2[T]$.

Proof. We show (i) by induction on n. To show (ii) we first note that $D = D(0) + \sum_{k=1}^{d} T^{n_k} = D(1) + \sum_{k=1}^{d'} (T+1)^{m_k}$, then we apply (i). ∎

Proposition 2.9. *Suppose $q = 2$ and let $A = T$ or $A = T + 1$. Let $M = A^n N$ with N monic and prime to A, and n a nonnegative integer. Then $\Phi_M(A) = 1$ if and only if either $n \neq 1$ and $N \neq 1$, or $n = 1$ and N is not a prime power.*

Proof. According to Proposition 2.4, $\Phi_M(A) = 1$ implies $M = A + 1$ or $\deg(M) \geq 2$. Assume that $\deg(M) \geq 2$. Then we have to consider the following cases.

1. If $n \geq 2$ and $N = 1$ then by (5) and Lemma 2.8 we have $\Phi_M(A) = \Phi_A(A^{A^{n-1}}) = \Phi_A(0) = A$.
2. If $n \neq 1$ and $N \neq 1$ then since $\Phi_{A^n}(A) = A$ even for $n = 0$ we obtain
$$\Phi_M(A) = \prod_{D\in\mathrm{Div}(N)} (\Phi_{A^n}(A^D))^{\mu(N/D)} = \prod_{D\in\mathrm{Div}(N)} (\Phi_{A^n}(A))^{\mu(N/D)}$$
$$= \prod_{D\in\mathrm{Div}(N)} (A)^{\mu(N/D)} = 1$$
by (6), Lemma 2.8(ii) and (7).
3. If $n = 1$ then since $\Phi_A(X) = X + A$ as explained in the introduction, we have
$$\Phi_M(X) = \prod_{D\in\mathrm{Div}(N)} (\Phi_A(X^D))^{\mu(N/D)} = \prod_{D\in\mathrm{Div}(N)} (X^D + A)^{\mu(N/D)}$$
$$= \prod_{D\in\mathrm{Div}(N)} ((X + A)^D)^{\mu(N/D)} = \Phi_N(X + A),$$
by (6) and Lemma 2.8(ii). Hence $\Phi_M(A) = \Phi_N(0)$. Therefore $\Phi_M(A) = 1$ if and only if N is not a prime power.

This completes the proof of the proposition. ∎

3. Proof of Theorem 1.1. We are now ready to prove

THEOREM 3.1. *Let $f \in \mathbb{F}_q[T][X]$ and let $a, b \in \mathbb{F}_q[T]$ be distinct. Let $\Gamma \subset \mathbb{F}_q[T]$ be an infinite set of monic polynomials. Suppose that f defines units on roots of $\rho_N(X) - a$ and on roots of $\rho_N(X) - b$ for all $N \in \Gamma$. Let $g \in \mathbb{F}_q[T][X]$ be an irreducible factor of f. Then g satisfies one of the following two conditions:*

(1) *There exists $\varepsilon \in \mathbb{F}_q^*$ and a monic $M \in \mathbb{F}_q[T]$ such that $g = \varepsilon\Phi_M$. Moreover, if $q > 2$ then $a, b \in \mathbb{F}_q^*$ and M divides all $N \in \Gamma$. If $q = 2$ then a and b have degree at most 1 and M is explicitly described in Propositions 2.7 and 2.9.*
(2) *$g \in \Delta_{a,b}$.*

Proof. Let $\alpha \in k^{\mathrm{ac}}$ be a root of g. The hypotheses imply that there exists an infinite sequence $N_0, N_1, \ldots$ of monic polynomials of strictly increasing degrees such that $\alpha^{N_i} - a$ and $\alpha^{N_i} - b$ are units in $\mathbb{F}_q[T][\alpha]$. Let S_0 be the set of places v of $L = k(\alpha)$ such that $b - a$ or α is not a unit at v. Let S_∞ be the set of places of L extending the place at infinity. Then $S = S_0 \cup S_\infty$

is finite. Let $\mathcal{O}_S$ be the Dedekind ring of elements of L that are integral at all places outside S. Then $\mathbb{F}_q[T][\alpha] \subset \mathcal{O}_S$, in particular if we put

$$U_i = \frac{b - \alpha^{N_i}}{b - a} \quad \text{and} \quad V_i = \frac{\alpha^{N_i} - a}{b - a},$$

then U_i and V_i are units in $\mathcal{O}_S$ and $U_i + V_i = 1$. Define $\Psi : \mathbb{N} \to \mathcal{O}_S^* \times \mathcal{O}_S^*$ by $\Psi(i) = (U_i, V_i)$, where $\mathcal{O}_S^*$ is the group of units of $\mathcal{O}_S$. If Ψ is not injective, then there exist $i_0 < i_1$ such that $\alpha^{N_{i_1} - N_{i_0}} = 0$. In particular g is, up to a nonzero constant, equal to a cyclotomic polynomial Φ_M. Moreover, for each $N \in \Gamma$ we must have $\Phi_{D_N}(a) \in \mathbb{F}_q^*$ and $\Phi_{D_N}(b) \in \mathbb{F}_q^*$, where $D_N = M/\gcd(M, N)$, thanks to Lemma 2.1. If $q > 2$ then since $a \neq b$ we deduce from Proposition 2.5 that $a, b \in \mathbb{F}_q^*$ and $D_N = 1$, in other words M divides all the polynomials N. If $q = 2$ we see from Proposition 2.4 that $\deg(a), \deg(b) \leq 1$. The corresponding polynomials M are described in Propositions 2.7 and 2.9.

Suppose that Ψ is injective. Then by [7, Theorem 7.19] there exist u and v in $\mathcal{O}_S^*$ and two strictly increasing sequences $(i_j)_{j\in\mathbb{N}}$ and $(d_j)_{j\in\mathbb{N}}$ of positive integers such that

$$U_{i_j} = u^{p^{d_j}} \quad \text{and} \quad V_{i_j} = v^{p^{d_j}}.$$

This implies

$$\frac{\alpha^{N_{i_j}} - a}{b - a} = \left(\frac{\alpha^{N_{i_0}} - a}{b - a}\right)^{p^{d_j - d_0}} \qquad \text{for any } j \geq 0.$$

In other words, g divides in $\mathbb{F}_q[T][X]$ all the polynomials

$$\frac{(b-a)^{p^{d_j - d_0}}}{b - a}(X^{N_{i_j}} - a) - \left(X^{N_{i_0}} - a\right)^{p^{d_j - d_0}}, \qquad j \geq 0.$$

This is exactly the definition of $g \in \Delta_{a,b}$. ∎

Acknowledgements. The authors express their sincere thanks to the referee for the meticulous reading of the manuscript. His remarks and suggestions were highly constructive and helpful.

References

[1] O. Broche and Á. del Río, *Polynomials defining many units*, Math. Z. 283 (2016), 1195–1200.

[2] L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc. 43 (1938), 167–182.

[3] J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications*, in: New Advances in Transcendence Theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, 110–174.

[4] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189 (1974), 77–91.

[5] D. R. Hayes, *Stickelberger elements in function fields*, Compos. Math. 55 (1985), 209–239.
[6] N. Jacobson, *The Theory of Rings*, Amer. Math. Soc. Math. Surveys II, Amer. Math. Soc., New York, 1943.
[7] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, New York, 2002.

Mohamed El Kati, Hassan Oukhaba
Université de Bourgogne Franche-Comté
Laboratoire de Mathématique (LMB)
16 Route de Gray
25030 Besançon Cedex, France
E-mail: nor712@live.fr
hassan.oukhaba@univ-fcomte.fr