PRESERVATION OF THE RESIDUAL CLASSES NUMBERS
BY POLYNOMIALS

JEAN-LUC CHABERT AND YOUSSEF FARES

(Communicated by Matthew A. Papanikolas)

Abstract. Let \( K \) be a global field and let \( \mathcal{O}_{K,S} \) be the ring of \( S \)-integers of \( K \) for some finite set \( S \) of primes of \( K \). We prove that whatever the infinite subset \( E \subseteq \mathcal{O}_{K,S} \) and the polynomial \( f(X) \in K[X] \), the subsets \( E \) and \( f(E) \) have the same number of residual classes modulo \( m \) for almost all maximal ideals \( m \) of \( \mathcal{O}_{K,S} \) if and only if \( \deg(f) = 1 \) when the characteristic of \( K \) is 0 and \( f(X) = g(X^p^k) \) for some integer \( k \) and some polynomial \( g \) with \( \deg(g) = 1 \) when the characteristic of \( K \) is \( p > 0 \).

1. Introduction

In 1968, Davenport raised the following question: what can be said about \( f, g \in \mathbb{Z}[X] \) when, for almost all primes \( p \), \( f(\mathbb{Z}) \mod p = g(\mathbb{Z}) \mod p \), that is, if the set formed by the classes modulo \( p \) of the elements of \( f(\mathbb{Z}) \) is equal to the corresponding set for \( g(\mathbb{Z}) \) for all but finitely many prime numbers \( p \) (see [5, abstract])? We are interested here in an analogous question. But first let us recall some results about Davenport’s problem.

Proposition 1.1 ([3] and [5]). Let \( f, g \in \mathbb{Z}[X] \) be such that \( f(\mathbb{Z}) \mod p = g(\mathbb{Z}) \mod p \) for almost all primes \( p \). If \( f \) is not of the form \( l \circ m \circ n \) where \( l, m, n \in \mathbb{Z}[X] \) are of degree \( \geq 2 \), then \( f \) and \( g \) are linearly related.

Two polynomials \( f \) and \( g \) with coefficients in a field \( L \) are said to be linearly related when there exist \( a \in L^* \) and \( b \in L \) such that \( g(X) = f(aX + b) \). There are generalizations of this result:

Proposition 1.2 ([2]). Let \( K \) be a number field and let \( \mathcal{O}_K \) be its ring of integers. Let \( f, g \in \mathcal{O}_K[X] \) be such that \( f(\mathcal{O}_K) \mod m = g(\mathcal{O}_K) \mod m \) for almost all maximal ideals \( m \) of \( \mathcal{O}_K \). If \( f \) is indecomposable and if \( \deg(f) \neq 7, 11, 13, 15, 21, 31 \), then \( f \) and \( g \) are linearly related.

Moreover, for each of these exceptional degrees, there exist counterexamples. From now on, we write \( f.a.a. \) instead of ‘for almost all’. As a consequence of the previous proposition, we have:

Corollary 1.3. For every number field \( K \) and every polynomial \( f \in K[X] \), if \( \#(f(\mathcal{O}_K) \mod m) = \#(\mathcal{O}_K/m) \) f.a.a. \( m \in \text{Max}(\mathcal{O}_K) \), then \( \deg(f) = 1 \).
For a subset $E$ of $\mathcal{O}_K$, $\#(E \mod m)$ denotes the cardinality of the set $E \mod m$ formed by the classes modulo $m$. This notation is extended to every subset $E$ of $K$ in the following way: $\#(E \mod m)$ denotes the cardinality of the set formed by the classes modulo $m(\mathcal{O}_K)_m$. Note that if the polynomial $f$ belongs to $(\mathcal{O}_K)_m[X]$, then $f(\mathcal{O}_K) \mod m = \mathcal{O}_K \mod m$ is equivalent to $\#(f(\mathcal{O}_K) \mod m) = \#(\mathcal{O}_K \mod m)$.

On the other hand, it is well known that every global field $K$ has the following property (see for instance [4] §X.11):

**Proposition 1.4.** Let $K$ be a global field, let $f \in K[X]$, and let $E$ be an infinite subset of $\mathcal{O}_K$. If $f(E) = E$, then $\deg(f) = 1$.

Along the lines of the last two results, we may be interested in the following generalized question:

Let $K$ be a number field, let $E$ be an infinite subset of the ring of integers $\mathcal{O}_K$ of $K$, and let $f \in K[X]$. Does the condition $f(E) \mod m = E \mod m$ for almost all maximal ideals $m$ of $\mathcal{O}_K$ imply that $\deg(f) = 1$?

We are going to answer yes. In fact, we will consider global fields instead of number fields only, and we will use a weaker hypothesis by replacing the identity of the residue sets with the equality of their cardinalities. Note also that, in the case of a global field $K$, we will speak of primes of $K$, instead of maximal ideals of $\mathcal{O}_K$, in order to avoid any reference a priori to a ring of integers, especially for function fields. Our main result is the following (Theorems 3.3 and 4.4):

**Theorem 1.5.** Let $K$ be a global field, let $S$ be a finite set of primes of $K$, let $E$ be an infinite subset of the ring $\mathcal{O}_{K,S}$ of $S$-integers of $K$, and let $f \in K[X]$. If $f' \neq 0$, then

\begin{equation}
(1) \quad \#(E \mod \mathcal{P}) = \#(f(E) \mod \mathcal{P}) \text{ f.a.a. primes } \mathcal{P} \text{ of } K \iff \deg(f) = 1.
\end{equation}

One implication of (1) is obvious. After some preliminary remarks (§2), we will prove the reverse implication, first for number fields (§3) and then for function fields (§4).

**Remark 1.6.** On the one hand, we weaken one of the hypotheses in Proposition 1.2 by replacing the whole domain $\mathcal{O}_K$ with any infinite subset $E$ of $\mathcal{O}_K$. On the other hand, we have to assume that the degree of one of the polynomials $f$ and $g$ is one. It seems difficult to obtain an assertion with two general polynomials $f$ and $g$ because of the following example which comes from [4]. Let $f \in \mathbb{Z}[X]$ which is not injective, for instance, such that $f(0) = f(1)$. Let $h \in \mathbb{Z}[X]$ such that $h(0) = 1$, for instance, $h(X) = X^2 + X + 1$. Let $g(X) = f(h(X))$ and $E = \{h^n(0) \mid n \geq 0\}$. Then $f(E) = g(E)$, while $f$ may be irreducible with any degree.

2. Preliminary remarks

**Notation.** In this section $D$ denotes an integral domain with quotient field $L$. Recall that, for every subset $E$ of $L$ and every maximal ideal $m$ of $D$, $\#(E \mod m)$ denotes the cardinality of the set formed by the classes modulo $mD_m$ of the elements of $E$. For every set $\mathcal{M}$ of maximal ideals of $D$, if $E$ and $F$ are subsets of $L$,

\begin{equation}
(2) \quad E \equiv_{\mathcal{M}} F \quad \text{will mean} \quad \#(E \mod m) = \#(F \mod m) \quad \text{for all } m \in \mathcal{M}.
\end{equation}

We begin with two examples.
Examples 2.1. (a) Assume that $D$ is semi-local (and $\neq L$). Let $E = J(D)$ be the Jacobson radical of $D$ and let $f(X) = X^n$ where $n \geq 2$. Then $J(D) \equiv_{\text{Max}(D)} f(J(D))$, while $J(D)$ is infinite and $\deg(f) \geq 2$.

(b) Assume that $D$ is not of finite character, that is, there exists a non-zero element $d \in D$ which belongs to infinitely many maximal ideals. Let $E = n$ where $n$ is any fixed maximal ideal, let $f(X) = dX$, and let $M = \{m \in \text{Max}(D) \mid m \neq n$ and $d \in m\}$. Then $\deg(f) = 1$, while $n \neq \mathcal{M} f(n)$ because, for every $m \in \mathcal{M}$, $\#(n \mod m) \geq 2$ and $\#(f(n) \mod m) = 1$.

Thus, for our purpose, it is necessary to consider non-semi-local domains with finite character. The following assertions are obvious:

Lemma 2.2. Let $E$ be a subset of $D$, let $f \in L[X]$, and let $d$ be a non-zero element of $D$. If $\mathcal{M}$ is a subset of $\text{Max}(D)$ such that $f \in D_m[X]$ for every $m \in \mathcal{M}$ and $N = \{m \in \mathcal{M} \mid d \not\in m\}$, then one has

\[(3) \quad E \equiv_{\mathcal{M}} f(E) \Rightarrow E \equiv_{\mathcal{N}} df(E)\]

and

\[(4) \quad E \equiv_{\mathcal{M}} f(E) \Rightarrow dE \equiv_{\mathcal{N}} g(dE)\]

where $dE = \{dx \mid x \in E\}$ and $g(X) = f(X/d)$.

Remarks 2.3. (i) Implication (3) shows that, when $D$ is a domain with finite character, to prove that, for every $f \in K[X]$, we have the implication

\[\#(E \mod m) = \#(f(E) \mod m) \quad \text{f.a.a.} \quad m \in \text{Max}(D) \Rightarrow \deg(f) = 1,\]

it is enough to prove this implication for every $f \in D[X]$.

(ii) Let $E \subseteq D$, $f \in D[X]$, and $m \in \text{Max}(D)$ such that $D/m$ is finite. Clearly,

\[\forall a, b \in D \quad [a - b \in m \Rightarrow f(a) - f(b) \in m],\]

and hence $f$ induces a surjective map

\[f_m : E \mod m \rightarrow f(E) \mod m,\]

so that $\#(f(E) \mod m) = \#(E \mod m)$ means that $f_m$ is injective; that is,

\[\forall a, b \in E \quad [a - b \notin m \Rightarrow f(a) - f(b) \notin m].\]

Lemma 2.4. If $D$ is of finite character and $\mathcal{M}$ is infinite, then

\[(5) \quad f(E) \equiv_{\mathcal{M}} E \Rightarrow f \text{ is injective on } E.\]

Proof. Let $a \neq b \in E$. Then the hypothesis on $D$ implies that there exists a maximal ideal $m \in \mathcal{M}$ such that $a - b \notin m$ and hence, by Remark 2.3(ii), such that $f(a) - f(b) \notin m$. Consequently, $f(a) \neq f(b)$. \qed

Lemma 2.5. Assume that the characteristic of $D$ is $p > 0$. For every subset $E$ of $D$, every $m \in \text{Max}(D)$, and every $f \in D[X]$, letting $g(X) = f(X^p)$, we have

\[\#(E \mod m) = \#(f(E) \mod m) \Leftrightarrow \#(E \mod m) = \#(g(E) \mod m).\]

This is an obvious consequence of the fact that $a - b \in m \Leftrightarrow a^p - b^p \in m$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Corollary 2.6. Assume that the characteristic of $D$ is $p > 0$. If, for all $f \in D[X]$ such that $f' \neq 0$, we have
\[
\#(E \mod m) = \#(f(E) \mod m) \text{ f.a.a. } m \in \text{Max}(D) \Rightarrow \deg(f) = 1,
\]
then, for all $f \in D[X]$, we have
\[
\#(E \mod m) = \#(f(E) \mod m) \text{ f.a.a. } m \in \text{Max}(D)
\Rightarrow f(X) = g(X^{nk}) \text{ for some } g \in D[X] \text{ with } \deg(g) = 1 \text{ and some } k \in \mathbb{N}.
\]

Notation. For every $f \in D[X]$, let
\[
\Phi_f(X,Y) = \frac{f(X) - f(Y)}{X - Y}.
\]
If $\deg(f) = n$, we may write
\[
\Phi_f(X,Y) = \sum_{k=1}^{n} (X - Y)^{k-1}f_k(Y) \text{ with } f_k \in D[X] \text{ and } f_1 = f'.
\]

Proposition 2.7. Let $E \subseteq D$, $f \in D[X]$, and $m \in \text{Max}(D)$. Assume that \#$(f(E) \mod m) = \#(E \mod m)$. Then
\[
\forall a,b \in E, a \neq b \quad [\Phi_f(a,b) \in m \Rightarrow f'(a) \in m \text{ and } f'(b) \in m].
\]

Proof. If $\Phi_f(a,b) \in m$, then $f(a) - f(b) \in m$. The hypothesis implies that $a - b \in m$ (see Remark (ii)). It follows then from the equality
\[
\Phi_f(a,b) = f'(b) + (a - b)f_2(b) + \ldots + (a - b)^{n-1}f_n(b)
\]
that $f'(b) \in m$. \hfill \Box

3. Number fields

Notation. Let $K$ be a global field, that is, a finite extension either of the rational number field $\mathbb{Q}$ or of a rational function field $F(t)$ over the finite field $\mathbb{F}_p$.

Let $S$ be a finite set of primes of $K$ and denote by $\mathcal{O}_{K,S}$ the ring of $S$-integers of $K$, that is,
\[
\mathcal{O}_{K,S} = \bigcap_{P \notin S} \{ x \in K \mid v_P(x) \geq 0 \}
\]
where $P$ denotes any prime of $K$ and $v_P$ the corresponding valuation.

Obviously, the fact that two subsets $E$ and $F$ of $\mathcal{O}_{K,S}$ satisfy
\[
\#(E \mod m) = \#(F \mod m) \text{ f.a.a. } m \in \text{Max}(\mathcal{O}_{K,S})
\]
does not depend on the choice of the finite set $S$, so that we are led to introduce the notation $E \equiv_K F$:
\[
E \equiv_K F \text{ means } \#(E \mod P) = \#(F \mod P) \text{ f.a.a. primes } P \text{ of } K.
\]
Moreover, if $E \equiv_K F$, then, for any finite extension $L$ of $K$, we also have $E \equiv_L F$. Thus, we may use the following notation.

Notation. $E \equiv F$ will mean that there exists a global field $K$ and a finite set $S$ of primes of $K$ such that $E, F \subseteq \mathcal{O}_{K,S}$ and, for almost all maximal ideals $m$ of $\mathcal{O}_{K,S}$, the sets $E$ and $F$ have the same number of classes modulo $m$ (this last assertion does not depend on the choices for $K$ and $S$).
Now we consider the case of number fields. In order to prove our theorem for the ring of integers of a number field, we first recall some results on δ-rings [1].

**Definition 3.1.** An integral domain \( D \) with quotient field \( L \) is said to be a δ-ring if, for every infinite subset \( F \) of \( D \), any rational function \( \varphi \in L(X) \) such that \( \varphi(F) \subseteq D \) admits at most one pole.

Clearly, if \( D \) is a δ-ring, all such rational functions which admit one pole do have the same pole \( e \). Moreover, if a polynomial \( g \in L[X] \) and an infinite subset \( F \subseteq D \) are such that \( g(F) \subseteq U(D) \) where \( U(D) \) denotes the group of units of \( D \), then \( g \) is of the form \( \lambda(X - e)^n \) where \( \lambda, e \in L \) and \( e \) is the previous unique pole.

**Proposition 3.2 ([1 Corollary 18]).** For every number field \( K \) and every finite set \( S \) of maximal ideals of \( \mathcal{O}_K \), the ring \( \mathcal{O}_{K,S} \) of \( S \)-integers of \( K \) is a δ-ring.

Note that if some rational function \( \varphi \in K(X) \) such that \( \varphi(F) \subseteq \mathcal{O}_{K,S} \) for some infinite subset \( F \) of \( \mathcal{O}_{K,S} \) admits a pole \( e \), then \( e \) does not depend on \( \varphi \) nor on \( F \).

**Theorem 3.3.** Let \( K \) be a number field and let \( S \) be a finite set of maximal ideals of \( K \). Let \( E \) be an infinite subset of the ring \( \mathcal{O}_{K,S} \) of \( S \)-integers of \( K \) and let \( f \in K[X] \). Then,

\[
(11) \quad f(E) \equiv E \Rightarrow \deg(f) = 1.
\]

**Proof.** By Remark 2.3, we may assume that \( f \in \mathcal{O}_{K,S}[X] \). Let \( E_1 = \{ a \in E \mid f'(a) \neq 0 \} \). Since the characteristic of \( K \) is 0, \( E_1 \) is infinite. Fix an element \( a \) in \( E_1 \) and let \( T = S \cup \{ m \in \max(\mathcal{O}_K) \mid f'(a) \in m\mathcal{O}_{K,S} \} \). By Proposition 2.7, for every \( x \in E_1 \setminus \{ a \} \), \( \Phi_f(a, x) \notin m \) when \( m \notin T \), that is, \( \Phi_f(a, x) \in \mathcal{O}_{K,T}^\times \). Since, by Proposition 3.2 \( \mathcal{O}_{K,T} \) is a δ-ring, it follows from the containment \( \Phi_f(a, E_1 \setminus \{ a \}) \subseteq \mathcal{O}_{K,T}^\times \) that the polynomial \( \Phi_f(a, X) \) of the form \( \lambda(X - e)^n \) where \( \lambda \) denotes the leading coefficient of \( f \) and \( n \) denotes its degree.

If we consider now another element \( b \in E_1 \), analogously we have \( \Phi_f(b, X) = \lambda(X - e)^n \) with the same \( \lambda \) and the same \( e \). Consequently, \( \deg_X(\Phi_f) = \deg_Y(\Phi_f) = 0 \) and \( n = 1 \). \( \square \)

### 4. Function fields

Now \( K \) denotes a function field with characteristic \( p \) and \( S \) denotes a finite set of primes of \( K \). Denote by \( \mathcal{O}_{K,S} \) the ring of \( S \)-integers of \( K \). The previous proof does not work, but since the group of units \( \mathcal{O}_{K,S}^\times \) is finitely generated [2][Prop. 14.2], we may use for our proof a special case of Voloch’s following result with \( G = \mathcal{O}_{K,S}^\times \times \mathcal{O}_{K,S}^\times \):

**Proposition 4.1 ([8 Theorem 2]).** If \( L \) is a field of characteristic \( p > 0 \) finitely generated over its prime field and \( G \) is a subgroup of \( L^* \times L^* \) such that \( \dim_\mathbb{Q} G \otimes \mathbb{Q} \) is finite, then the equation \( ax + by = 1 \) has at most finitely many solutions \( (x, y) \in G \) unless \( (a, b)^n \in G \) for some \( n \geq 1 \).

**Lemma 4.2.** Let \( K \) be a function field and let \( S \) be a finite set of primes of \( K \). Let \( E \) be an infinite subset of \( \mathcal{O}_{K,S} \), let \( f \in \mathcal{O}_{K,S} \) with degree \( n \geq 2 \), and let \( M \) be an infinite subset of \( \text{Max}(\mathcal{O}_{K,S}) \). If \( f(E) \equiv M \), then

\[
\forall m \in M \forall a, b \in E | a - b \neq 0 \text{ and } a - b \in m \Rightarrow f'(a) \in m \text{ and } f'(b) \in m.
\]
Proof. Fix $a \neq b$ in $E$. Note first that if $a - b \in \mathfrak{m}$, then $f'(a) \in \mathfrak{m}$ is equivalent to $f'(b) \in \mathfrak{m}$, because of the equalities

\begin{align*}
(12) & \quad \Phi_f(a, b) = f'(a) + (b - a)f_2(a) + \ldots + (b - a)^{n-1}f_n(a), \\
(13) & \quad \Phi_f(a, b) = f'(b) + (a - b)f_2(b) + \ldots + (a - b)^{n-1}f_n(b).
\end{align*}

Thus, it is enough to show that $f'(a)f'(b) \in \mathfrak{m}$, and, to do this, we may assume that $f'(a)f'(b) \neq 0$.

By considering a decomposition field $L$ of $\Phi_f(a, X)\Phi_f(b, X)$, we may write

\begin{align*}
\Phi_f(a, X) = \prod_{i=1}^{n-1} (X - a_i) & \quad \text{and} \quad \Phi_f(b, X) = \prod_{j=1}^{n-1} (X - b_j).
\end{align*}

Clearly, for all $i, j$, $\Phi_f(a, a_i) = \Phi_f(b, b_j) = 0$, and hence $f(a_i) = f(a)$ and $f(b) = f(b_j)$. By Lemma 2.4, $f$ is injective on $E$ and $a_i \neq b_j$ for all $i, j$.

Let $T = S \cup \{n \in \text{Max}(\mathcal{O}_{K, S}) | f'(a)f'(b) \in \mathfrak{n}\}$. The set $T$ is finite because of our assumption that $f'(a)f'(b) \neq 0$. Then, by Proposition 2.7, for every $\mathfrak{m} \notin T$, we have: for every $x \in E \setminus \{a\}$, $\Phi_f(a, x) \notin \mathfrak{m}$; and for every $x \in E \setminus \{b\}$, $\Phi_f(b, x) \notin \mathfrak{m}$.

Let $W$ be the set of primes of $L$ dividing the primes of $K$ which are in $T$. Then, for every $x \in E \setminus \{a\}$, the $x - a_i$’s are $W$-units; and for every $x \in E \setminus \{b\}$, the $x - b_j$’s are $W$-units, so that, for every $i, j$, the equation

$$b_j - a_i X + b_j - a_i Y = 1$$

admits infinitely many solutions $(x, y) \in \left(\mathcal{O}_{L, W}^\times\right)^2$, namely $(x - a_i, b_j - x)$ for $x \in E \setminus \{a, b\}$. It follows from Proposition 4.1 that for all $i, j$, $a_i - b_j \in \mathcal{O}_{L, W}^\times$.

For a fixed $i$, we have

$$\Phi_f(a_i, b) = \frac{f(a_i) - f(b)}{a_i - b} = \prod_{j=1}^{n-1} (a_i - b_j).$$

Consequently, $f(a_i) - f(b)$ is also a $W$-unit. Since $\deg(f) \geq 2$, there is at least one $a_i$, and hence $f(a) = f(a_i)$ implies that $f(a) - f(b)$ is a $T$-unit.

Assuming now that $a - b \in \mathfrak{m}$, we also have $f(a) - f(b) \in \mathfrak{m}$. Necessarily, $\mathfrak{m} \in T$; that is, $f'(a)f'(b) \in \mathfrak{m}$. \hfill \Box

**Proposition 4.3.** Let $K$ be a function field, let $S$ be a finite set of primes of $K$, let $E$ be an infinite subset of $\mathcal{O}_{K, S}$, and let $f \in K[X]$. If there exists some element $a \in E$ such that $f'(a) \neq 0$ and such that, for infinitely many $\mathfrak{m} \in \text{Max}(\mathcal{O}_{K, S})$, there exists an element $b_\mathfrak{m} \in E$ with $a - b_\mathfrak{m} \in \mathfrak{m}$, then $\deg(f) = 1$.

**Proof.** Assume that $\deg(f) \geq 2$. Then it follows from the previous lemma that $f'(a) \in \mathfrak{m}$ for infinitely many $\mathfrak{m} \in \text{Max}(\mathcal{O}_{K, S})$. Thus, $f'(a) = 0$. This is a contradiction. \hfill \Box

**Theorem 4.4.** Let $K$ be a function field with characteristic $p > 0$ and let $S$ be a finite set of primes of $K$. For every infinite subset $E$ of $\mathcal{O}_{K, S}$ and every $f \in K[X]$, one has

$$f(E) \equiv_K E \Rightarrow f(X) = g(X^{p^k}) \text{ where } k \in \mathbb{N} \text{ and } \deg(g) = 1.$$
Proof. Let $D = \mathcal{O}_{K,S}$. It follows from Lemma 2.3 that we may assume that $f' \neq 0$. It is then enough to prove that every infinite subset $E$ of $D$ has an element $a$ which satisfies the property given in Proposition 4.3. Assume that there exists a subset $E$ which does not have such an element $a$. Replacing $E$ by $E \setminus \{a | f'(a) = 0\}$, we have

$$\forall a \in E \exists m_1, \ldots, m_s \forall m \in \text{Max}(D) \setminus \{m_1, \ldots, m_s\} \forall x \in E \setminus \{a\} x - a \notin m.$$

Fix two distinct elements $a$ and $b$ in $E$. It follows from the hypothesis on $E$ that there exists a finite subset $T$ of Max($D$) such that for every $m \in \text{Max}(D) \setminus T$ and every $x \in E \setminus \{a, b\}$, $x - a$ and $x - b$ do not belong to $m$. Since we are looking for a contradiction, we may replace $D$ with the ring $D_T$ and assume that

$$\forall x \in E \setminus \{a, b\} (x - a)(x - b) \in U(D),$$

where $U(D)$ denotes the group of units of $D$ (in fact the group of $S \cup T$-units of $K$).

For each $x \in E \setminus \{a, b\}$, let $X = \frac{x - a}{b - a}$ and $X^* = \frac{b - x}{a - b}$. Then $X, X^* \in U(D)$ and $X + X^* = 1$. Furthermore, the hypothesis on $E$ implies that there are infinitely many such pairs. But we know (see for instance [7] Thm. 7.19) that there are only finitely many pairs of separable non-constant units $(U, U^*)$ of $D$ such that $U + U^* = 1$ and that all the solutions of $Y + Y^* = 1$ in non-constant units are of the form $(U^{p^m}, U^{*p^m})$ where $m \geq 0$. Consequently, there exists at least one pair $(U_0, U_0^*)$ of separable units such that $U_0 + U_0^* = 1$ and such that, for infinitely many $m \geq 0$, $(U_0^{p^m}, U_0^{*p^m})$ is some of the previous pairs $(X, X^*)$. Thus we may consider a strictly increasing sequence of integers $\{m_k\}_{k \geq 0}$ such that

$$U_0^{p^m_k} = X_{m_k} = \frac{x_{m_k} - a}{b - a} \text{ with } x_{m_k} \in E.$$

Let $q = p^f$ be the cardinality of the constant field of $K$. From the infinite sequence $\{m_k\}_{k \geq 0}$, we may extract another infinite strictly increasing sequence $\{t_k\}_{k \geq 0}$ such that $t_k \equiv t_0 \text{ (mod } f)$. Let us write $t_k = t_0 + kr_k$. Then

$$X_{t_k} = U_0^{p_{r_k}} = U_0^{p_{r_k} \times q_{r_k}} = X_{t_0}^{p^{r_k}}.$$

We also know (see for instance [7] Thm. 5.12) that there exists $t_0$ such that for every $l \geq t_0$, the function field $K$ has at least one maximal ideal $m_l$ with norm $q^l$. Finally, for $k$ large enough, we have

$$X_{t_k} - X_{t_0} = X_{t_0}^{p^{r_k}} - X_{t_0} \in m_{r_k}.$$ 

Equivalently, for $k$ large enough, $x_{t_k} - x_{t_0} \in m_{r_k}$. Thus, the element $x_{t_0} \in E$ leads to a contradiction to the assumption on $E$. \hfill $\Box$

ACKNOWLEDGMENT

The authors thank David Adam for his advice about function fields.

REFERENCES


DÉPARTEMENT DE MATHEMATIQUES, LAMFA CNRS-UMR 6140, UNIVERSITÉ DE PICARDIE, 80039 AMIENS, FRANCE
E-mail address: jean-luc.chabert@u-picardie.fr

DÉPARTEMENT DE MATHEMATIQUES, LAMFA CNRS-UMR 6140, UNIVERSITÉ DE PICARDIE, 80039 AMIENS, FRANCE
E-mail address: youssef.fares@u-picardie.fr