SUB | NIEDERSÄCHSISCHE STAATS- UND UNIVERSITÄTSBIBLIOTHEK GÖTTINGEN

Werk

Titel: Manuscripta Mathematica
Verlag: Springer
Jahr: 1987
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN365956996_0059
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN365956996_0059

LOG Id: LOG_0032
LOG Titel: Wronskians and linear independence in fields of prime characeteristic.
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN365956996
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN365956996
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=365956996

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.
Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.
Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

manuscripta math. 59, 457 - 469 (1987)

manuscripta mathematica
© Springer-Verlag 1987

WRONSKIANS AND LINEAR INDEPENDENCE IN FIELDS OF PRIME CHARACTERISTIC

Arnaldo Garcia (*) and J.F. Voloch

Introduction

Let k be a field, t a variable and $x_0, x_1, \ldots, x_n$ elements of the power series field $k((t))$. If k has characteristic zero, then $x_0, x_1 \ldots, x_n$ are linearly independent over k if and only if $\det\left(\frac{d^i x_j}{dt^i}\right)_{0 \le i,j \le n} \neq 0$. When k has prime characteristic p the non-vanishing of this determinant (called Wronskian) is equivalent to linear independence over $k((t^p))$. To obtain linear independence criteria over k in positive characteristic F.K. Schmidt [6] introduced generalized Wronskians.

In section 1 we use these generalized Wronskians to obtain our main result (theorem 1 below) which gives a linear independence criterion over $k((t^{p^m}))$ for each $m \geq 1$.

In section 2 we discuss some consequences of this result for function fields of algebraic curves in the context of the theory of Weierstrass Points. In particular, we investigate the plane curves X that are non-classical for the Veronese Morphism, i.e., the plane curves X such that at every point $P \in X$ there exists a conic C with $I(P;X,C) \geq 6$,

(*) This work was completed while the first author was in Heidelberg with a grant from the Alexander von Humboldt-Stiftung

where $I(P;X,C)$ is the intersection multiplicity of X and C at P.

In section 3 we determine when a Fermat Curve X (given by $x^n + y^n + 1 = 0$) is non-classical for the Veronese Morphism.

§ 1 - Linear independence criterion

Following F.K. Schmidt [6], we work in a more general context. Let K be a field. An iterative derivation $\{D^{(i)}, i = 0,1,2,\ldots\}$ on K is a sequence of additive operators on K such that $D^{(0)}$ is the identity operator and

(1) $D^{(i)}(zw) = \sum_{j=0}^{i} D^{(j)}(z)\, D^{(i-j)}(w)$ for all $z,w \in K$.

(2) $D^{(i)} D^{(j)} = \binom{i+j}{i} D^{(i+j)}$, where $\binom{i+j}{i}$ is the binomial coefficient.

From now on every time we refer to (1) or to (2) it will be meant the formulas in the above definition of an iterative derivation.

By (1), $D^{(1)}$ is a derivation on K which we denote simply by D. Also, from (2) it follows that $i!\, D^{(i)} = D^i$. So, in characteristic zero, an iterative derivation is essentially a derivation D and its iterates D^i.

We shall need the following result (see, e.g., [6], Hilfssatz 3).

Lemma 1. Let p be a prime number. Let $a = \sum_{i\geq 0} a_i p^i$ and $b = \sum_{i\geq 0} b_i p^i$, with $0 \leq a_i, b_i \leq p-1$, be the p-adic expansions of the natural numbers a and b. Then $\binom{a}{b}$ is not divisible by p if and only if $a_i \geq b_i$ for all $i \geq 0$.

Let now K be a field of characteristic $p > 0$. We denote by $K_m = \{x \in K \mid D^{(i)}(x) = 0 \text{ for } 1 \leq i < p^m\}$ and by $K_\infty = \{x \in K \mid D^{(i)}(x) = 0 \text{ for } i \geq 1\}$.

Proposition 1. For all $m \geq 1$, K_m is a field. Moreover, $D^{(p^m)}$ is a derivation on K_m and $K_{m+1} = \{x \in K_m \mid D^{(p^m)}(x) = 0\}$.

Proof: For $i < p$ we have $D^{(i)} = \frac{1}{i!} D^i$. It follows that $K_1 = \{x \in K \mid D(x) = 0\}$, and hence that K_1 is a field. Assume that K_m is a field. Then it follows from (1) that $D^{(p^m)}$ is a derivation on K_m. Let $L = \{x \in K_m \mid D^{(p^m)}(x) = 0\}$. We shall show that $K_{m+1} = L$ and the lemma follows by induction. By definition it suffices to show that $D^{(i)}(x) = 0$ for $x \in L$ and for $p^m < i < p^{m+1}$. We write $i = r p^m + s$ with $1 \leq r \leq p-1$ and $0 \leq s \leq p^m - 1$. It follows from (2) that

$$D^{(s)}\left(D^{(p^m)}\right)^r = r!\, D^{(s)} D^{(r p^m)} = r! \binom{i}{s} D^{(i)}.$$

From lemma 1 we have $\binom{i}{s} \not\equiv 0 \bmod p$. Hence, for $x \in L$,

$$D^{(i)}(x) = \frac{1}{r!} \binom{i}{s}^{-1} D^{(s)}\left(D^{(p^m)}\right)^r (x) = 0 . \qquad \square$$

Remark 1. Let k be a field of characteristic $p > 0$ and t a variable. Define $D^{(i)}$ on $k((t))$ by $D^{(i)}(t^j) = \binom{j}{i} t^{j-i}$. For any field K with $k(t) \subseteq K \subseteq k((t))$, K finite algebraic over $k(t)$, we have that $\{D^{(i)}, i = 0,1,2,\ldots\}$ is an iterative derivation on K with $K_m = k K^{p^m}$ and $K_\infty = k$. (See [1], Satz 10)

Theorem 1. Let K be a field of characteristic $p > 0$ and $x_0,\ldots,x_n \in K$. Then $x_0,\ldots,x_n$ are linearly independent over K_m if and only if there exist integers $0 = \varepsilon_0 < \varepsilon_1 < \ldots < \varepsilon_n < p^m$ with $\det\left(D^{(\varepsilon_i)}(x_j)\right) \neq 0$.

Proof: Assume that $x_0,\ldots,x_n$ are linearly dependent over K_m, i.e., that there exist $z_0,\ldots,z_n \in K_m$ (not all zero) with $\sum_{j=0}^{n} z_j x_j = 0$. From (1) and from the definition of K_m, $\sum_{j=0}^{n} z_j D^{(i)}(x_j) = 0$ for $0 \leq i < p^m$. This proves the "if" part of the theorem.

The proof of the "only if" part will be by induction on n, the case $n = 0$ being trivial. Let $x_0, x_1, \ldots, x_n$ be linearly independent over K_m and assume that the conclusion of the theorem does not hold, i.e., that the $n + 1$ vectors

$$(x_j, D^{(1)}(x_j), D^{(2)}(x_j), \ldots, D^{(p^m-1)}(x_j)) \text{ with } 0 \leq j \leq n$$

are linearly dependent over K. Then there exist $z_0, \ldots, z_n \in K$ such that:

$$(*) \qquad \sum_{j=0}^{n} z_j D^{(i)}(x_j) = 0 \quad \text{for} \quad 0 \leq i \leq p^m - 1 .$$

Since $x_0, x_1, \ldots, x_{n-1}$ are linearly independent over K_m we have (by the induction hypothesis) that the n vectors above, for $0 \leq j \leq n-1$, are linearly independent over K. Hence $z_n \neq 0$ and, without loss of generality, we can assume that $z_n = 1$. We shall show that $z_j \in K_m$, for $j = 0, 1, \ldots, n-1$, and then equation (*) with $i = 0$ will give a contradiction that completes the proof.

To prove that $z_j \in K_m$, by proposition 1, it suffices to show that $D^{(r)}(z_j) = 0$ for $1 \leq r \leq p^{m-1}$. This will be done by induction on r.

For $r = 1$, applying the operator D to (*) we have:

$$(i+1) \qquad \sum_{j=0}^{n} z_j D^{(i+1)}(x_j) + \sum_{j=0}^{n-1} D(z_j) D^{(i)}(x_j) = 0 .$$

It follows from (*) that $(i+1) \sum_{j=0}^{n} z_j D^{(i+1)}(x_j) = 0$ for $i < p^m - 1$; this is also true for $i = p^m - 1$ since in this case $i + 1 = 0$ on K. Hence $\sum_{j=0}^{n-1} D(z_j) D^{(i)}(x_j) = 0$ for $0 \leq i \leq p^m - 1$. Since the n vectors above (for $0 \leq j \leq n - 1$) are linearly independent over K we conclude that $D(z_j) = 0$ for $j = 0, 1, \ldots, n-1$.

Assume that $D^{(s)}(z_j) = 0$ for $1 \leq s < r \leq p^{m-1}$ and for $0 \leq j \leq n-1$. Apply now the operator $D^{(r)}$ to (*). It follows from (1) and (2) and from this assumption that:

$$\binom{i+r}{i} \sum_{j=0}^{n} z_j D^{(i+r)}(x_j) + \sum_{j=0}^{n-1} D^{(r)}(z_j) D^{(i)}(x_j) = 0 .$$

As in the case $r = 1$ to prove that $D^{(r)}(z_j) = 0$, it suffices to show that $\binom{i+r}{i} \sum_{j=0}^{n} z_j D^{(i+r)}(x_j) = 0$ for $0 \leq i \leq p^m - 1$. For $i + r < p^m$ this follows from (*), and hence we can assume that $i + r \geq p^m$. We then have:

$$p^m \leq i+r < p^m + p^{m-1} \text{ and } p^m > i \geq p^m - r \geq (p-1)p^{m-1}.$$

Hence the coefficient of p^{m-1} in the p-adic expansion of $i + r$ is zero and that of i is $p-1$. It now follows from lemma 1 that $\binom{i+r}{i} \equiv 0 \bmod p$, and this finishes the proof of the theorem. □

Remark 2. F.K. Schmidt's result (see [6]) is that $x_0,\ldots,x_n$ are linearly independent over K_∞ if and only if there exist $0 = \varepsilon_0 < \varepsilon_1 < \ldots < \varepsilon_n$ with $\det\left(D^{(\varepsilon_i)}(x_j)\right) \neq 0$. This result was generalized by Okugawa (see [4]) for several commuting derivations. Our result is also capable of a similar generalization.

§ 2 - Intersections with conics

Here K will be the function field of an irreducible algebraic curve X defined over an algebraically closed field k of characteristic $p > 0$. Let $\{D^{(i)}, i \geq 0\}$ be an iterative derivation on K defined as in remark 1, where t is a separating variable of K. If $x_0,\ldots,x_n \in K$ are linearly independent over k, then the smallest possible integers $0 = \varepsilon_0 < \varepsilon_1 < \ldots < \varepsilon_n$ (in the lexicographic order) with $\det\left(D^{(\varepsilon_i)}(x_j)\right) \neq 0$ are called the orders of the morphism $\phi : X \longrightarrow \mathbb{P}^n$ given by $(x_0 : x_1 : \ldots : x_n)$ (see [7] or [8]). The morphism ϕ is called classical if $\varepsilon_i = i$ for $i = 0,1,\ldots,n$ and it is called non-classical otherwise.

We shall need the following result (see [7], Satz 4 or [8], corollary 1.9):

Lemma 2. Let $r < \varepsilon$ be two natural numbers. If ε is an order of the morphism ϕ and $\binom{\varepsilon}{r} \not\equiv 0 \bmod p$, then r is also an order of the morphism ϕ.

Proposition 2. Let $0 = \varepsilon_0 < \varepsilon_1 < \ldots < \varepsilon_n$ be the orders of the morphism ϕ. Suppose that $\varepsilon_i = i$ for $i < n$ and that $p \geq n$. If $\varepsilon_n > n$, i.e., if ϕ is non-classical, then ε_n is a power of p.

Proof: First we notice, by lemma 2, that $\varepsilon_n \geq p$. If ε_n is not a power of p, then it follows easily from lemma 1 that we can find r, $p \leq r < \varepsilon_n$, with $\binom{\varepsilon_n}{r} \not\equiv 0 \bmod p$. Now by lemma 2, r is also an order of the morphism ϕ which is absurd since $\varepsilon_{n-1} < r < \varepsilon_n$. □

Suppose now that X is a plane curve given by the equation $f(x,y) = 0$ and let $\phi_1 : X \longrightarrow \mathbb{P}^2$ be the morphism given by $(1 : x : y)$. Since ϕ_1 is an embedding, we have $\varepsilon_i = i$ for $i = 0,1$. Hence, the hypothesis of proposition 2 are satisfied for all $p > 0$. It now follows from theorem 1 that $\varepsilon_2 \geq p^m$ if and only if there exist $z_0, z_1, z_2 \in K$, not all zero, with $z_0 {}^{p^m} + z_1 {}^{p^m} x + z_2 {}^{p^m} y = 0$ on K. By clearing denominators we may assume that z_j (for $j = 0,1,2$) is a polynomial in $k[x,y]$. Hence, $\varepsilon_2 \geq p^m$ if and only if there exist $h, z_0, z_1, z_2 \in k[x,y]$, $h \neq 0$, with $hf = z_0 {}^{p^m} + z_1 {}^{p^m} x + z_2 {}^{p^m} y$. In other words, a plane curve X is such that every simple point on it is a flex if and only if a multiple of the plane equation $f(x,y)$ for X is of the form $z_0 {}^{p^m} + z_1 {}^{p^m} x + z_2 {}^{p^m} y$, where $z_j \in k[x,y]$ for $j = 0,1,2$ and $p^m \geq 3$. A most surprising result, due to Pardini [5] for $m = 1$ and to Hefez [2] for arbitrary m, is that one can take $h = 1$ if X is a non-singular plane curve, i.e., in this case the plane equation $f(x,y)$ for X is itself of the above form. If one allows singularities, then one cannot

always take $h = 1$. For example, for $p \neq 2$, if X is given by

$$f(x,y) = z_o{}^p + z_1{}^p x + z_2{}^p x^2 + z_3{}^p y + z_4{}^p xy + z_5{}^p y^2$$

with $z_o,\ldots,z_5 \in k[x,y]$ and $z_o = \dfrac{z_1^2 z_5 + z_2 z_3^2 - z_1 z_3 z_4}{4 z_2 z_5 - z_4^2}$,

then X is ϕ_1-non-classical. This is so since in this case we have $H(f) = 2(4 z_2 z_5 - z_4^2) f$, where $H(f) = f_{yy} f_x^2 - 2 f_{xy} f_x f_y + f_{xx} f_y^2$ is the Hessian of f.

Remark 3. The curves $y^p + y = x^{p+1}$ are among the first known examples of non-classical curves for the canonical morphism. They are non-singular plane curves of degree $p+1$, and hence of genus $g = \frac{p(p-1)}{2}$. The orders of the morphism ϕ_1 are $0,1$ and p. Since the effective canonical divisors are given by intersections with the curves of degree $p-2$, we conclude that $\{a+bp \,/\, a+b \leq p-2\}$ are the orders of the canonical morphism, which is a result due to F.K. Schmidt [7].

Let now $\phi_s : X \to \mathbb{P}^{N-1}$, $N = \binom{s+2}{2}$, be the s-uple embedding, i.e., the morphism given by $(\ldots : x^i y^j : \ldots)$ with $i+j \leq s$. We have:

Theorem 2. Let X be an irreducible plane curve of degree $d > s$ and suppose that $ds > p \geq N$. Then ϕ_s is a non-classical morphism if and only if a multiple of the plane equation for X is of the form $\sum_{i+j \leq s} z_{ij}^p x^i y^j$, where $z_{ij} \in k[x,y]$ for $i+j \leq s$.

Proof: The hypothesis $d > s$ is just to make sure that the coordinate functions of ϕ_s are linearly independent over k. If $p > ds$, then ϕ_s is always classical (see [8]). Now if ϕ_s is a non-classical morphism, by lemma 2, the last order of ϕ_s is $\geq p$. By theorem 1, we conclude that $x^i y^j$, for $i+j \leq s$, are linearly dependent over $K_1 = K^p$. Conver-

sely, $\sum_{i+j\leq s} z_{ij}^{p} x^i y^j = 0$ on K implies that $\sum_{i+j\leq s} z_{ij}^{p} D^{(r)}(x^i y^j) = 0$ for $r < p$. Hence the last order of ϕ_s is $\geq p$. Since $p \geq N$ by hypothesis, we conclude that ϕ_s is non-classical. □

Now we restrict our attention to the Veronese Morphism $\phi_2 : X \to \mathbb{P}^5$ given by $(1 : x : x^2 : y : xy : y^2)$. If X is ϕ_1-non-classical, then for a generic point $P \in X$ there are lines intersecting X at P with multiplicities 0,1 and $\varepsilon \geq 3$. By proposition 2, ε is a power of p. By taking all products of two of these lines, we conclude that 0,1,2,ε,ε+1 and 2ε are the orders of ϕ_2. Suppose now that X is classical for the morphism ϕ_1. Then 0,1,2,3,4 are orders of ϕ_2, and the hypothesis in proposition 2 are satisfied for $p \geq 5$. We conclude (for $p \geq 5$) that if ϕ_2 is non-classical, then ε_5 is a power of p. To see that some restriction on p is necessary consider the curve $y^8 + y = x^3$ in $p = 2$. Then ϕ_1 is classical and ϕ_2 has the orders 0,1,2,3,4 and 6. For $p \geq 5$, by theorem 1, we have that $\varepsilon_5 \geq p^m$ if and only if there exist $h, z_0, z_1, \ldots, z_5 \in k[x,y]$, $h \neq 0$, with $hf = z_0^{p^m} + z_1^{p^m} x + z_2^{p^m} x^2 + z_3^{p^m} y + z_4^{p^m} xy + z_5^{p^m} y^2$. Unlike the previous case (the morphism ϕ_1), one cannot take $h = 1$ if X is non-singular. As an example take X as the curve given by

$$(1 + x)^p + y^p x + y^{p+1} + x^{p-1} = 0 .$$

It is not hard to check that X is non-singular, ϕ_1 is classical and ϕ_2 is non-classical for $p > 5$ (take $h = x$). Clearly, in this example one cannot take $h = 1$.

§ 3 - Fermat Curves

Let X be the Fermat Curve given by the equation $x^n + y^n + 1 = 0$. We assume that $p \nmid n$, i.e., that X is an irreducible curve. We want to investigate when the Fermat Curve X is non-classical for the morphism ϕ_2. We know al-

ready that if ϕ_1 is non-classical, say with orders 0, 1 and ε where $\varepsilon \geq 3$ is a power of p, then the orders of ϕ_2 are $0,1,2,\varepsilon,\varepsilon+1$ and 2ε, and hence ϕ_2 is also non-classical. For $p \geq 3$, form Pardini's result [5], we know that ϕ_1 is non-classical if and only if p divides $(n-1)$.

We shall need the following result (see [8], corollary 1.7).

Lemma 3. Let $j_0 < j_1 < \ldots < j_{N-1}$ be the orders of a morphism $\phi : X \to \mathbb{P}^{N-1}$ at a point $P \in X$. If the morphism ϕ is non-classical, then we have that p divides $\prod_{i>s} (j_i - j_s)/(i-s)$.

We assume now that $p \nmid (n-1)$ and $p > 5$. A Weierstrass point for the morphism ϕ_1 is a point with $xy = 0$ or a point at infinity, with orders 0,1 and n, as one can easily check. Then we have that $j_0 = 0$, $j_1 = 1$, $j_2 = 2$, $j_3 = n$, $j_4 = n+1$ and $j_5 = 2n$ are the orders of the morphism ϕ_2 at such a Weierstrass point. It now follows from lemma 3 that if ϕ_2 is non-classical, then we have that $p \mid (n-2)(n+1)(2n-1)$ for $p \geq 7$. Conversely, if $p \geq 7$ and $p \mid (n-2)(n+1)(2n-1)$, then ϕ_2 is non-classical as follows from the following identities:

$$n = mp + 2;\ (x^m)^p x^2 + (y^m)^p y^2 + 1 = 0 .$$

$$n = mp - 1;\ (x^m)^p y + (y^m)^p x + xy = xy(x^n + y^n + 1) = 0 .$$

$$2n = mp + 1;\ (x^n + y^n + 1)^2 = x^{2n} + y^{2n} + 2x^n y^n - 1 = 0, \text{ hence}$$
$$\left[(x^m)^p x + (y^m)^p y - 1 \right]^2 = 4 (x^m y^m)^p xy .$$

This proves the following theorem.

Theorem 3. Let X be the Fermat Curve $x^n + y^n + 1 = 0$. Suppose that the characteristic p does not divide n and that $p > 5$. Then X is non-classical for the Veronese Morphism ϕ_2 if and only if p divides $(n-2)(n-1)(n+1)(2n-1)$.

Remark 4. Consider the Fermat Curve $x^n + y^n + 1 = 0$ in characteristic $p = 2n-1$ (for example, $n = 6,7,9,10,\ldots$). One can show that the orders of ϕ_2 are $0,1,2,3,4$ and p. From this one can determine the orders of ϕ_{n-3}, i.e., the orders of the canonical morphism. They are

$$\{a + 2b + (2n-1)c \mid a + b + 2c \leq n - 3\} .$$

These orders are originally determined by Matzat [3].

Theorem 4. Let X be the Fermat Curve $x^n + y^n + 1 = 0$. Suppose that the characteristic p does not divide n.

(a) In characteristic $p = 5$, we have:

a1) If $n = 5d+1$, ϕ_2 is non-classical.

a2) If $n = 5d+2$, ϕ_2 is non-classical if and only if $d \equiv 0 \bmod 5$.

a3) If $n = 5d+3$, ϕ_2 is non-classical if and only if $d \equiv 2 \bmod 5$.

a4) If $n = 5d+4$, ϕ_2 is non-classical if and only if $d \equiv 4 \bmod 5$.

(b) In characteristic $p = 3$, ϕ_2 is always non-classical.

(c) In characteristic $p = 2$, ϕ_2 is classical if and only if $n \equiv 3 \bmod 8$.

Proof: If $n = 5d+1$, then ϕ_1 is non-classical and hence ϕ_2 also. We may assume that $p \nmid (n-1)$. From lemma 3, if ϕ_2 is non-classical, then $p = 5$ divides $\frac{(n-2)(n+1)(2n-1)}{5}$. From this it follows the congruences for d in a2), a3) and a4). The converse follows from the following identities:

If $n = 5d+2$ and $d = 5d'$, then $n = 25d'+2$.

Hence $(x^{d'})^{25} x^2 + (y^{d'})^{25} y^2 + 1 = 0$.

If $n = 5d+3$ and $d = 5d'+2$, then $n = 25d'+13$ and $2n = 25(2d'+1) + 1$.

As before $(x^{2n} + y^{2n} - 1)^2 = 4 x^{2n} y^{2n}$, and hence

$$\left[(x^{2d'+1})^{25} x + (y^{2d'+1})^{25} y - 1 \right]^2 = 4 (x^{2d'+1})^{25} (y^{2d'+1})^{25} xy .$$

If $n = 5d+4$ and $d = 5d'+4$, then $n = 25\,d'+24$. Hence
$(x^{d'+1})^{25} y + (y^{d'+1})^{25} x + xy = xy(x^n + y^n + 1) = 0$.

In characteristic $p = 3$, we may assume $n = 3d+2$ since in the case $n = 3d+1$ we have that ϕ_1 is non-classical. If $d = 3d'$, then $n = 9d'+2$. Hence

$$(x^{d'})^9 x^2 + (y^{d'})^9 y^2 + 1 = 0 .$$

If $d = 3d'+1$, then $n = 9d'+5$ and $2n = 9(2d'+1) + 1$. Hence

$$\left[(x^{2d'+1})^9 x + (y^{2d'+1})^9 y - 1\right]^2 = 4(x^{2d'+1})^9 (y^{2d'+1})^9 xy .$$

If $d = 3d'+2$, then $n = 9d'+8$. Hence

$$(x^{d'+1})^9 y + (y^{d'+1})^9 x + xy = xy(x^n + y^n + 1) = 0 .$$

In characteristic $p = 2$ we have that ϕ_1 is non-classical, and hence ϕ_2 also, for $n \equiv 1$ and $n \equiv 5 \bmod 8$. For $n = 8d+7$, ϕ_2 is non-classical as follows from:

$$(x^{d+1})^8 y + (y^{d+1})^8 x + xy = xy(x^n + y^n + 1) = 0 .$$

So we just have to prove that if $n = 8d+3$, then ϕ_2 is classical. The classical Wronskian for the morphism ϕ_2, i.e., the Wronskian made up with the orders 0,1,2,3,4,5 is (all derivations being derivations with respect to x):

$$\det = \det \begin{pmatrix} D^{(3)}(y) & D^{(3)}(xy) & D^{(3)}(y^2) \\ D^{(4)}(y) & D^{(4)}(xy) & D^{(4)}(y^2) \\ D^{(5)}(y) & D^{(5)}(xy) & D^{(5)}(y^2) \end{pmatrix} .$$

Using $p = 2$ and property (1) of an iterative derivation,

$$\det = \det \begin{pmatrix} D^{(3)}(y) & D^{(2)}(y) & 0 \\ D^{(4)}(y) & D^{(3)}(y) & (D^{(2)}(y))^2 \\ D^{(5)}(y) & D^{(4)}(y) & 0 \end{pmatrix} .$$

Hence $\det = (D^{(2)}(y))^2 (D^{(3)}(y)\ D^{(4)}(y) + D^{(2)}(y)\ D^{(5)}(y))$.
By direct computations we have:

$$y^{n-1}\ D^{(1)}(y) = x^{n-1}\ ;\ y^{2n-1}\ D^{(2)}(y) = x^{n-2}\ ;$$

$$y^{3n-1}\ D^{(3)}(y) = x^{n-3}\ ;\ y^{3n-1}\ D^{(4)}(y) = x^{2n-4}\ ;\ D^{(5)}(y) = 0.$$

This shows that $\det \neq 0$ and hence that ϕ_2 is classical.
This finishes the proof of the theorem. □

Remark 5. Let X be the Fermat Curve $x^n + y^n + 1 = 0$ in characteristic $p \geq N = \binom{s+2}{2}$ and let $n > s$. A Weierstrass point (we assume that $p \nmid (n-1)$) for the morphism ϕ_1 has orders 0,1 and n. Then we have that $\{an + b \mid a + b \leq s\}$ are the orders of the morphism ϕ_s at such a Weierstrass point. It now follows from lemma 3 that if ϕ_s is non-classical, then p divides $\prod_{r=1}^{s} \prod_{t=-s}^{s-r} (rn + t)$. It is possible that the converse also holds.

References

[1] HASSE, H., SCHMIDT, F.K.: Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. J.reine angew.Math. 177, 215 - 237, (1937)

[2] HEFEZ, A.: Projective plane curves in Positive Characteristic, preprint

[3] MATZAT, B.H.: Über Weierstrasspunkte von Fermatkörpern. Dissertation, Universität Karlsruhe (1972)

[4] OKUGAWA, K.: Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory. J.Math. Kyoto Univ. 2, 295 - 322, (1963)

[5] PARDINI, R.: Some remarks on plane curves over fields of finite characteristic. Composito Math. 60, 3 - 17, (1986)

[6] SCHMIDT, F.K.: Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern. Math.Z. 45, 62 - 74, (1939)

[7] SCHMIDT, F.K.: Zur arithmetischen Theorie der algebraischen Funktionen. II. Math.Z. 45, 75 - 96, (1939).

[8] STÖHR, K.O., VOLOCH, J.F.: Weierstrass points and curves over finite fields. Proc.London Math.Soc. (3) 52, 1 - 19, (1986)

Instituto de Matemática Pura e Aplicada (IMPA)
Estrada Dona Castorina 110
22.460 - Rio de Janeiro - R.J.
BRAZIL

(Received July 8, 1987)