STABLE TRANSCENDENCE FOR FORMAL POWER SERIES, GENERALIZED ARTIN-SCHREIER POLYNOMIALS AND A CONJECTURE CONCERNING p-GROUPS

PETER FLEISCHMANN AND CHRIS WOODCOCK

ABSTRACT. Let $f(x)$ be a formal power series with coefficients in the field k and let $n \geq 1$. We define the notion of *n-transcendence* of $f(x)$ over k and, more generally, the *stable transcendence function* $d_k(f(x), n)$. It is shown that, if k has prime characteristic p, this function determines the minimal Krull dimension $d_k(G)$ of the *universal* modular Galois-algebras of an elementary Abelian p-group G, introduced in [2, 3, 4, 5]. Since the concept of n-transcendence is of independent interest in all characteristics, a number of fundamental theorems are proved where the *generalized Artin-Schreier polynomials* surprisingly play a central role. We make a plausible conjecture in the case when $k = \mathbb{F}_p$, the truth of which would imply a conjectural result concerning $d_{\mathbb{F}_p}(G)$ previously investigated by the authors.

MSC: 13A50, 13B05, 13F25, 20C20

1. INTRODUCTION

In this paper we introduce the notion of *n-transcendence* (where n is a positive integer) of a formal power series $f(x)$ over a field k and the *stable transcendence function* $d_k(f(x), n)$. It is shown that if k has prime characteristic p then, for suitable $f(x)$, this function evaluates to the minimal Krull dimension $d_k(G)$ of the *universal* modular "Galois-algebras" of a finite elementary Abelian p-group G of order p^n (see Theorem 5.1). Universal algebras were introduced in [5] as the weakly initial objects in the category of all Galois-algebras of G and it was shown there that every such algebra can be obtained from any universal one simply by "extending the invariant ring" (see [5], Lemma 2.4). Apart from the application mentioned above, we believe that the general notion of n-transcendence and the

Date: March 19, 2018.

function $d_k(f(x), n)$ should be of independent interest in algebra.

In Section 2 we therefore prove a number of theorems concerning these concepts for general k. In particular, we show that if k has characteristic zero and $f(x)$ is not a polynomial then $f(x)$ is always n-transcendental over k. We discuss the plausible conjecture that this is still the case if $k = \mathbb{F}_p$ and show that it fails for proper extension fields.

In section 3 we study an interesting special class of formal power series, the "roots" of the *generalized Artin-Schreier polynomials*, which play a particularly important role in the case when k has prime characteristic p.

In Section 4 we turn our attention to the universal Galois-algebras. In particular we discuss the fundamental conjecture that if $k = \mathbb{F}_p$ then $d_k(G) = n$ where G is a finite group of order p^n. For general k, $d_k(G)$ is always bounded below by the essential dimension $e_k(G)$ of G over k (see [7] for the definition) but it seems very challenging to obtain a sharper lower bound.

In section 5 we prove Theorem 5.1 (as highlighted above) and hence relate the two conjectures in sections 2 and 4. Finally, we prove a theorem which provides the most striking evidence we have at present in direct support of these conjectures.

Acknowledgements: The authors would like to thank an anonymous referee for a careful reading and many helpful comments.

2. n-Transcendence

We investigate a special case of the general problem of the stability of algebraic independence of formal power series under "polynomial perturbation" which turns out to be closely connected to Conjecture 4.11 in the case when G is elementary Abelian (see Section 4). Throughout this section k will be a field, $f(x) = \sum_{i=0}^{\infty} f_i x^i \in k[[x]]$, $n \geq 1$ an integer and p a prime number.

Definition 2.1 (n-transcendental)**.** *The power series $f(x)$ is said to be n-transcendental over k if the n power series in n variables,*
$f(x_i) + P_i(x_1, x_2, \ldots, x_n) \in k[[x_1, x_2, \ldots x_n]]$ *$(1 \leq i \leq n)$, are algebraically independent over k for all choices of polynomials $P_i(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$.*

More generally, we let $d_k(f(x), n)$ *denote the minimum possible transcendence degree over* k *of any field of the form*
$k(f(x_1) + P_1(x_1, \ldots, x_n), f(x_2) + P_2(x_1, \ldots, x_n), \ldots, f(x_n) + P_n(x_1, \ldots, x_n))$
$\subseteq k((x_1, x_2, \ldots, x_n))$ *where* $P_i(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$ *for* $1 \leq i \leq n$.
Thus $d_k(f(x), n) \leq n$ *and* $d_k(f(x), n) = n$ *if and only if* $f(x)$ *is* n*-transcendental over* k.
Clearly $d_k(f(x), n)$ *is subadditive in* n *and so in particular* $\lim_{n\to\infty} \frac{d_k(f(x),n)}{n}$ *exists.*

Remarks 2.2. *It is clear from the definition that:*

(1) *If* $f(x)$ *is* $(n+1)$*-transcendental over* k *then it is* n*-transcendental over* k.
(2) *The property of* n*-transcendence over* k *is stable under "polynomial perturbation".*
(3) *The power series* $f(x)$ *is* 1*-transcendental over* k *if and only if it is not a polynomial.*
(4) *If* $f(x)$ *is transcendental over* $k[x]$ *then it is* n*-transcendental over* k *(since "polynomial perturbations" of the* $f(x_i)$ *are algebraically independent over* $k(x_1, x_2, \ldots, x_n)$ *and so over* k*).*
(5) *If* $R(x) \in xk[x] \setminus \{0\}$ *and* $f(R(x)) \in k[[x]]$ *is* n*-transcendental over* k *then so is* $f(x)$.
(6) *If* k *has prime characteristic* p *and* $f(x)^p$ *is* n*-transcendental over* k *then so is* $f(x)$*. (Indeed, if* $f(x_i)+P_i$ *for* $i = 1, ..., n$ *were not algebraically independent over* k*, then so would be* $f(x_i)^p + P_i^p$*, contradicting* n*-transcendence of* $f(x)^p$*.)*

The following lemma will be needed in the proof of Theorem 2.4:

Lemma 2.3. *Let* R *be a ring (commutative with identity element) and let* $b(x) \in R[x]$ *with positive degree and leading coefficient invertible in* R*. Let* $a(x) \in R[x]$ *with* $(a(x), b(x)) = R[x]$*. Then there is no equation of the form (*)*
$a(x_1)^{\mu_1} a(x_2)^{\mu_2} \ldots a(x_n)^{\mu_n} b(x_1)^{\lambda_1} b(x_2)^{\lambda_2} \ldots b(x_n)^{\lambda_n} =$
$c_1(x_1, x_2, \ldots, x_n) b(x_1)^{\lambda_1+1} + c_2(x_1, x_2, \ldots, x_n) b(x_1)^{\lambda_1} b(x_2)^{\lambda_2+1} + \cdots$

$+c_n(x_1, x_2, \ldots, x_n)b(x_1)^{\lambda_1}b(x_2)^{\lambda_2}\ldots b(x_{n-1})^{\lambda_{n-1}}b(x_n)^{\lambda_n+1} \in R[x_1, x_2, \ldots, x_n]$ *where each* $c_r(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ *and each* μ_i, λ_j *is a natural number.*

Proof. Suppose otherwise so that, for some minimal $n \geq 1$ and some ring R, there exists such an equation (*). Clearly $n > 1$ for otherwise we have $a(x_1)^{\mu_1}b(x_1)^{\lambda_1} = c_1(x_1)b(x_1)^{\lambda_1+1}$ and so $a(x_1)^{\mu_1} = c_1(x_1)b(x_1)$ which contradicts $(a(x), b(x)) = R[x]$. Now divide equation (*) by $b(x_1)^{\lambda_1}$ and then reduce it modulo $b(x_1)$. We hence obtain an equation of the form (*) but now with n replaced by $n-1$ and R replaced by $R' = R[x_1]/(b(x_1))$, the required contradiction to the minimality of n. Note that $a(x_1)$ reduces to an invertible element of R'. □

Let $k[x]_{(x)}$ denote the localization of $k[x]$ at the prime ideal (x).

Theorem 2.4 (Rational Functions)**.** *Suppose that* $f(x) \in k[x]_{(x)} \setminus k[x] \subseteq k[[x]]$ *is rational but not polynomial. Then* $f(x)$ *is* n*-transcendental over* k *for all* $n \geq 1$.

Proof. We have $f(x) = a(x)/b(x)$ where $a(x)$, $b(x) \in k[x]$ with $\deg(b(x)) \geq 1$, $b(0) \neq 0$ and the ideal $(a(x), b(x)) = k[x]$. Suppose that $P_i(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$ for $1 \leq i \leq n$ and $P(X_1, X_2, \ldots, X_n) \in k[X_1, X_2, \ldots, X_n] \setminus \{0\}$ with leading monomial $X_1^{\mu_1}X_2^{\mu_2}\ldots X_n^{\mu_n}$ (with lex ordering).
Suppose further that we have the equation (+)
$P(f(x_1) + P_1(x_1, \ldots, x_n), f(x_2) + P_2(x_1, \ldots, x_n), \ldots, f(x_n) + P_n(x_1 \ldots, x_n)) = 0$.
We must derive a contradiction from this. Now multiply equation (+) by
$b(x_1)^{\mu_1+\lambda_1}b(x_2)^{\mu_2+\lambda_2}\ldots b(x_n)^{\mu_n+\lambda_n}$ where λ_1, λ_2, …, λ_n are suitably large positive integers to obtain an equation of the form (*) contradicting Lemma 2.3 (with $R = k$), as required. □

Before considering the general situation we will need some preliminary results:

Lemma 2.5. *Suppose* $X_1, X_2, \ldots, X_n \in k[[x_1, x_2, \ldots, x_n]]$ *have non-zero Jacobian determinant. Then* $X_1, X_2, \ldots, X_n$ *are algebraically independent over* k.

Proof. This is a well known result! Without loss of generality we may suppose that k is perfect. If X_1, X_2, …, X_n are algebraically dependent over k then choose a

non-trivial polynomial relation between them of least possible total degree. Now partially differentiate it to obtain the required contradiction. □

Of course the converse is false but see [12] for an interesting necessary and sufficient condition for algebraic independence (of polynomials) in prime characteristic p involving what is in effect a subtle "p-adic lifting" of the Jacobian criterion. Unfortunately we haven't been able to utilize this idea at present.

Lemma 2.6. *Suppose that $h(x) \in k[[x]] \setminus k[x]_{(x)}$ is a non-rational formal power series. Let Q be an $n \times n$ matrix with entries in $k[x_1, x_2, \ldots, x_n]$ and let H be the diagonal $n \times n$ matrix with diagonal entries $h(x_1)$, $h(x_2)$, $\ldots$, $h(x_n)$. Then the $n \times n$ matrix $M = H + Q$ has non-zero determinant.*

Proof. The result clearly holds if $n = 1$ since $h(x_1) + Q_{11}(x_1) \neq 0$. Suppose that, for some minimal $n > 1$, $\det(M) = 0$. We will show that $h(x_1)$ is rational, the required contradiction. Expanding the determinant of M by the first row we obtain $0 = dh(x_1) + b$ where d, $b \in k[[x_2, \ldots, x_n]][x_1]$. Now d is an $(n-1) \times (n-1)$ determinant which is non-zero by the minimality of n (just put $x_1 = 0$). Therefore $h(x_1) = -b/d \in k((x_2, \ldots, x_n))(x_1)$. Hence clearly $h(x_1) \in k(x_1)$, as required. □

Proposition 2.7. *Suppose that $f'(x) \in k[[x]] \setminus k[x]_{(x)}$. Then $f(x)$ is n-transcendental over k.*

Proof. This follows directly from Lemmas 2.5 and 2.6. □

Theorem 2.8. *Suppose that $f'(x) \in k[[x]] \setminus k[x]$. Then $f(x)$ is n-transcendental over k.*

Proof. By Proposition 2.7 we may suppose that $f'(x) \in k[x]_{(x)} \setminus k[x]$. Then $f'(x) = a(x)/b(x)$ where $a(x)$, $b(x) \in k[x]$ with $\deg(b(x)) \geq 1$, $b(0) \neq 0$ and the ideal $(a(x), b(x)) = k[x]$ so that there exist $c(x)$, $d(x) \in k[x]$ with $a(x)c(x) + b(x)d(x) = 1$ (*). Now let $P_i(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$ and put $X_i = f(x_i) + P_i(x_1, x_2, \ldots, x_n)$ for $1 \leq i \leq n$. By Lemma 2.5 it is enough to show

that the Jacobian determinant $[J]$ of X_1, X_2, ..., X_n is non-zero. Suppose otherwise so that $[J] = 0$. Then by expanding the determinant $[J]$ and multiplying by $\prod_{i=1}^{n} b(x_i)$ we deduce that $\prod_{i=1}^{n} a(x_i) \in I = (b(x_1), b(x_2), \ldots, b(x_n)) \subset k[x_1, x_2, \ldots, x_n]$. Now put $\alpha = \prod_{i=1}^{n} a(x_i)c(x_i) \in k[x_1, x_2, \ldots, x_n]$. Then clearly $\alpha \in I$ and, by (*) above, $\alpha - 1 \in I$, the required contradiction since I is a proper ideal of $k[x_1, x_2, \ldots, x_n]$. □

Theorem 2.9 (n-transcendence in characteristic zero)**.** *If k has characteristic zero and $f(x)$ is not a polynomial then $f(x)$ is n-transcendental over k.*

Proof. Clearly $f'(x) \in k[[x]] \setminus k[x]$ and so the result follows from Theorem 2.8. □

We next consider the case when k is finite:

Proposition 2.10 (Integrality)**.** *Let k be a finite field of order q. Suppose that $f(x)$ is not integral over $k[x]$. Then $f(x)$ is n-transcendental over k.*

Proof. Suppose that $P_i(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$ for $1 \leq i \leq n$ and $P(X_1, X_2, \ldots, X_n) \in k[X_1, X_2, \ldots, X_n] \setminus \{0\}$ with leading monomial $X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$ (with lex ordering). Suppose further that $P(f(x_1) + P_1(x_1, x_2, \ldots, x_n), f(x_2) + P_2(x_1, x_2, \ldots, x_n), \ldots, f(x_n) + P_n(x_1, x_2, \ldots, x_n)) = 0$ (*). We need to show that $f(x)$ is integral over $k[x]$. We first note that $f(x^{q^m}) = f(x)^{q^m}$ for all $m \geq 0$. Now substitute $x_i = x^{q^{m_i}}$ for $1 \leq i \leq n$ into (*) above where we choose a suitably rapidly increasing sequence of positive integers $m_n, m_{n-1}, \ldots, m_1$ in turn to demonstrate the required integrality of $f(x)$. □

Remark 2.11. *As Theorem 2.9 shows, Proposition 2.10 also holds if k has characteristic zero and may indeed hold for an arbitrary field k. Certainly if $f(x)$ is transcendental over $k[x]$ or if $f(x) \in k[x]_{(x)} \setminus k[x] \subset k[[x]]$ then $f(x)$ is n-transcendental over k (see Remark 2.2(4) and Theorem 2.4).*

Definition 2.12. *Let q be an integer with $q > 1$. Then we define the power series $F_q(x) = \sum_{r=0}^{\infty} x^{q^r} \in k[[x]]$.*

Theorem 2.13 (n-transcendence over a finite field)**.** *Suppose that k is a finite field of order p^m and $f(x)$ is not a polynomial. Suppose further that $f(x)$ is not n-transcendental over k (where $n > 1$). Then either*

(1) *$f(x) = Q(x) + g(x)^{p^s}$ where $Q(x) \in k[x]$, $s \geq 1$, and $g(x) \in xk[[x]]$ is integral over $k[x]$ and is n-transcendental over k, or*
(2) *$f(x) = Q(x) + F_{p^s}(R(x))$ where $Q(x) \in k[x]$, $R(x) \in xk[x]$ and $s \geq 1$.*

(In particular of course $f(x)$ is integral over $k[x]$ and $f'(x) \in k[x]$. Note that $F_{p^s}(x) - F_{p^s}(x)^{p^s} = x$.)

Proof. Recall from Theorem 2.8 and Proposition 2.10 that $f'(x) \in k[x]$ and $f(x)$ is integral over $k[x]$. Without loss of generality we may suppose that $f(x)$ and all the subsequently constructed series have zero constant term. Then $f(x) = Q_0(x) + f_0(x)^p$ where $Q_0(x) \in xk[x]$ has no exponent divisible by p and $f_0(x) \in xk[[x]]$ where $f_0(x)^p$ is not n-transcendental over k. Now if $f_0(x)$ is n-transcendental over k we stop and note that by Proposition 2.10, $f_0(x)^p$ and therefore $f_0(x)$ is integral. Otherwise $f_0(x)$ is not n-transcendental over k, in which case we repeat this procedure with $f(x)$ replaced by $f_0(x)$. Continuing in this way we eventually find that either $f(x)$ has the first form given in the theorem or $f(x) = \sum_{i=0}^{\infty} Q_i(x)^{p^i}$ is algebraic over $k[x]$, where all the $Q_i(x) \in xk[x]$ have no exponent divisible by p. Hence by [13], Corollary 5.4 the k-vector space $\langle \Omega(f) \rangle$ is finite dimensional, where $\Omega(f)$ denotes the orbit of f under the semigroup generated by certain operators E_i defined in [12]. In the present case we have: $E_0(f) = \sum_{i \geq 1} Q_i(x)^{p^{i-1}}$ and $E_0^k(f) = \sum_{i \geq k} Q_i(x)^{p^{i-k}}$ (using the fact that the Q_i have zero constant term). Since k is a finite field and $\langle \Omega(f) \rangle$ is finite-dimensional, the set $\Omega(f)$ is finite, hence $E_0^{r+s}(f) = E_0^r(f)$ for some $r, s \in \mathbb{N}$. It follows that

$$\sum_{i=0}^{\infty} (Q_{i+r}(x))^{p^i} = \sum_{i=0}^{\infty} (Q_{i+r+s}(x))^{p^i}$$

and so $Q_{i+r}(x) = Q_{i+r+s}(x)$, since each $Q_j(x)$ has no exponent divisible by p. Therefore the series $(Q_j)_{j \geq r}$ is periodic of period s. Hence $f(x)$ has the second form given in the theorem since the power series $F_{p^s}(x)$ is additive. □

Remarks 2.14. *Suppose that k has prime characteristic p.*

(1) *By Remarks 2.2 (6) if $f(x) \in k[[x]]$ then $f(x)$ is n-transcendental over k whenever $f(x)^p$ is. If the converse also holds then the first possibility in Theorem 2.13 would be ruled out.*

(2) *Let $s \geq 1$ and $r \geq 1$. If $F_{p^s}(x)$ is n-transcendental over k then so is $F_{p^{sr}}(x)$ by Remarks 2.2 (5) since $F_{p^s}(x) = F_{p^{sr}}(\sum_{j=0}^{r-1} x^{p^{sj}})$. In particular, if some $F_{p^r}(x)$ is not n-transcendental over k then neither is $F_p(x)$.*

(3) *Suppose that $R(x) \in xk[x] \setminus \{0\}$ and $f(x) \in k[[x]]$ with $f(R(x)) \in k[[x]]$ not a polynomial. By Remarks 2.2 (5), if $f(R(x))$ is n-transcendental over k then so is $f(x)$. If the converse also holds then the second possibility in Theorem 2.13 would be ruled out if and only if $F_p(x)$ is n-transcendental over k (by remark (2) just above) and the first possibility in Theorem 2.13 would be ruled out if $k = \mathbb{F}_p$ (taking $R(x) = x^p$; see remark (1) just above).*

Example 2.15. *Let $r \in \mathbb{Z} \setminus \{1\}$ with $(p, r) = 1$. Put $f(x) = (1 + x)^{1/r} = \sum_{j=0}^{\infty} a_j x^j \in k[[x]]$ where $a_j \in \mathbb{F}_p \subseteq k$ denotes the reduction modulo p of $\binom{1/r}{j} \in \mathbb{Z}_p$, the p-adic integers. Then, by Theorem 2.8, $f(x)$ is n-transcendental over k since $f'(x)$ is not a polynomial. Put $g(x) = f(x)^{p^m} \in k[[x]]$ with $m \in \mathbb{N}$.*

(1) *Suppose that $r > 1$. Then $g(x)$ is integral over $k[x]$ with $g'(x) = 0$. However $g(x)$ is still n-transcendental over k at least if $p^m < r$.*
For, if we embed $k[f(x_1), f(x_2), \ldots, f(x_n)] \subseteq k[[x_1, x_2, \ldots, x_n]]$ in $k[t_1, t_2, \ldots, t_n]$ via $f(x_i) = t_i$ for $1 \leq i \leq n$, then $g(x_i) = t_i^{p^m}$ and $x_i = t_i^r - 1$. Hence it is enough to show that the n polynomials $X_i = t_i^{p^m} + Q_i(t_1^r, t_2^r, \ldots, t_n^r) \in k[t_1, t_2, \ldots, t_n]$ $(1 \leq i \leq n)$ are algebraically independent over k for all choices of Q_1, Q_2, …, $Q_n \in k[t_1, t_2, \ldots, t_n]$ (where, without loss of generality we suppose that each Q_i has zero constant term). The result is now clear if $p^m < r$ by considering lowest degree terms. We don't know whether or not $g(x)$ is still always n-transcendental over k if $p^m > r$.

(2) *Suppose that $r = -1$. Then $g(x)$ is rational but not polynomial and so is n-transcendental over k by Theorem 2.4.*

(3) *Suppose that* $r < -1$. *Then* $g(x)$ *is not integral over* $k[x]$ *and so is* n-*transcendental over* k *by Proposition 2.10 at least if* k *is finite.*

(4) *Now let* $R(x) \in xk[x] \setminus \{0\}$ *and put* $h(x) = f(R(x)) = (1 + R(x))^{1/r} \in k[[x]]$. *Then* $h(x)$ *is* n-*transcendental over* k *if* $h'(x) \notin k[x]$ *(by Theorem 2.8) while if* $h'(x) \in k[x] \setminus \{0\}$ *then* $h(x) = (1 + R(x))^{1/r} = rh'(x)(1 + R(x))/R'(x) \in k(x)$ *and so clearly* $h(x) \in k[x]$.

The following conjecture is plausible by Theorem 5.5 below. It would also imply Conjecture 4.11 if G is elementary abelian (see Corollary 5.2):

Conjecture 2.16 (n-transcendence over $\mathbb{F}_p$)**.** *If* $k = \mathbb{F}_p$ *and* $f(x)$ *is not a polynomial then* $f(x)$ *is* n-*transcendental over* k *for all* $n \geq 1$.

Remark 2.17. *The conjecture is certainly false if* k *strictly contains* $\mathbb{F}_p$. *For example, in this case* $F_p(x)$ *is not* 2-*transcendental over* k. *For if* $\alpha \in k \setminus \mathbb{F}_p$ *then the power series* $G_1(x_1, x_2) = F_p(x_1) + (\alpha^{p-1} - 1)^{-1}(x_1 + \alpha^p x_2)$ *and* $G_2(x_1, x_2) = F_p(x_2) - (\alpha^p - \alpha)^{-1}(x_1 + \alpha^p x_2)$ *in* $k[[x_1, x_2]]$ *are algebraically dependent over* k *since* $(G_1 - G_1^p) + \alpha^p(G_2 - G_2^p) = 0$.

If $n = 2$ then we have the following positive result:

Proposition 2.18. *If* $s, r \geq 1$, *then* $F_{p^{sr}}(x)$ *is* 2-*transcendental over* $\mathbb{F}_{p^s}$.

Proof. We embed $R = \mathbb{F}_{p^s}[x, y]$ in $\mathbb{F}_{p^s}[[X, Y]]$ by putting $x = F_{p^{sr}}(X)$ and $y = F_{p^{sr}}(Y)$ so that $X = x - x^{p^{sr}}$ and $Y = y - y^{p^{sr}}$. Hence if $f(X, Y)$, $g(X, Y) \in \mathbb{F}_{p^s}[X, Y]$ we have that $F_{p^{sr}}(X) + f(X, Y) = x + f(x - x^{p^{sr}}, y - y^{p^{sr}}) = A(x, y) \in R$ (say) and $F_{p^{sr}}(Y) + g(X, Y) = y + g(x - x^{p^{sr}}, y - y^{p^{sr}}) = B(x, y) \in R$ (say). We must show that $A(x, y)$ and $B(x, y)$ are algebraically independent over $\mathbb{F}_{p^s}$. Suppose otherwise. (H)

Put $S = \mathbb{F}_{p^s}[A, B] \subseteq R$ and let T be the integral closure of S in R. Then, by hypothesis (H), S is a one-dimensional affine algebra. Since T is an integral extension thereof, it is also one dimensional (see [11], Ex. 9.2, pg. 69). It then follows from [1], Theorem 1, that T is a polynomial $\mathbb{F}_{p^s}$-algebra, $T = \mathbb{F}_{p^s}[t]$ (say). Now let $G = (\mathbb{F}_{p^s}, +)^2$ act on R by putting $(\alpha, \beta)(x) = x + \alpha$ and $(\alpha, \beta)(y) = y + \beta$

for all $(\alpha, \beta) \in G$. Then $(\alpha, \beta)(A) = A + \alpha$ and $(\alpha, \beta)(B) = B + \beta$, so G acts faithfully on S and therefore also on $T = \mathbb{F}_{p^s}[t]$. Now if $g \in G$ then $g(t) = \lambda_g t + \mu_g$ with $\lambda_g \in \mathbb{F}_{p^s}^*$ and $\mu_g \in \mathbb{F}_{p^s}$. Since $g^p = 1_G$ it follows that $\lambda_g = 1$ and therefore the map $g \mapsto \mu_g$ must be injective, so $|G| \leq |\mathbb{F}_{p^s}| = p^s$, a contradiction to the definition of G. So the hypothesis (H) is false. □

3. Generalized Artin-Schreier Polynomials

We now consider a class of formal power series $f(x)$ where the function $d_k(f(x), n)$ can be calculated entirely in terms of rational functions and $f(x)$ is "potentially" not n-transcendental over k (see Theorem 3.5). Throughout this section, k denotes a field of prime characteristic $p > 0$ and $f(x) = \sum_{j=1}^{\infty} f_j x^j \in xk[[x]]$ is a formal power series with zero constant term. We say that the series $f(x)$ satisfies *Property (P)* if,

"given $M > 0$, there are only finitely many exponents j with $f_j \neq 0$ and p-adic valuation $v_p(j) < M$" .

We now characterize all series $f(x)$ which satisfy Property (P) and are algebraic over $k(x)$:

Definition 3.1 (Generalized Artin-Schreier Polynomials)**.** *A polynomial $\theta(x, T) \in k[x][T]$ of the form $\sum_{i=0}^{N} \theta_i T^{p^i} - h(x)$ (where each $\theta_i \in k$, $\theta_0 \neq 0$ and $h(x) \in xk[x]$) is said to be a generalized Artin-Schreier polynomial (AS-polynomial).*

Theorem 3.2. *A generalized Artin-Schreier polynomial $\sum_{i=0}^{N} \theta_i T^{p^i} - h(x)$ has a unique root $f(x) \in xk[[x]]$. Further $f(x)$ satisfies property (P) and is integral over $k[x]$.*

Proof. Without loss of generality we may clearly suppose that $\theta_0 = 1$. Define an $\mathbb{F}_p$-linear map $\alpha : xk[[x]] \longrightarrow xk[[x]]$ by putting $\alpha(g) = \sum_{i=1}^{N} \theta_i g^{p^i}$ for all $g \in xk[[x]]$. Then clearly $I_{xk[[x]]} + \alpha : xk[[x]] \longrightarrow xk[[x]]$ is invertible with inverse $\sum_{s=0}^{\infty} (-1)^s \alpha^s$, which is well defined, as any finite-dimensional piece of $xk[[x]]$ involves only finitely many terms of the sum. Note that any exponent j appearing in $\alpha^s(g)$ with $\alpha^s(g)_j \neq 0$ is divisible by p^s. Now $(I_{xk[[x]]} + \alpha)(f) = h$ and so

$f = (I_{xk[[x]]} + \alpha)^{-1}(h) = \sum_{s=0}^{\infty}(-1)^s\alpha^s(h) \in xk[[x]]$ is a root of the Artin-Schreier polynomial and uniquely determined. It also satisfies property (P), because each $\alpha^s(h)$ is a polynomial. Clearly $f(x)$ is integral over $k[x]$. □

Thus, for example, $T^{p^s} - T + x$ has root $F_{p^s}(x)$ (see Definition 2.12). We now prove a converse to Theorem 3.2:

Theorem 3.3. *Suppose that $f(x) = \sum_{j=1}^{\infty} f_j x^j \in xk[[x]]$ is algebraic over $k(x)$ and satisfies property (P). Then the series $f(x)$ is a root of a generalized Artin-Schreier polynomial, that is (E): $\sum_{m=0}^{N} \theta_m f(x)^{p^m} = h(x) \in xk[x]$ where each $\theta_m \in k$ with $\theta_0 \neq 0$.*

Proof. Without loss of generality we may suppose that k is perfect: indeed, let k^{per} be the perfect closure of k, $B \subseteq k^{per}$ a k-basis of k^{per} and $f(x) \in xk[[x]]$ satisfying (P). Then $f(x) \in xk^{per}[[x]]$ satisfying (P). By the assumption there is an AS polynomial $\Theta := \sum_{m=0}^{N} \theta_m T^{p^m} - h(x) \in k^{per}[x, T]$ with $\Theta(x, f(x)) = 0$ and $\theta_0 \neq 0$. It is easily seen that $\Theta(x, T) = \sum_{b\in B} \Theta_b(x, T) \cdot b$ with AS polynomials $\Theta_b(x, T) \in k[x, T]$. It follows that $0 = \sum_{b\in B} \Theta_b(x, f(x)) \cdot b \in \oplus_{b\in B} k[x]b = k^{per}[x]$, with $\Theta_b(x, f(x)) \in k[x]$. Hence $\Theta_b(x, f(x)) = 0$ for all $b \in B$ and at least one has "$\theta_0 \neq 0$".

So we now assume that k is perfect. Since $f(x)$ satisfies property (P), $f(x) = \sum_{s=0}^{\infty} Q_s(x)^{p^s}$ where each $Q_s(x) \in xk[x]$ has no exponent (with non-zero coefficient) appearing which is divisible by p. Now, for each $m \geq 0$, put $f_m(x) = \sum_{s=0}^{\infty} Q_{s+m}(x)^{p^s} \in xk[[x]]$. Then, since $f(x)$ is algebraic over $k(x)$, it follows from [13] Corollary 5.4, similarly to the proof of 2.13 above, that $\{f_m(x)\}$ $(m \geq 0)$ span a finite dimensional vector space over k. Hence there exist θ_0, θ_1, ..., $\theta_N \in k$ (w.l.o.g. $\theta_N \neq 0$) such that $\sum_{m=0}^{N} \theta_m f_m(x) = 0$. Now each $f_m(x)^{p^m} = f(x) - \sum_{s=0}^{m-1} Q_s(x)^{p^s}$. Hence, putting $\phi_m = (\theta_{N-m})^{p^N} \in k$, we have the equation $\sum_{m=0}^{N} \phi_m f(x)^{p^m} = h(x) \in xk[x]$ (say) with $\phi_0 \neq 0$, and so $f(x)$ is a root of a generalized Artin-Schreier polynomial, as required. □

In the situation of Theorem 3.3, for each $n \geq 1$, we can calculate $d_k(f(x), n)$ entirely in terms of rational functions:

Corollary 3.4. *Employing the notation of Theorem 3.3 and putting* $\phi(T) = \sum_{m=0}^{N} \phi_m T^{p^m} \in k[T]$, $d_k(f(x), n)$ *is the minimum possible transcendence degree over* k *of any field of the form* $k(h(x_1)+\phi(P_1), h(x_2)+\phi(P_2), \ldots, h(x_n)+\phi(P_n)) \subseteq k(x_1, x_2, \ldots, x_n)$ *where* $P_i = P_i(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$ *for* $1 \leq i \leq n$. *If, further,* $h(x) = cx$ *where* $c \in k$ *with* $c \neq 0$, *then, putting* $y_i = \phi(x_i)$ *for* $1 \leq i \leq n$, $d_k(f(x), n)$ *is the minimum possible transcendence degree over* k *of any field of the form* $k(x_1 + Q_1, x_2 + Q_2, \ldots, x_n + Q_n) \subseteq k(x_1, x_2, \ldots, x_n)$ *where* $Q_i = P_i(y_1, y_2, \ldots, y_n) \in k[x_1, x_2, \ldots, x_n]$ *for* $1 \leq i \leq n$.

Proof. $k[T]$ is integral over $k[\phi(T)]$ and so $k[f(x_1)+P_1, f(x_2)+P_2, \ldots, f(x_n)+P_n]$ is integral over $k[h(x_1)+\phi(P_1), h(x_2)+\phi(P_2), \ldots, h(x_n)+\phi(P_n)]$ since $\phi(f(x)) = h(x)$. The first result now follows from Definition 2.1. Now assume that $h(x) = cx$ with $c \neq 0$. W.l.o.g. $c = 1$ and $\phi(f(x_i)) = x_i$. By definition, $d_k(f(x), n) = \min\, tr.deg.k[f(x_i) + P_i(x_1, \cdots, x_n) \mid i = 1, \cdots, n] =$

$$\min\, tr.deg.k[f(x_i) + P_i(\phi(f(x_1)), \cdots, \phi(f(x_n))) \mid i = 1, \cdots, n] =$$

$$\min\, tr.deg.k[x'_i + P_i(\phi(x'_1), \cdots, \phi(x'_n)) \mid i = 1, \cdots, n] =$$

$$\min\, tr.deg.k[x'_i + P_i(y'_1, \cdots, y'_n) \mid i = 1, \cdots, n],$$

where we set $x'_i := f(x_i)$ and $y'_i = \phi(x'_i)$. Re-replacing x'_i by x_i gives the claim. □

Theorem 3.5. *Suppose that* k *is a perfect field of prime characteristic* p *and* $f(x) \in xk[[x]]$ *is not a polynomial. Suppose further that* $f(x)$ *is not* n*-transcendental over* k *(where* $n > 1$*). Then either*

(1) $f(x) = Q(x) + g(x)^{p^s}$ *where* $Q(x) \in xk[x]$, $s \geq 1$ *and* $g(x) \in xk[[x]]$ *is algebraic over* $k(x)$ *and is* n*-transcendental over* k *or*
(2) $f(x)$ *is a root of a generalized Artin-Schreier polynomial.*

Proof. We follow the proof of Theorem 2.13 (1) and (2). By Remark 2.2 4. $f(x)$ is algebraic; in case (1) this implies that $g(x)$ is algebraic. In case (2) the proof shows that $f(x)$ has the form $\sum_{i=0}^{\infty} Q_i(x)^{p^i}$ with $Q_i(x) \in xk[x]$ and no exponent divisible by p, so $f(x)$ has property (P) and hence by Theorem 3.3 is a root of a generalized Artin-Schreier polynomial. □

Remark 3.6. *Suppose that k is finite. Then we may assume that the equation (E) in Theorem 3.3 has the form $f(x)^{p^M} - f(x) =: R(x) \in xk[x]$.*
For we may first suppose that $\phi_0 \neq 0$ and $\phi_N = 1$. Let $\phi(T) = \sum_{m=0}^{N} \phi_m T^{p^m} \in Tk[T]$ so that $\phi(T)$ is a monic and separable "p-polynomial" (see [10]*, Chapter 3, Section 4). Hence $\phi(T)$ has distinct roots V (say) in a splitting field $K \supseteq k$ where $|K| = p^M$ (say) and V is an $\mathbb{F}_p$-subspace of K. Hence $\phi(T) = \prod_{\alpha \in V}(T - \alpha)$.*
Put $D(T) = T^{p^M} - T \in Tk[T]$. Then $D(T)$ is a p-polynomial with $D(T) = \prod_{\beta \in K}(T - \beta)$. Now $\phi : K \longrightarrow K$ (where $\beta \mapsto \phi(\beta)$) is an $\mathbb{F}_p$-linear, $\mathrm{Gal}(K/k)$-equivariant map with kernel V and image W (say). Hence, if we put $D_W(T) = \prod_{w \in W}(T - w) \in Tk[T]$ (not just $TK[T]$), then $D_W(T)$ is a p-polynomial and further it follows easily that $D(T) = D_W(\phi(T))$ (a "symbolic product" of p-polynomials; see [10]*, Chapter 3, Section 4).*
Since $\phi(f(x)) = h(x)$ we therefore have that

$$f(x)^{p^M} - f(x) = D(f(x)) = D_W(\phi(f(x))) = D_W(h(x)) = R(x)$$

(say) where $R(x) \in xk[x]$ (see also Theorem 2.13 (2)).

4. Universal Algebras

We now consider an outstanding conjecture concerning "non-linear" modular representations of finite p-groups: Let k be a field of prime characteristic p and let G be a finite p-group of order p^n ($n \geq 1$). We recall some results from [2], [3], [4] and [5]:

Definition 4.1 (Trace-Surjective Algebras)**.** *Let A be a finitely generated k-algebra (commutative with identity element 1) together with a faithful action of G on A. Then A is said to be* trace-surjective *if there exists $w \in A$ such that $\mathrm{tr}_G(w) := \sum_{g \in G} g(w) = 1$. Equivalently A is a Galois extension of the invariant ring $A^G := \{a \in A \mid g(a) = a \text{ for all } g \in G\}$ (see* [2]*, Proposition 4.4).*

Remark 4.2. *Let $(A^G)G$ be the group ring of G over A^G. Then A is a free $(A^G)G$-module of rank one generated by any element w of A with $tr_G(w) = 1$ and hence A is a free A^G-module of rank $|G|$ (see* [2]*, Theorem 4.1).*

Examples 4.3. (1) *$A = K$, a Galois field extension of $k = K^G$ with* $\mathrm{Gal}(K/k) = G$.

(2) *Let V be a finite dimensional linear representation of G over k, $S(V) :=$* $\mathrm{Sym}(V)$*, the symmetric algebra of V and $A := S(V)_v$ or $S(V)/(v-1)$, where $v \in V^G \setminus \{0\}$ with $v^m = tr_G(f)$ for some $f \in S(V)$ and $m \geq 1$. Only for relatively few groups G will there be such an "almost linear" A defined over $\mathbb{F}_p$ and with Krull dimension as low as n (see* [3]*).*

(3) *Let $A = U_k(G)$ be the algebra defined in* [2] *Theorem 5.4. Then A is a polynomial k-algebra of Krull dimension n with faithful G-action. This action is non-linear (but "triangular"), it is defined over $\mathbb{F}_p$ and the invariant ring A^G is also polynomial (see* [2, 3, 4, 5]*). For example:*

(a) *If $G =< \sigma_1, \sigma_2, \ldots, \sigma_n >$ is elementary Abelian then* $U_k(G) = k[x_1, x_2, \ldots, x_n]$ *where each* $\sigma_i(x_j) = x_j + \delta_{ij}$ *and* $\mathrm{tr}_G((-1)^n x_1^{p-1} x_2^{p-1} \ldots x_n^{p-1}) = 1$. *Further* $U_k(G)^G = k[x_1 - x_1^p, x_2 - x_2^p, \ldots, x_n - x_n^p]$.

(b) *If $G =< \sigma >$ is cyclic of order p^2 then $U_k(G) = k[x, y]$ where* $\sigma(x) = x+1$, $\sigma(y) = y+x^{p-1}$ *and* $\mathrm{tr}_G(x^{p-1}y^{p-1}) = 1$. *Further, if $F(x)$ denotes the reduction modulo p of the polynomial $B_{p^2-p+1}(x)/(p^2-p+1) - B_p(x)/p - \delta_{p,2}/4 \in \mathbb{Z}_p[x]$ (where $B_r(x)$ denotes the r-th Bernoulli polynomial) then $U_k(G)^G = k[x^p - x, y^p - y - F(x)]$. This follows directly from Remark 4.2, the von Staudt-Clausen theorem and the basic difference equation for the Bernoulli polynomials (see* [8]*, Chapter 2).*

We do not know whether or not $U_k(G)$ is the only trace-surjective polynomial k-algebra U of dimension n which is "triangular" in the sense of Proposition 4.7. However it follows easily from [5], Proposition 2.9 that its tensor square $U \otimes_k U$ is independent of the choice of U.

Definition 4.4. *A trace-surjective algebra A_0 is said to be universal if whenever A is a trace-surjective algebra there is a G-equivariant k-algebra homomorphism $\theta : A_0 \longrightarrow A$.*

Remark 4.5. *In the standard categorical terminology such an algebra A_0 would be described as being "weakly initial" rather than "universal". However here it carries rather more than usual significance since it can be shown that A is isomorphic to $A_0 \otimes_{A_0^G} A^G$ (see* [2]*, the proof of Theorem 1.2). In particular the minimal number $m_k(G)$ of generators for A_0 as an A_0^G-algebra is independent of the choice of universal algebra A_0 and every trace-surjective algebra A can be generated as an A^G-algebra by $m_k(G)$ elements. Further, taking $A_0 = U_k(G)$, we obtain an explicit "structure theorem" for A (see* [2]*, Theorem 1.2). For example this recovers the Artin-Schreier theorem in the case when G is cyclic of order p and $A^G = k$.*

Example 4.6. *$A_0 = S(V)_v$, $S(V)/(v-1)$ and $U_k(G)$ (as in Examples 4.3 (2) and (3) above) are universal algebras. In fact both $U_k(G)$ and $S(V)/(v-1)$ are polynomial with "triangular" action of G (see Proposition 4.7 below).*

The following Proposition provides a ready source of universal algebras:

Proposition 4.7. *A trace-surjective polynomial algebra $A_0 = k[x_1, x_2, \ldots, x_m]$ is universal if the action of G on A_0 is "triangular" in the sense that $g(x_i) - x_i \in k[x_1, x_2, \ldots, x_{i-1}]$ for all $g \in G$ and $1 \leq i \leq n$. Further the invariant ring A_0^G is "stably polynomial".*

Proof. This follows directly from Proposition 2.9, Theorem 2.11 and Theorem 2.13 of [5]. □

Remark 4.8. *As noted above the invariant ring $U_k(G)^G$ is actually polynomial. We also conjecture that the invariant ring $(S(V)/(v-1))^G$ is always polynomial which is certainly the case if either G is cyclic or V is a free kG-module (see* [4]*, Theorems 4 and 5). Note however that not every "stably polynomial" k-algebra is polynomial (see* [6]*).*

Definition 4.9. *We denote by $d_k(G)$ the minimum value of the Krull dimension of a universal algebra A_0.*

Remarks 4.10. (1) *Thus $d_k(G) \leq n$ since the universal (polynomial) algebra $U_k(G)$ has Krull dimension n.*

(2) *Clearly we may restrict attention to trace-surjective subalgebras A_0 of $U_k(G)$ (or of any other fixed universal algebra) which are themselves necessarily universal.*

(3) *If H is a subgroup of G then $d_k(H) \leq d_k(G)$. For, by Proposition 4.7, $U_k(G)$ is universal for H and any trace-surjective k-subalgebra for G is also trace-surjective for H.*

It can be shown that $d_k(G)$ is always bounded below by the essential dimension $e_k(G)$ of G over k and further if G is elementary Abelian then $e_k(G) \leq 2$ (see [5], section 4). However, based on the evidence presently available, we venture to make the following sharp conjecture in the case when $k = \mathbb{F}_p$.

Conjecture 4.11 (Krull Dimension)**.** *If $k = \mathbb{F}_p$ then $d_k(G) = n$ (this value being achieved by the universal polynomial algebra $U_k(G)$ as above).*

Remarks 4.12. (1) *If G is elementary Abelian then the conjecture implies a substantial difference between $d_k(G)$ and $e_k(G)$. We consider this important special case in Section 5.*

(2) *Conjecture 4.11 is true for $n \leq 2$ (see Proposition 4.14 and* [5]*, section 4).*

(3) *If, as is conjectured (see* [9]*), the essential dimension $e_{\mathbb{F}_p}(G)$ over $\mathbb{F}_p$ of a cyclic group G of order p^n is equal to n then Conjecture 4.11 holds for G.*

(4) *If we restrict consideration to universal algebras A_0 which are polynomial then the conjecture is true. More generally if $k = \mathbb{F}_p$ then any universal algebra requires at least n k-algebra generators (see* [2]*, Proposition 5.5).*

(5) *The conjecture would certainly be false if k were to contain $\mathbb{F}_p$ strictly. For example if G is elementary Abelian and $|k| \geq p^n$ then we have a universal algebra $A_0 = k[t]$ with $g(t) = t + \theta(g)$ for all $g \in G$ where $\theta : G, . \longrightarrow k, +$ is an injective group homomorphism (see Remark 2.17 and Theorem 5.3 and also* [5]*, Theorem 3.15). Hence $d_k(G) = 1$.*

We will need the following Lemma below and in Section 5:

Lemma 4.13. *The minimal Krull dimension of a trace-surjective k-subalgebra A of $U_k(G)$ is $d_k(G)$. Further A can be taken to be of the form $\theta(U_k(G))$ where $\theta : U_k(G) \longrightarrow U_k(G)$ is a G-equivariant k-algebra homomorphism. In particular $d_k(G) = n$ if and only if every such θ is injective.*

Proof. If θ is not injective then $\theta(U_k(G)) \subset U_k(G)$ is universal of Krull dimension less than n. On the other hand if A is universal of Krull dimension $d < n$ then we have G-equivariant k-algebra homomorphisms $\theta : U_k(G) \longrightarrow A$ and $\phi : A \longrightarrow U_k(G)$. Hence the composition $\phi \circ \theta : U_k(G) \longrightarrow U_k(G)$ is not injective and the Krull dimension of $(\phi \circ \theta)(U_k(G))$ is at most d. The result now follows from Remarks 4.10, (1) and (2). □

We conclude this section with a characterization of the pairs G, k for which $d_k(G) = 1$ thereby confirming the truth of Conjecture 4.11 when $n = 2$:

Proposition 4.14. *The following conditions are equivalent:*

(1) $d_k(G) = 1$,

(2) *The group $(G, .)$ embeds in $(k, +)$,*

(3) *G is elementary Abelian and $|G| \leq |k|$.*

Thus Conjecture 4.11 holds when $n = 2$.

Proof. Clearly conditions (2) and (3) are equivalent and conditions (2), (3) imply condition (1) by Remarks 4.12 (5). Finally if $d_k(G) = 1$ then by Lemma 4.13 there is a trace-surjective k-subalgebra A of $U_k(G)$ with Krull dimension one. Let B be the integral closure of A in the polynomial ring $U_k(G)$. In the same way as in the proof of Proposition 2.18 we see that B is a trace-surjective k-subalgebra of $U_k(G)$ of Krull dimension one. Again by [1], Theorem 1, B is a polynomial k-algebra, $B = k[t]$ (say). The faithful action of G on B is given by $g(t) = \lambda_g t + \mu_g$ where $\lambda_g \in k^*$ and $\mu_g \in k$ for all $g \in G$. Since G is a p-group $\lambda_g = 1$ for all $g \in G$. Therefore the mapping $\psi : (G, .) \longrightarrow (k, +)$, given by putting $\psi(g) = \mu_g$ for all $g \in G$, is an injective group homomorphism and so condition (1) implies condition (2), as required. □

5. A Link between the Conjectures when G is elementary Abelian

Let k be a field of prime characteristic p and let G be an elementary Abelian p-group of order p^n $(n \geq 1)$.

Theorem 5.1. *If G is elementary Abelian of order p^n then $d_k(G) = d_k(F_p(x), n)$.*

Proof. Recall, from Examples 4.3 (3)(a), that if $G =< \sigma_1, \sigma_2, \ldots, \sigma_n >$ is elementary Abelian then $U_k(G) = k[x_1, x_2, \ldots, x_n]$ where each $\sigma_i(x_j) = x_j + \delta_{ij}$ and $U_k(G)^G = k[x_1 - x_1^p, x_2 - x_2^p, \ldots, x_n - x_n^p]$. Now let $\theta : U_k(G) \longrightarrow U_k(G)$ be a G-equivariant k-algebra homomorphism. Then each $\theta(x_i) = x_i + P_i(x_1 - x_1^p, x_2 - x_2^p, \ldots, x_n - x_n^p) \in x_i + U_k(G)^G$ (and conversely). Consider the inclusion of $k[x_1, x_2, \ldots, x_n]$ in $k[[X_1, X_2, \ldots, X_n]]$ where each $x_i = F_p(X_i)$ and so $x_i - x_i^p = X_i$. Then each $\theta(x_i) = F_p(X_i) + P_i(X_1, X_2, \ldots, X_n)$. The result now follows directly from Definition 2.1 and the proof of Lemma 4.13. □

Corollary 5.2. *If G is elementary Abelian then Conjecture 2.16 implies Conjecture 4.11.*

Corollary 5.3 (Link)**.** *If G is elementary Abelian then the power series $F_p(x) = \sum_{r=0}^{\infty} x^{p^r}$ is n-transcendental over k if and only if $d_k(G) = n$. In this case $F_{p^s}(x)$ is also n-transcendental over k for all $s \geq 1$ (see Remark 2.14 (2)).*

We conclude by showing that if $k = \mathbb{F}_p$ then $F_p(x)$ is at least n-transcendental over k in respect of "polynomial perturbations" which either are all affine or all have zero affine parts! This is perhaps the most striking evidence we have at present in support of Conjecture 4.11 when G is elementary Abelian. First we need a curious lemma from linear algebra:

Lemma 5.4. *Let A, B be $n \times n$ matrices with entries in the field k. Suppose that $B - A$ is invertible so that the augmented matrix $[A|B]$ has rank n. Then A can be transformed into an invertible matrix by a sequence of elementary row operations on $[A|B]$ and interchanges of corresponding rows of "A" and "B" (the latter type of operation is only employed if and when a row of "A" is zero).*

Proof. First note that the allowable transformations of $[A|B]$ maintain the invertibility of $B - A$ and hence the full rank of $[A|B]$. We will say that a row of A is "safe" if the corresponding row of B is zero and such rows will be left alone. Clearly the safe rows of A are linearly independent. If all the rows of A are safe then B is zero and A is invertible. It is therefore enough to show that if A is not invertible then we can increase the number of safe rows of A. Choose a non-safe row of A which is a linear combination of the other rows of A. Reduce it to zero by elementary row operations on $[A|B]$ and then interchange it with the corresponding row of B to create an extra safe row of A, as required. □

Theorem 5.5. *Let $X_i = F_p(x_i) + P_i(x_1, x_2, \ldots, x_n) \in \mathbb{F}_p[[x_1, x_2, \ldots, x_n]]$ where $P_i(x_1, x_2, \ldots, x_n) \in R = \mathbb{F}_p[x_1, x_2, \ldots, x_n]$ for $1 \leq i \leq n$. Suppose that either (1) all the $P_i(x_1, x_2, \ldots, x_n)$ have degree at most one or (2) all the $P_i(x_1, x_2, \ldots, x_n)$ have no non-zero terms of degree one. Then $X_1, X_2, \ldots, X_n$ are algebraically independent over $\mathbb{F}_p$.*

Proof. Without loss of generality we may clearly suppose that all the polynomials $P_i(x_1, x_2, \ldots, x_n)$ have zero constant term. Case (2) of the theorem follows directly from Lemma 2.5. We now consider case (1). Clearly the X_i $(1 \leq i \leq n)$ are algebraically independent over $\mathbb{F}_p$ if and only if the $Y_i = x_i + P_i(x_1 - x_1^p, x_2 - x_2^p, \ldots, x_n - x_n^p) = x_i + \sum_{j=1}^n a_{ij}x_j - \sum_{j=1}^n a_{ij}x_j^p \in R$ (say) are algebraically independent over $\mathbb{F}_p$ (see Corollary 3.4). Put $A = (a_{ij})$, an $n \times n$ matrix with entries in $\mathbb{F}_p$. We apply Lemma 5.4 to the augmented matrix $[A + I|A]$ to obtain $[C|D]$ with $C = (c_{ij})$ invertible and $D = (d_{ij})$. Note that the row operations in Lemma 5.4 correspond to taking linear combinations of the Y_i and the interchanges correspond to taking p-th roots. Hence, putting $Z_i = \sum_{j=1}^n c_{ij}x_j - \sum_{j=1}^n d_{ij}x_j^p \in R$ $(1 \leq i \leq n)$, we have that $S = \mathbb{F}_p[Z_1, Z_2, \ldots, Z_n]$ is a purely inseparable extension of $T = \mathbb{F}_p[Y_1, Y_2, \ldots, Y_n]$. Now the Jacobian determinant of the Z_i $(1 \leq i \leq n)$ is equal to $\det(C) \neq 0$. Hence, by Lemma 2.5, the Z_i, and therefore also the Y_i, are algebraically independent over $\mathbb{F}_p$, as required. □

References

[1] P. Eakin, *A note on finite dimensional subrings of polynomial rings*, Proc. Amer. Math. Soc. 31 (1972) 75 - 80.

[2] P. Fleischmann and C.F. Woodcock, *Non-linear group actions with polynomial invariant rings and a structure theorem for modular Galois extensions*, Proc. LMS, 103 (5) (2011) 826 - 846.

[3] P. Fleischmann and C.F. Woodcock, *Universal Galois algebras and cohomology of p-groups*, Journal of Pure and Applied Algebra 217 (3) (2013) 530 - 545.

[4] P. Fleischmann and C.F. Woodcock, *Galois ring extensions and localized modular rings of invariants of p-groups*, Transformation Groups 18 (1) (2013) 131 - 147.

[5] P. Fleischmann and C.F.Woodcock, *Free actions of p-groups on affine varieties in characteristic p*, Math. Proc. Camb. Phil. Soc., https://doi.org/10.1017/S0305004117000317 (Published online: 04 April 2017)

[6] N. Gupta, *On the cancellation problem for the affine space* $\mathbb{A}^3$ *in characteristic p*, Invent. Math. 195 (2014) 279 - 288.

[7] M.-C. Kang, *Essential dimensions of finite groups*, https://arxiv.org/abs/math/0611673, 2006, pp. 1 - 24.

[8] S. Lang, *Cyclotomic Fields*, Springer-Verlag New York 1978.

[9] A. Ledet, *On the essential dimension of p-groups*, Galois Theory and Modular Forms (eds. K. Hashimoto, K. Miyake, H. Nakamura), Springer Science & Business Media (2013) 159 - 172.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, editor G.-C. Rota, Addison-Wesley Reading 1983.

[11] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, Cambridge, 1986.

[12] J. Mittmann, N. Saxena and P. Scheiblechner, *Algebraic independence in positive characteristic: a p-adic calculus*, Trans. Amer. Math. Soc. 366 (7) (2014) 3425 - 3450.

[13] H. Sharif and C.F. Woodcock, *Algebraic functions over a field of positive characteristic and Hadamard products*, J. London Math. Soc. (2) 37 (1988) 395 - 403.

School of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury CT2 7FS, United Kingdom.

E-mail address: P.Fleischmann@kent.ac.uk

E-mail address: C.F.Woodcock@kent.ac.uk