Algebra & Number Theory

Volume 20
2026
No. 8

Transcendence properties of the Artin–Hasse exponential modulo p

Joe Kramer-Miller

msp

msp

ALGEBRA AND NUMBER THEORY 20:8 (2026)
https://doi.org/10.2140/ant.2026.20.1597

Transcendence properties of the Artin–Hasse exponential modulo p

Joe Kramer-Miller

Let $E_p(x)$ denote the Artin–Hasse exponential and $\bar{E}_p(x)$ denote its reduction modulo p in $\mathbb{F}_p[\![x]\!]$. We study transcendence properties of $\bar{E}_p(x)$ over $\mathbb{F}_p[x]$. We give two proofs that $\bar{E}_p(x)$ is transcendental, affirmatively answering a question of Thakur. We also prove algebraic independence results: (i) for $f_1, \dots, f_r \in x\bar{\mathbb{F}}_p[x]$ satisfying certain linear independence properties, we show that the $\bar{E}_p(f_1), \dots, \bar{E}_p(f_r)$ are algebraically independent over $\mathbb{F}_p[x]$; and (ii) we determine the algebraic relations between the $\bar{E}_p(\xi x)$ for $\xi \in \mathbb{F}_p^\times$. Our proof studies the higher derivatives of $\bar{E}_p(x)$ and makes use of iterative differential Galois theory.

1. Introduction

The Artin–Hasse exponential is defined by

$$E_p(x) := \exp\left(\sum_{n=0}^{\infty} \frac{x^{p^n}}{p^n}\right)$$

and is known to have coefficients in $\mathbb{Z}_{(p)}$. This series plays an enormous role in p-adic analysis, showing up in the construction of Witt vectors (see, e.g., [Dieudonné 1957]) and the p-adic approach to exponential sums (see, e.g., [Adolphson and Sperber 1989; Wan 1993]). From the relation $E_p(x^p)/E_p(x)^p = \exp(-xp)$, it is immediate that $E_p(x)$ is a transcendental function over $\mathbb{C}(x)$. However, we may also consider the reduction of $E_p(x)$ modulo p, which we denote by $\bar{E}_p(x)$. Then $\bar{E}_p(x)$ is a power series in $\mathbb{F}_p[\![x]\!]$ that in some sense plays the role of the exponential function in characteristic p. For example, one can use $\bar{E}_p(x)$ to translate Witt vector addition into power series multiplication, as explained in [Dieudonné 1957]. Here we investigate the transcendence properties of $\bar{E}_p(x)$. We give two proofs that $\bar{E}_p(x)$ is transcendental over $\mathbb{F}_p(x)$. This answers a question posed by Dinesh Thakur (see, e.g., [Thakur 2020] or the open questions in [Allouche and Shallit 2003, Chapter 12]). We also prove algebraic independence results for the evaluations of $\bar{E}_p(x)$ at different values in $x\bar{\mathbb{F}}_p[x]$.

1.1. *Main results and outline.*

Our first result is the following.

Theorem 1.1. *The series $\bar{E}_p(x)$ is transcendental over $\mathbb{F}_p(x)$.*

We give two proofs of Theorem 1.1. The first proof is given in Section 2. It uses Christol's automatic criterion for algebraicity of power series together with a functional equation: for $\xi \in \mathbb{F}_p^\times$, we have

MSC2020: 11B85, 11J91.

Keywords: transcendence in positive characteristic, differential Galois theory.

© 2026 The Author, under license to MSP (Mathematical Sciences Publishers). Distributed under the Creative Commons Attribution License 4.0 (CC BY). Open Access made possible by subscribing institutions via Subscribe to Open.

$\bar{E}_p(\xi x) = \bar{E}_p(x)^{[\xi]}$, where $[\xi]$ denotes the Teichmüller lift of ξ (i.e., $[\xi]$ is the unique $p-1$-st root of unity whose reduction modulo p is ξ). This proof is relatively elementary and short, but has the disadvantage of requiring p to be at least 5. The second proof uses iterative differential Galois theory and iterative Frobenius equations. These are the same methods we use for the stronger algebraic independence results, which we describe in detail below.

To state our first algebraic independence result, we need the following definition.

Definition 1.2. Let $f(x) = \sum c_i x^i \in \bar{\mathbb{F}}_p[x]$. We define the *primitive* part of f to be

$$f^*(x) := \sum_{\substack{i \geq 0 \\ p \nmid i}} c_i^*(f) x^i, \; c_i^*(f) := \sum_{k \geq 0} c_{ip^k}^{1/p^k}.$$

Note that $f^*(x) = 0$ if and only if $f(x) = g(x)^p - g(x)$ for some $g(x) \in \bar{\mathbb{F}}_p[x]$.

Theorem 1.3. *Let $f_1, \dots, f_r \in x\bar{\mathbb{F}}_p[x]$ be nonzero. Assume that one of the following conditions holds*:

(1) *The elements $f_1^*, \dots, f_r^*$ are linearly independent over $\mathbb{F}_p$.*

(2) *The f_i^* are not all zero and no nontrivial power product of the f_i are contained in $\bar{\mathbb{F}}_p(x)^p$. In other words, if $f_1^{n_1} \cdots f_r^{n_r}$ is a p-th power, then $n_1, \dots, n_r \in p\mathbb{Z}$.*

Then $\bar{E}_p(f_1), \dots, \bar{E}_p(f_r)$ are algebraically independent.

Example 1.4. For $f(x) = x^k$ with $p \neq k$, we have $f^*(x) = f(x)$. In particular, we see that the elements of $\{\bar{E}_p(x^k)\}_{k \geq 1, \, p \nmid n}$ are algebraically independent using the first condition of Theorem 1.3. It is also clear that the second condition of Theorem 1.3 does not apply, as for any k_1, k_2 coprime to p we can find n_1, n_2 coprime to p so that $p \mid (n_1 k_1 + n_2 k_2)$. In particular $(x^{k_1})^{n_1} \cdot (x^{k_2})^{n_2} \in \bar{\mathbb{F}}_p(x)^p$, but $n_1, n_2 \notin p\mathbb{Z}$.

Example 1.5. Let $f_1, \dots, f_r \in x\bar{\mathbb{F}}_p[x]$ be nonzero. Assume that there exists $c_1, \dots, c_r \in \bar{\mathbb{F}}_p$ such that $f_i(c_i) = 0$ and $f_i(c_j) \neq 0$ for $i \neq j$. We furthermore assume that the zero of f_i at c_i is simple. Then, for integers $n_1, \dots, n_r$ with $p \nmid n_i$, the order of $f_1^{n_1} \cdots f_r^{n_r}$ at c_i is coprime to p. In particular, the product $f_1^{n_1} \cdots f_r^{n_r}$ cannot be in $\bar{\mathbb{F}}_p(x)^p$. Thus, the second condition of Theorem 1.3 is satisfied. On the other hand, it is clear that the first condition of Theorem 1.3 can fail. For example, take $c_1, \dots, c_r$ to be distinct elements of $\mathbb{F}_p$ and set $f_i = x(x - c_i)$. Assume that $p \geq 3$ and $r \geq 3$. Then $f_i^* = f_i$ and the $f_1^*, \dots, f_r^*$ are linearly dependent over $\mathbb{F}_p$.

Example 1.6. Consider the case where $f_2 = f_1^p$. Then $\bar{E}_p(f_1)$ and $\bar{E}_p(f_2)$ are algebraically dependent, as $\bar{E}_p(f_2) = \bar{E}_p(f_1)^p$. We know $f_2 \in \bar{\mathbb{F}}_p(x)^p$, so the second condition of Theorem 1.3 fails. It is also easy to verify that $f_2^* = f_1^*$, so the first condition of Theorem 1.3 fails.

Our second algebraic independence result is the following.

Theorem 1.7. *We have*

$$\operatorname{tr.deg}_{\mathbb{F}_p(x)} \mathbb{F}_p(x)(\bar{E}_p(\xi x))_{\xi \in \mathbb{F}_p^\times} = \phi(p-1),$$

where ϕ is the Euler totient function.

The proofs of Theorems 1.3 and 1.7 follow the same strategy. This strategy can be broken into three steps, which we outline below. For simplicity, we restrict our attention to the case where the f_i in Theorem 1.3 have coefficients in $\mathbb{F}_p$.

Iterated Frobenius equations. Let σ be the lifted Frobenius endomorphism of $\mathbb{Z}_p[\![x]\!]$ that fixes $\mathbb{Z}_p$ and sends x to x^p. For $f \in x\mathbb{Z}_p[\![x]\!]$, we define $\tau(f)$ to be the unique solution to $y^\sigma - y = f$ in $x\mathbb{Z}_p[\![x]\!]$ (explicitly, $\tau(f) = \sum_{n\geq 0} f^{\sigma^n}$). Let $b_1, \ldots, b_k$ be positive integers coprime to p and consider the power series defined by

$$y_1 = \tau(x^{b_1}), \quad y_2 = \tau(x^{b_2} y_1), \quad \ldots, \quad y_k = \tau(x^{b_k} y_{k-1}).$$

We refer to y_k as an iterated Frobenius solution (abbreviated IF-solution) of depth k. This terminology is justified by observing that the y_i satisfy the iterated Frobenius equations

$$y_1^\sigma - y_1 = x^{b_1}, \quad y_2^\sigma - y_2 = x^{b_2} y_1, \quad \ldots, \quad y_k^\sigma - y_k = x^{b_k} y_{k-1}.$$

Let M_k denote the $\mathbb{Z}_p(x)$-module generated by all IF-solutions of depth at most k and let $M = \bigcup M_k$. In Section 3, we study M_k and M. More precisely, we do the following:

(1) We prove that the IF-solutions freely generate M_k (i.e., there are no relations over $\mathbb{Z}_p(x)$ between different IF-solutions).

(2) We show that M is closed under multiplication and $M_{k_1} M_{k_2} \subset M_{k_1+k_2}$. Furthermore, we study the multiplication law in terms of the IF-solutions.

Higher derivatives. Let $\partial^{(k)}$ denote the differential operator $\frac{1}{k!} d^k/d^k x$ and let $\mathrm{dLog}^{(k)}$ be the operator sending f to $\partial^{(k)}(f)/f$. We regard $\partial^{(k)}$ and $\mathrm{dLog}^{(k)}$ as operators on $\mathbb{F}_p[\![x]\!]$ and on $\mathbb{Z}_p[\![x]\!]$. Note that, if f is contained in a finite separable extension L of $\mathbb{F}_p(x)$, then so is $\mathrm{dLog}^{(k)}(f)$ for all $k \geq 0$. This gives a differential transcendence criterion: if the $\mathrm{dLog}^{(k)}(f)$ generate an infinite extension of $\mathbb{F}_p(x)$, then f is transcendental over $\mathbb{F}_p(x)$. In Section 4, we study the iterated differential equations satisfied by $\bar{E}_p(x)$ and power products of the $\bar{E}_p(f_r)$. Define $\overline{M}_k$ to be M_k/pM_k. We prove that $\mathrm{dLog}^{(k)}(\bar{E}_p(x))$ is contained in $\overline{M}_k$, but not in $\overline{M}_{k-1}$. For example, when $k = 1$, a quick calculation shows that $\frac{d}{dx} E_p(x) = \frac{y}{x} E_p(x)$, where $y = \tau(x)$. More precisely, we determine $\mathrm{dLog}^{(k)}(\bar{E}_p(x))$ modulo $\overline{M}_{k-1}$. This is enough to show $\bar{E}_p(x)$ is transcendental. Next, using standard properties of higher derivatives and results from Section 3, we are able to determine $\mathrm{dLog}^{(k)}(\bar{E}_p(f_1)^{n_1} \cdots \bar{E}_p(f_r)^{n_r})$ modulo $\overline{M}_{k-1}$, where $n_i \in \mathbb{Z}$ and $f_i \in \mathbb{F}_p[x]$.

Iterative differential Galois groups. Let K be the algebraic closure of $\mathbb{F}_p(x)$ in $\bar{\mathbb{F}}_p((x))$. An ID-module over K is a vector space over K with compatible actions of $\partial^{(k)}$. For any $f \in x\mathbb{F}_p[x]$, we let N_f denote the ID-module associated to the differential equation satisfied by $\bar{E}_p(f)$ (see Section 5.1 for a precise description of this ID-module). Following Matzat and van der Put [2003], we may define an ID-Galois group $\mathrm{Gal}(N_f)$. Then $\mathrm{Gal}(N_f)$ is a closed subgroup of the multiplicative group $\mathbb{G}_m$ over $\bar{\mathbb{F}}_p$ and is equal to all of $\mathbb{G}_m$ precisely when $\bar{E}_p(f)$ is transcendental over $\mathbb{F}_p(x)$. More generally, the algebraic independence of $\bar{E}_p(f_1), \ldots, \bar{E}_p(f_r)$ is equivalent to the ID-Galois group $\mathrm{Gal}(N_{f_1} \oplus \cdots \oplus N_{f_r})$ being isomorphic to $\mathbb{G}_m^r$. Using the Tannakian interpretation of ID-Galois groups, it is enough to

prove $\overline{E}_p(f_1)^{n_1} \cdots \overline{E}_p(f_r)^{n_r}$ is transcendental for any $n_i \in \mathbb{Z}$. This is essentially a version of Kolchin's theorem [1968] for iterated differential equations. We then address this transcendence question assuming the hypotheses of Theorems 1.7 and 1.3 using the results from Section 4.

Remark 1.8. The appearance of differential Galois theory naturally places Theorem 1.3 in a rich historical context. Ostrowski [1946] gives a simple algebraic independence criterion for integrals of elements of a differential field K of meromorphic functions. This was extended to include exponentials of elements of a differential field (as well as further results) by Kolchin [1968]. The use of algebraic groups and differential Galois theory has since played an outstanding role in the transcendence theory of functions. To the best of our knowledge, this paper is the first application of differential Galois theory to transcendence in positive characteristic. However, we mention that the use of Tannakian theory for Frobenius equations has played an exceptional role in function field arithmetic. This was pioneered by Papanikolas [2008] and lays the framework for studying transcendence of periods of Drinfeld modules and t-motives.

1.2. ***Further questions.*** It would be interesting to completely determine the algebraic relations between values $\overline{E}_p(f)$ for $f \in x\overline{\mathbb{F}}_p[x]$. More generally, it would be interesting to determine the algebraic relations between values of $\overline{E}_p(x)$ at any algebraic power series. At the moment it is even unclear to the author what the algebraic relations are between the $\overline{E}_p(\xi x)$ where ξ ranges over $\overline{\mathbb{F}}_p$. The reader may observe the influence of Ax's work [1971] on Schanuel's conjecture on the final steps of the proof of Theorem 1.3. Thus, it is natural to ask if an analogue of Ax–Schanuel holds for the Artin–Hasse exponential.

2. An automatic approach to the transcendence of $\overline{E}_p(x)$

In this section we give a short proof of the transcendence of $\overline{E}_p(x)$ using the functional equation satisfied by $\overline{E}_p(x)$ and automatic methods.

2.1. ***A transcendental criterion.*** We recall Christol's well-known automatic criterion for algebraicity of series in $\mathbb{F}_p[\![x]\!]$. See [Christol 1979] or [Christol et al. 1980] for proofs.

Theorem 2.1. *Let $f = \sum f_n x^n \in \mathbb{F}_p[\![x]\!]$. The following are equivalent*:

(1) *The series f is algebraic over $\mathbb{F}_p[x]$.*

(2) *There is a p-automaton that gives output f_n on input n.*

(3) *There are only finitely many subsequences of $(f_n)_{n\geq 0}$ of the form $(f_{p^k n+r})_{n\geq 0}$, where k is positive and r is in the range $0 \leq r < p^k$.*

This allows us to establish the following transcendence criterion.

Lemma 2.2. *Let $\lambda \in \mathbb{Z}_p$. Let $f \in 1 + x\mathbb{F}_p[\![x]\!]$ be algebraic over $\mathbb{F}_p[x]$. Then $f^\lambda \in \mathbb{F}_p[\![x]\!]$ is algebraic over $\mathbb{F}_p[x]$ if and only if λ is rational.*

Proof. This is a special case of [Allouche et al. 1988]. We give a proof in the interest of having a quick and self-contained automatic proof that $\overline{E}_p(x)$ is transcendental. We easily reduce to the case where $f = 1 + x$. If λ is rational, it is clear that $(1 + x)^\lambda$ is algebraic. For the other direction, assume λ is

irrational. Write $\lambda = \sum_{n=0}^{\infty} a_n p^n$. For $1 \le c \le p-1$, we define sets

$$S_c := \{n \mid a_n = c\} \quad \text{and} \quad S_c^k := S_c \cap \mathbb{Z}_{>k}.$$

We then set $\lambda_c = \sum_{n \in S_c} a_n p^n$. If λ_c is nonzero and rational, we may replace λ with $\lambda - \lambda_c$. In particular, we may assume each λ_c is either zero or irrational. Let c_0 be the largest number such that $\lambda_{c_0} \neq 0$. As λ_{c_0} is irrational, for each $k, m > 0$ we have

$$m + S_{c_0}^k \neq S_{c_0}^{k+m}, \tag{1}$$

as otherwise the digits of λ_{c_0} would eventually be periodic.

Next, write $(1+x)^\lambda = \sum b_n x^n$. By using the product expansion $(1+x)^\lambda = \prod (1+x^{p^n})^{a_n}$, we see that

$$b_{c_0 p^k} = \begin{cases} 1 & \text{if } k \in S_{c_0}, \\ 0 & \text{otherwise.} \end{cases}$$

Consider the sequences $B_k = (b_{np^k})_{n \ge 1}$. By Theorem 2.1, if we prove that the B_k are all distinct, we will know $(1+x)^\lambda$ is transcendental. Note that the $c_0 p^n$-th element in B_k is 1 if $n + k \in S_{c_0}^k$ and zero otherwise. In particular, if $B_k = B_{k+m}$, then we must have $m + S_{c_0}^k = S_{c_0}^{k+m}$. However, by (1) we know this can never happen, which proves the lemma. □

2.2. *A short proof of the transcendence of $\bar{E}_p(x)$.* The first step is to prove that $\bar{E}_p(x)$ satisfies a functional equation.

Lemma 2.3. *For $\xi \in \mathbb{F}_p^\times$, we have $\bar{E}_p(\xi x) = \bar{E}_p(x)^{[\xi]}$, where $[\xi] \in \mathbb{Z}_p$ denotes the Teichmüller lift of ξ (i.e., $[\xi]$ is the unique $p-1$-st root of unity in $\mathbb{Z}_p$ that reduces to ξ modulo p).*

Proof. For $f_0 \in \mathbb{Q}_p[\![x]\!]$ and $f_1, \ldots, f_n \in x\mathbb{Q}_p[\![x]\!]$, we may take the composition $f_0 \circ \cdots \circ f_n \in \mathbb{Q}_p[\![x]\!]$, and this operation is associative. For $c \in \mathbb{Z}_p$ we define

$$g(x) = \sum_{n=0}^{\infty} \frac{x^{p^n}}{p^n}, \quad L_c(x) = cx \quad \text{and} \quad P_c(x) = (1+x)^c = \sum_{n=0}^{\infty} \binom{c}{n} x^n.$$

Note that $E_p(x) = \exp \circ g$. Also, for $\xi \in \mathbb{F}_p^\times$, we have the relations

$$g \circ L_{[\xi]} = L_{[\xi]} \circ g \quad \text{and} \quad \exp \circ L_{[\xi]} = P_{[\xi]} \circ (\exp(x) - 1).$$

The first relation comes from the fact that $[\xi]^p = [\xi]$. Thus, we compute

$$E_p([\xi]x) = \exp \circ g \circ L_{[\xi]} = \exp \circ L_{[\xi]} \circ g = P_{[\xi]} \circ (\exp(x) - 1) \circ g = P_{[\xi]} \circ (E_p(x) - 1) = E_p(x)^{[\xi]}.$$

The lemma follows by reducing modulo p. □

Theorem 2.4. *The series $\bar{E}_p(x)$ is transcendental over $\mathbb{F}_p(x)$ if $p \ge 5$.*

Proof. Take $\xi \in \mathbb{F}_p^\times$. Since $p \ge 5$, we can pick ξ to not be 1 or -1. This means $[\xi]$ is an algebraic integer that is not an integer. Thus, $[\xi]$ is irrational. Assume $\bar{E}_p(x)$ is algebraic. This implies $\bar{E}_p(\xi x)$ is algebraic. Thus, by Lemma 2.3, $\bar{E}_p(x)^{[\xi]}$ is algebraic. However, $[\xi]$ is not rational, so Lemma 2.2 tells us that $\bar{E}_p(x)^{[\xi]}$ is transcendental. This is a contradiction. □

Remark 2.5. One can get algebraic independence results using the full result of [Allouche et al. 1988]. In particular, the argument above can be extended to show $\mathrm{tr.deg}_{\mathbb{F}_p(x)}(\overline{E}_p(\xi x))_{\xi\in\mathbb{F}_p^\times} \geq \phi(p-1)-1$. As we prove in Section 5 that $\mathrm{tr.deg}_{\mathbb{F}_p(x)}(\overline{E}_p(\xi x))_{\xi\in\mathbb{F}_p^\times} = \phi(p-1)$, we omit the proof of this weaker result.

3. Solutions to iterated Frobenius equations

Let $\mathbb{F}_q$ be the field with $q = p^f$ elements and fix $\zeta \in \mathbb{F}_q$ such that $\zeta, \zeta^p, \dots, \zeta^{p^{f-1}}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Let $\mathbb{Z}_q$ denote the p-typical Witt vectors of $\mathbb{F}_q$. By abuse of notation, we regard ζ as an element of $\mathbb{Z}_q$ by identifying ζ^{p^j} with its Teichmüller lift. It will be convenient to define $x_j^i = \zeta^{p^j} x^i$ for $i \geq 1$ and any $j \in \mathbb{Z}$. We also define the set

$$X := \{x_j^i \mid 1 \leq j \leq f,\ i \geq 1,\ p\nmid i\}.$$

3.1. ***Iterated Frobenius equations.*** Let $\sigma : \mathbb{Z}_q((x)) \to \mathbb{Z}_q((x))$ denote the $\mathbb{Z}_p$-linear endomorphism sending x to x^p and acting as the Frobenius endomorphism on $\mathbb{Z}_q$. Let $f \in x\mathbb{Z}_q[\![x]\!]$. We define $\tau(f)$ to be the unique solution to $y^\sigma - y = f$ in $x\mathbb{Z}_q[\![x]\!]$. Concretely, we have

$$\tau(f) = \sum_{n=0}^{\infty} f^{\sigma^n}.$$

We regard τ as a $\mathbb{Z}_p$-linear map. Note that τ satisfies the two fundamental equations

$$\tau(f)\tau(g) = \tau(f\tau(g)) + \tau(g\tau(f)) - \tau(fg), \tag{2}$$

$$\tau(f^\sigma \tau(g)) = \tau(f\tau(g)) + \tau(f^\sigma g) - f\tau(g). \tag{3}$$

Definition 3.1. Let $[k]$ denote the set $\{1, \dots, k\}$ and let $[0]$ denote the empty set. An *iterated Frobenius datum* b (abbreviated as IF-datum) of depth k is a function

$$b : [k] \to X.$$

We denote the depth of b by $\mathrm{dep}(b)$. We remark that there is exactly one IF-datum of depth 0. We define D to be the set of all IF-data.

Definition 3.2. We let b^{tr} denote the restriction of b to $[k-1]$ (we think of b as a list of elements and b^{tr} as the truncation of the last element, whence the "tr" in the superscript). Also, for any $z \in X$, we let $\mathrm{cat}(b, z)$ be the IF-datum of depth $k+1$ defined by

$$\mathrm{cat}(b,z)(i) \begin{cases} b(i) & \text{if } i \in [k], \\ z & \text{if } i = k+1. \end{cases}$$

Definition 3.3. Let b be an IF-datum of depth k. We recursively define $w_b \in x\mathbb{Z}_q[\![x]\!]$ as

$$w_b = \begin{cases} 1 & \text{if } \mathrm{dep}(b) = 0, \\ \tau(b(k) w_{b^{\mathrm{tr}}}) & \text{if } \mathrm{dep}(b) = k > 0. \end{cases}$$

We refer to w_b as an iterative Frobenius solution (abbreviated as IF-solution).

Remark 3.4. Let b be an IF-datum of depth k. For $i \in [k]$, let b_i denote the IF-datum obtained by restricting b to $[i]$. Consider the iterated Frobenius equation

$$y_1^\sigma - y_1 = b(1), \quad y_2^\sigma - y_2 = b(2)y_1, \quad \ldots, \quad y_k^\sigma - y_k = b(k)y_{k-1}.$$

Note that we obtain a solution to this equation by setting $y_i = w_{b_i}$. This justifies the terminology "IF-solution".

3.2. ***Spaces generated by* IF-*solutions.*** We define

$$M_k := \left\{ \sum_{\substack{b \in D \\ \mathrm{dep}(b) \le k}} a_b w_b \;\middle|\; a_b \in \mathbb{Z}_q(x) \right\}, \quad \widehat{M}_k := p\text{-adic completion of } M_k \text{ in } \mathbb{Z}_q[\![x]\!]\langle x^{-1}\rangle,$$

$$A_k := \left\{ \sum_{\substack{b \in D \\ \mathrm{dep}(b) \le k}} a_b w_b \;\middle|\; a_b \in \mathbb{Z}_q[x] \right\}.$$

Here $\mathbb{Z}_q[\![x]\!]\langle x^{-1}\rangle$ denotes the p-adic completion of $\mathbb{Z}_q[\![x]\!][x^{-1}]$.

Lemma 3.5. *For $k \ge 0$, we have $\tau(xA_k) \subset A_{k+1}$. In particular, for any $z \in x\mathbb{Z}_q[x]$, we have $\tau(zA_k) \subset A_{k+1}$.*

Proof. We proceed by induction on k. For $k = 0$, we are reduced to showing $\tau(x_j^i) \in A_1$. Write $i = p^t h$, where h is coprime to p. Then

$$\tau(x_j^i) = \tau(x_{j-t}^h) - \sum_{m=1}^{t} x_{j-m}^{p^{t-m}h},$$

so $\tau(x_j^i) \in A_1$. For $k > 0$, it suffices to show $\tau(x_j^i w_b) \in A_{k+1}$ for any IF-datum b of depth k. Again we write $i = p^t h$. By repeatedly using (3), we obtain

$$\tau(x_j^i w_b) = \tau(x_{j-t}^h w_b) + \sum_{m=1}^{t} \tau(x_{j-m}^{p^{t-m}h} b(k) w_{b^{\mathrm{tr}}}) - \sum_{m=1}^{t} x_{j-m}^{p^{t-m}h} w_b.$$

Note that $\tau(x_{j-t}^h w_b)$ is an IF-solution of degree $k+1$, so it is contained in A_{k+1}. The second summation is clearly contained in A_k. Finally, by our inductive hypothesis, $\tau(x_{j-m}^{p^{t-m}h} b(k) w_{b^{\mathrm{tr}}})$ is contained in A_k. □

Lemma 3.6. *We have $\sigma(M_k) \subset M_k$ and $\sigma(\widehat{M}_k) \subset \widehat{M}_k$.*

Proof. Let b be an IF-datum of depth k. We have $w_b^\sigma = w_b + b(k) w_{b^{\mathrm{tr}}}$, which is in M_k. Thus, $\sigma(M_k) \subset M_k$. We see $\sigma(\widehat{M}_k) \subset \widehat{M}_k$ by taking p-adic limits. □

Lemma 3.7.

$$\frac{d}{dx}\widehat{M}_k \subset \widehat{M}_k.$$

Proof. We induct on k. When $k = 0$, the statement is immediate, since $\widehat{M}_0$ is the ring $\mathbb{Z}_q\langle x, x^{-1}\rangle$, which is preserved by $\frac{d}{dx}$. Let $k > 0$ and assume the lemma holds for $k-1$. From the definitions and the Leibnitz rule, we reduce to showing $\frac{d}{dx} w_b \in \widehat{M}_k$ whenever $\mathrm{dep}(b) = k$. Applying $\frac{d}{dx}$ to the equation $w_b^\sigma - w_b = b(k) w_{b^{\mathrm{tr}}}$ and using the chain rule gives

$$px^{p-1}(w_b')^\sigma + w_b' = b(k)' w_{b^{\mathrm{tr}}} + b(k) w_{b^{\mathrm{tr}}}'.$$

We deduce that

$$w_b' = \sum_{n=0}^{\infty} p^n x^{p^{n+1}-1} (b(k)' w_{b^{\mathrm{tr}}} + b(k) w_{b^{\mathrm{tr}}}')^{\sigma^n}. \tag{4}$$

By our inductive hypothesis, we know $w_{b^{\mathrm{tr}}}' \in \widehat{M}_{k-1}$. Then, from Lemma 3.6, we see that each summand in (4) is in $\widehat{M}_{k-1}$. As the terms in the sum converge p-adically, the lemma follows. □

Remark 3.8. It is not true that $\frac{d}{dx} M_k \subset M_k$. For example, we see that $\frac{d}{dx}\tau(x) = \sum p^i x^{p^i-1}$ is not in M_1. This is the sole reason for introducing the p-adically closed spaces $\widehat{M}_k$.

Lemma 3.9. *For $k_1, k_2 \geq 0$, we have $M_{k_1} M_{k_2} \subset M_{k_1+k_2}$ and $\widehat{M}_{k_1} \widehat{M}_{k_2} \subset \widehat{M}_{k_1+k_2}$.*

Proof. We will show $A_{k_1} A_{k_2} \subset A_{k_1+k_2}$. The lemma will follow by inverting x and taking the p-adic completion. We proceed by induction on $k = k_1 + k_2$. The case $k = 0$ is immediate. Let $k > 0$ and assume the result holds for $k-1$. Let b_i be an IF-datum of degree k_i. Then, using (2), we have

$$w_{b_1} w_{b_2} = \tau(b_1(k_1) w_{b_1^{\mathrm{tr}}} w_{b_2}) + \tau(b_2(k_2) w_{b_2^{\mathrm{tr}}} w_{b_1}) - \tau(b_1(k_1) w_{b_1^{\mathrm{tr}}} b_2(k_2) w_{b_2^{\mathrm{tr}}}).$$

The lemma follows from our inductive hypothesis and Lemma 3.5. □

3.3. IF-*solutions modulo p*. We now study the space of IF-solutions modulo p.

Definition 3.10. Let b be an IF-datum. We define $\overline{w}_b$ to be the reduction of w_b modulo p in $\mathbb{F}_q[\![x]\!]$.

We define the spaces

$$\overline{M}_k := \left\{ \sum_{\substack{b \in D \\ \mathrm{dep}(b) \leq k}} a_b \overline{w}_b \;\middle|\; a_b \in \mathbb{F}_q(x) \right\}, \quad \overline{M} = \bigcup_{n \geq 1} \overline{M}_k.$$

Our main result of this section is the following proposition.

Proposition 3.11. *The elements $\overline{w}_b$, where b ranges over $b \in D$, are linearly independent over $\mathbb{F}_q(x)$. In particular, the set $\{\overline{w}_b\}_{b \in D}$ is a basis of $\overline{M}$ over $\mathbb{F}_q(x)$.*

Proof. It will be useful for us to introduce an ordering on D. We set $b_1 > b_2$ if $\mathrm{dep}(b_1) > \mathrm{dep}(b_2)$ and, for IF-data with the same depth k, we use the lexicographical ordering on $(b(k), \ldots, b(1))$. Consider $c = \{c_b\}_{b \in D}$ with $c_b \in \mathbb{F}_q(x)$, where almost all $c_b = 0$. We define $\max(c)$ to be the largest b such that $c_b \neq 0$. Assume there exists such a c such that

$$\sum_{b \in D} c_b \overline{w}_b = 0. \tag{5}$$

We may further assume that $\max(c)$ is minimal in the sense that, for any other $c' = \{c_b'\}_{b \in D}$ with $\max(c') < \max(c)$, the corresponding sum $\sum c_b' \overline{w}_b$ is nonzero. Set $b_{\max} = \max(c)$ and $k_{\max} = \mathrm{dep}(b_{\max})$. After multiplying (5) with an element of $\mathbb{F}_q(x)$, we may assume $c_{b_{\max}} = 1$.

Let F be the p-th power Frobenius. For $b \in D$ with $\mathrm{dep}(b) = k$, we have

$$(F-1) c_b \overline{w}_b = c_b^p \overline{w}_b^p - c_b \overline{w}_b = (c_b^p - c_b) \overline{w}_b + c_b^p b(k) \overline{w}_{b^{\mathrm{tr}}}.$$

Thus, if we apply $F-1$ to (5), we get

$$\sum_{b\in D} d_b \overline{w}_b = 0,$$

where, for b of depth k,

$$d_b := (c_b^p - c_b) + \sum_{\substack{\beta\in D\\ \beta^{\mathrm{tr}}=b}} c_\beta \beta(k+1).$$

It is clear that $d_{b_{\max}} = 0$ and $\max(d) < \max(c)$. Thus, we are reduced to proving that not all the d_b are zero, as this will contradict our minimality condition on c.

First assume each $c_b \in \mathbb{F}_p$. Then

$$d_{b^{\mathrm{tr}}_{\max}} = \sum_{\substack{b\in D\\ b^{\mathrm{tr}}=b^{\mathrm{tr}}_{\max}}} c_b b(k_{\max}).$$

The terms $b_0(k_{\max})$ are all distinct elements of X. In particular, they are linearly independent over $\mathbb{F}_p$. Not all of the c_b are equal to zero, since we know $c_{b_{\max}} \neq 0$, so we see that $d_{b^{\mathrm{tr}}_{\max}} \neq 0$. Next, assume that not all the c_b are in $\mathbb{F}_p$. Let b_0 be the largest IF-datum such that $c_{b_0} \notin \mathbb{F}_p$ and let $k_0 = \mathrm{dep}(b_0)$. If $d_{b_0} = 0$, we have

$$c_{b_0}^p - c_{b_0} = -\sum_{\substack{\beta\in D\\ \beta^{\mathrm{tr}}=b_0}} c_\beta \beta(k_0+1).$$

The left side of this equation is zero, as $c_{b_0} \notin \mathbb{F}_p$. However, the right side is an $\mathbb{F}_p$-linear combination of terms of the form $x_j^i = \zeta^{p^j} x^i$, where $p \nmid i$. In particular, the right side is a polynomial $f(x) \in \mathbb{F}_q[x]$ whose degree is coprime to p. However, the equation $y^p - y = f(x)$ cannot have a solution in $\mathbb{F}_q(x)$, which gives a contradiction. □

Corollary 3.12. *The space M_k (resp. $\widehat{M}_k$) is freely generated by $\{w_b\}_{\mathrm{dep}(b)\le k}$ over $M_0 = \mathbb{Z}_q(x)$ (resp. $\widehat{M}_0 = \mathbb{Z}_q\langle x, x^{-1}\rangle$).*

Corollary 3.13. *For all $k, m \ge 0$, we have $p^m \mathbb{Z}_q((x)) \cap \widehat{M}_k = p^m \widehat{M}_k$. In particular, let $x, y \in \widehat{M}_{k+1}$. If $p^m x \equiv p^m y \bmod \widehat{M}_k$, then $x \equiv y \bmod \widehat{M}_k$.*

In light of Proposition 3.11, we make the following definitions.

Definition 3.14. Let $f \in \overline{M}$. By Proposition 3.11, we may express f uniquely as a sum $\sum a_b \bar{b}$, where $a_b \in \mathbb{F}_q(x)$ and almost all the a_b are zero. We define the depth of f, written as $\mathrm{dep}(f)$, to be the largest k such that, for some b with $\mathrm{dep}(b) = k$, we have $a_b \neq 0$. Equivalently, the depth of $f \in \overline{M}$ is the unique $k \ge 0$ such that $f \in \overline{M}_k$ and $f \notin \overline{M}_{k-1}$.

Corollary 3.15. *Let $\alpha_1, \alpha_2, \ldots$ be a sequence of elements in $\overline{M}$ with $\mathrm{dep}(\alpha_k) = k$ for each k. Then the α_k are linearly independent over $\mathbb{F}_p(x)$.*

Definition 3.16. Let $\{\dot{w}_b\}_{b\in D}$ be the basis of $\mathrm{Hom}_{\mathbb{F}_p(x)}(\overline{M}, \mathbb{F}_p(x))$ that is dual to $\{\overline{w}_b\}_{b\in D}$. That is, for $b, b' \in D$, $\dot{w}_b(\overline{w}_{b'})$ is one if $b = b'$ and zero otherwise.

3.4. ***Products of* IF-*solutions.*** Let $b_1, \dots, b_r$ be IF-data with $\mathrm{dep}(b_i) = k_i$. Let $k = k_1 + \cdots + k_r$. From Lemma 3.9, we know $w_{b_1} \cdots w_{b_r}$ is in M_k, and thus, by Corollary 3.12, can be uniquely written as a sum $\sum_{\mathrm{dep}(b) \leq k} a_b w_b$ with $a_b \in M_0$. In this subsection, we determine a_b when $\mathrm{dep}(b) = k$. In particular, in Proposition 3.21, we completely determine $w_{b_1} \cdots w_{b_r}$ modulo M_{k-1}.

Definition 3.17. Let $k_1, \dots, k_r \geq 1$ and set $k = k_1 + \cdots + k_r$. We define

$$[k_1, \dots, k_r] := \{(i, j) \mid 1 \leq i \leq r,\ j \in [k_i]\}.$$

A splicing function is a bijection $\eta : [k] \to [k_1, \dots, k_r]$ such that, for any $1 \leq j_1 < j_2 \leq k_i$, we have $\eta^{-1}(i, j_1) < \eta^{-1}(i, j_2)$. We let $C(k_1, \dots, k_r)$ denote the set of all splicing functions. Note that $C(k_1, \dots, k_r)$ has cardinality $\binom{k}{k_1, \dots, k_r}$.

Definition 3.18. Let $b_1, \dots, b_r$ be IF-data with $\mathrm{dep}(b_i) = k_i$. For $\eta \in C(k_1, \dots, k_r)$, we define the splicing of $b_1, \dots, b_r$ according to η to be the IF-datum of depth k defined by the composition

$$b_\eta : [k] \xrightarrow{\eta} [k_1, \dots, k_r] \xrightarrow{(i,j) \mapsto b_i(j)} X.$$

We let $S(b_1, \dots, b_r)$ denote the multiset of all possible splicings of $b_1, \dots, b_r$. That is,

$$S(b_1, \dots, b_r) := \{b_\eta \mid \eta \in C(k_1, \dots, k_r)\}.$$

The next lemma follows immediately from these definitions.

Lemma 3.19. *Let b_i and k_i be as in Definition 3.18. Then*

$$S(b_1, \dots, b_r) = \bigsqcup_{i=1}^{r} \{\mathrm{cat}(b, b_i(k_i)) \mid b \in S(b_1, \dots, b_{i-1}, b_i^{\mathrm{tr}}, b_{i+1}, \dots, b_r)\},$$

where the $\sqcup$ denotes a disjoint union.

Lemma 3.20. *Continuing with the same notation, we define*

$$\mathcal{B}_r := \prod_{i=1}^{r} w_{b_i} \quad \text{and} \quad \mathcal{B}_r^{(j)} := w_{b_j^{\mathrm{tr}}} \prod_{\substack{1 \leq i \leq r \\ i \neq j}} w_{b_i}.$$

Then we have

$$\mathcal{B}_r = \sum_{i=1}^{r} \tau(b_i(k_i)\mathcal{B}_r^{(i)}) \mod M_{k-1}.$$

Proof. We proceed by induction on r, with the base case $r = 1$ being immediate. Let $r > 1$ and assume the lemma holds for $r - 1$. In particular, we have

$$\mathcal{B}_{r-1} \equiv \sum_{i=1}^{r-1} \tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)}) \mod M_{k-k_r-1}. \tag{6}$$

We know $M_{k-k_r-1} M_{k_r} \subset M_{k-1}$ by Lemma 3.9. Thus, multiplying (6) by w_{b_r} gives

$$\mathcal{B}_r \equiv w_{b_r} \sum_{i=1}^{r-1} \tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)}) \mod M_{k-1}. \tag{7}$$

For $1 \le i \le r-1$, we know by (2) that

$$w_{b_r}\tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)}) = \tau\big(b_r(k_r)w_{b_r^{\mathrm{tr}}}\tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)})\big) + \tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)}w_{b_r}) - \tau(b_r(k_r)w_{b_r^{\mathrm{tr}}}b_i(k_i)\mathcal{B}_{r-1}^{(i)}). \quad (8)$$

We know $\mathcal{B}_{r-1}^{(i)} \in M_{k-k_r-1}$ and $w_{b_r^{\mathrm{tr}}} \in M_{k_r-1}$, so that the last term in the right side of (8) is in M_{k-1}. As $\mathcal{B}_{r-1}^{(i)}w_{b_r} = \mathcal{B}_r^{(i)}$, we have

$$w_{b_r}\tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)}) \equiv \tau\big(b_r(k_r)w_{b_r^{\mathrm{tr}}}\tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)})\big) + \tau(b_i(k_i)\mathcal{B}_r^{(i)}) \mod M_{k-1}. \quad (9)$$

Next, by our inductive hypothesis (6) and the linearity of τ, we obtain

$$\sum_{i=1}^{r-1}\tau\big(b_r(k_r)w_{b_r^{\mathrm{tr}}}\tau(b_i(k_i)\mathcal{B}_{r-1}^{(i)})\big) \equiv \tau(b_r(k_r)w_{b_r^{\mathrm{tr}}}\mathcal{B}_{r-1}) \mod M_{k-1}.$$

We can combine this with (9) and (7) to get

$$\mathcal{B}_r \equiv \tau(b_r(k_r)w_{b_r^{\mathrm{tr}}}\mathcal{B}_{r-1}) + \sum_{i=1}^{r-1}\tau(b_i(k_i)\mathcal{B}_r^{(i)}) \mod M_{k-1}.$$

The result follows by observing that $\mathcal{B}_r^{(r)} = w_{b_r^{\mathrm{tr}}}\mathcal{B}_{r-1}$. □

Proposition 3.21. *Continue with the notation from Lemma 3.20. We have*

$$\mathcal{B}_r \equiv \sum_{b\in S(b_1,\dots,b_r)} w_b \mod M_{k-1}.$$

Proof. We induct on r. When $r = 1$, the result is immediate. Let $r > 1$ and assume the result holds for $r-1$. From Lemma 3.20, we know

$$\mathcal{B}_r = \sum_{i=1}^{r}\tau(b_i(k_i)\mathcal{B}_r^{(i)}) \mod M_{k-1}.$$

By our inductive hypothesis, we have

$$\mathcal{B}_r^{(i)} \equiv \sum_{b\in S(b_1,\dots,b_{i-1},b_i^{\mathrm{tr}},b_{i+1},\dots,b_r)} w_c \mod M_{k-2}.$$

The proposition then follows from Lemmas 3.19 and 3.5. □

We will now give some corollaries of Proposition 3.21. First we need a definition.

Definition 3.22. Let $k > 0$ and $z \in X$. Let β_z^k be the IF-datum of depth k such that $\beta_z^k(i) = z$ for each $1 \le i \le k$. We define ω_z^k to be $w_{\beta_z^k}$. We let $\bar{\omega}_z^k$ be the reduction of ω_z^k modulo p and we let $\dot{\omega}_z^k$ be $\dot{w}_{\beta_z^k}$, as defined in Definition 3.16.

We readily compute that

$$\omega_z^k = \sum_{i_k\ge\cdots\ge i_1\ge 0} z^{bp^{i_1+\cdots+i_k}}.$$

The elements ω_z^k and $\bar{\omega}_z^k$ will appear when studying the higher derivatives of the Artin–Hasse exponential. We have the following corollaries of Proposition 3.21.

Corollary 3.23. *Fix $z \in X$. Let $k_1, \dots, k_r \geq 1$ and set $k = k_1 + \cdots + k_r$. Then*

$$\prod_{i=1}^{r} \omega_z^{k_i} \equiv \binom{k}{k_1, \dots, k_r} \omega_z^k \mod M_{k-1}.$$

Proof. This follows from Proposition 3.21 and the fact that there are $\binom{k}{k_1,\dots,k_r}$ splicing functions. □

Corollary 3.24. *For $z \in X$, we have $\tau(z)^k \equiv k!\omega_z^k \bmod M_{k-1}$.*

Corollary 3.25. *Let $b_1, \dots, b_r \in D$, let $k_i = \deg(b_i)$, and set $k = k_1 + \cdots + k_r$. Then, for any $z \in X$, we have*

$$\dot{\omega}_z^k(\overline{w}_{b_1} \cdots \overline{w}_{b_r}) = \begin{cases} \binom{k}{k_1,\dots,k_r} & \text{if each } \overline{w}_{b_i} = \bar{\omega}_z^{k_i}, \\ 0 & \text{otherwise.} \end{cases}$$

4. Higher derivatives and the Artin–Hasse exponential

4.1. ***Higher derivatives and a transcendental criterion.*** We define the *higher derivatives* on $\mathbb{F}_q((x))$ and $\mathbb{Z}_q((x))$,

$$\partial^{(k)} := \frac{1}{k!}\frac{d^k}{d^k x}.$$

We define the *higher logarithmic derivatives* of $f \in \mathbb{F}_q((x))$ or $f \in \mathbb{Z}_q((x))$ by

$$\mathrm{dLog}^{(k)}(f) := \frac{\partial^{(k)}(f)}{f}.$$

Note that $\partial^{(k)}$ and $\mathrm{dLog}^{(k)}$ restrict to maps on $\mathbb{F}_q(x)$. Furthermore, if K is a finite separable extension of $\mathbb{F}_q(x)$, then each $\partial^{(k)}$ and $\mathrm{dLog}^{(k)}$ extends uniquely to K by a theorem of Schmidt (see [Matzat and van der Put 2003, Section 2]). We begin with the following general transcendence result.

Theorem 4.1. *Let $\alpha_1, \alpha_2, \dots$ be a sequence of power series in $\mathbb{F}_q[\![x]\!]$. Let $f(x) \in \mathbb{F}_q[\![x]\!]$ be a power series satisfying the iterative differential equation*

$$\mathrm{dLog}^{(k)}(f) = \alpha_k \quad \text{for all } k \geq 1.$$

If $\mathbb{F}_q(x)(\alpha_1, \alpha_2, \dots)$ is an infinite extension of $\mathbb{F}_q(x)$, then $f(x)$ is transcendental over $\mathbb{F}_q(x)$.

Proof. Assume $f(x)$ is algebraic (necessarily separable) and contained in a field K. As $\mathrm{dLog}^{(k)}$ extends to K, we see that α_n is contained in K as well. This contradicts our assumption that $\mathbb{F}_q(x)(\alpha_1, \alpha_2, \dots)$ is an infinite extension of $\mathbb{F}_q(x)$. □

Corollary 4.2. *Let $\alpha_1, \alpha_2, \dots$ be a sequence of power series contained in $\overline{M}$ with $\deg(\alpha_k) = k$ for each k. Let $f(x) \in \mathbb{F}_q[\![x]\!]$ be a power series satisfying $\mathrm{dLog}^{(k)}(f) = \alpha_k$ for all $k \geq 1$. Then $f(x)$ is transcendental.*

Proof. From Corollary 3.15, we know that the α_k are linearly independent over $\mathbb{F}_q(x)$, so they cannot be contained in a finite extension. Then use Theorem 4.1. □

4.2. ***Estimating*** $\mathbf{dLog^{(k)}(E_p(x))}$**.** Let L denote the differential operator $\frac{d}{dx} - \tau(x)/x$ on $\mathbb{Z}_q((x))$. Using the description $E_p(x) = \exp\bigl(\sum_{n=0}^{\infty} x^{p^n}/p^n\bigr)$, we see that, for $k \geq 1$,

$$k! \cdot \mathrm{dLog}^{(k)}(E_p(x)) = L^{k-1}\left(\frac{\tau(x)}{x}\right). \tag{10}$$

We have the following proposition.

Proposition 4.3. *For $k \geq 1$, we have*

$$k! \cdot \mathrm{dLog}^{(k)}(E_p(x)) \equiv \frac{\tau(x)^k}{x^k} \mod \widehat{M}_{k-1}.$$

Proof. We proceed by induction on k. When $k = 1$, the result is immediate. Assume the result holds for k. From (10) and our inductive hypothesis, we have

$$L^k\left(\frac{\tau(x)}{x}\right) = L\left(\frac{\tau(x)^k}{x^k} + c\right),$$

where $c \in \widehat{M}_{k-1}$. We know $\frac{d}{dx}(\tau(x)^k/x^k + c) \in \widehat{M}_k$ from Lemmas 3.7 and 3.9. We also know $\tau(x)/xc \in \widehat{M}_k$ by Lemma 3.9. Thus,

$$L\left(\frac{\tau(x)^k}{x^k} + c\right) \equiv \frac{\tau(x)^{k+1}}{x^{k+1}} \mod \widehat{M}_k.$$

The proposition follows from (10). □

Corollary 4.4. *For $k \geq 1$, we have* $\mathrm{dLog}^{(k)}(\bar{E}_p(x)) \equiv \bar{\omega}_x^k/x^k \mod \overline{M}_{k-1}$.

Proof. From Corollary 3.24 and Proposition 4.3, we know $k! \cdot \mathrm{dLog}^{(k)}(E_p(x)) \equiv k!\omega_x^k/x^k \mod \widehat{M}_{k-1}$. By Corollary 3.13, we see that $\mathrm{dLog}^{(k)}(E_p(x)) \equiv \omega_x^k/x^k \mod \widehat{M}_{k-1}$. The corollary follows by reducing modulo p. □

At this point we may establish the transcendence of $\bar{E}_p(x)$.

Theorem 4.5. *The series $\bar{E}_p(x)$ is transcendental over $\mathbb{F}_p(x)$.*

Proof. Set $\alpha_k = \mathrm{dLog}^{(k)}(\bar{E}_p(x))$. From Corollary 4.4, we see that $\alpha_k \in \overline{M}$ and $\mathrm{dep}(\alpha_k) = k$. The theorem follows from Corollary 4.2. □

4.3. ***Estimating*** $\mathbf{dLog^{(k)}[\bar{E}_p(f_1)^{n_1} \cdots \bar{E}_p(f_r)^{n_r}]}$**.** Recall from the introduction that, for $f = \sum c_i x^i \in x\mathbb{F}_q[x]$, we define

$$f^* = \sum_{\substack{i \geq 0 \\ p \nmid i}} c_i^*(f) x^i \quad \text{with } c_i^*(f) = \sum_{k \geq 0} c_{ip^k}^{1/p^k}.$$

We can express $c_i^*(f)$ uniquely as $\sum_{j=0}^{f-1} c_{x_j^i}^* \zeta^{p^j}$, where $c_{x_j^i}^* \in \mathbb{F}_p$. In particular, we have

$$f^* = \sum_{z \in X} c_z^* z.$$

In this subsection we prove the following proposition.

Proposition 4.6. *Let $k \geq 0$ and let $n_1, \dots, n_r \geq 0$. Let $f_1, \dots, f_r \in x\mathbb{F}_q[x]$. Then*

$$\Delta_k := \mathrm{dLog}^{(k)}[\bar{E}_p(f_1)^{n_1} \cdots \bar{E}_p(f_r)^{n_r}]$$

is in $\overline{M}_k$ and, for any $z \in X$, we have

$$x^k \dot{\omega}_z^k\big(\mathrm{dLog}^{(k)}[\bar{E}_p(f_1)^{n_1} \cdots \bar{E}_p(f_r)^{n_r}]\big) = \left(\sum_{i=1}^{r} n_i c_z^*(f_i)\, \mathrm{dLog}^{(1)}(f_i)\right)^k.$$

In particular, Δ_k has depth exactly k if there exists $z \in X$ such that $\sum_{i=1}^{r} n_i c_z^*(f_i)\, \mathrm{dLog}^{(1)}(f_i)$ is nonzero.

The proof of Proposition 4.6 is broken into several steps. The main ingredients are Corollary 4.4 and the following well-known identities on higher derivatives:

$$\partial^{(k)}(f_1 \cdots f_n) = \sum_{\substack{k_1,\dots,k_n \geq 0 \\ k_1+\cdots+k_n=k}} \partial^{(k_1)}(f_1) \cdots \partial^{(k_n)}(f_n), \tag{11}$$

$$\partial^{(k)}(f(g)) = \sum_{j=1}^{k} \partial^{(j)}(f)(g) \cdot \sum_{\substack{k_1,\dots,k_j \geq 1 \\ k_1+\cdots+k_j=k}} \partial^{(k_1)}(g) \cdots \partial^{(k_j)}(g). \tag{12}$$

Lemma 4.7. *Let n be any p-adic integer. We have*

$$\mathrm{dLog}^{(k)}(\bar{E}_p(x)^n) \equiv n^k \frac{\bar{\omega}_x^k}{x^k} \mod \overline{M}_{k-1}.$$

Proof. First assume n is a positive integer. By Corollaries 4.4 and 3.23 and (11), we have

$$\begin{aligned}
\mathrm{dLog}^{(k)}(\bar{E}_p(x)^n) &\equiv \sum_{\substack{k_1,\dots,k_n \geq 0 \\ k_1+\cdots+k_n=k}} \frac{1}{x^k} \bar{\omega}_x^{k_1} \cdots \bar{\omega}_x^{k_n} \mod \overline{M}_{k-1} \\
&\equiv \sum_{\substack{k_1,\dots,k_n \geq 0 \\ k_1+\cdots+k_n=k}} \binom{k}{k_1, \dots, k_n} \frac{\bar{\omega}_x^k}{x^k} \mod \overline{M}_{k-1} \\
&\equiv n^k \frac{\bar{\omega}_x^k}{x^k} \mod \overline{M}_{k-1}.
\end{aligned}$$

For the general result, write $n = a + p^m b$, where a is a positive integer. If $m > v_p(k)$, we have $\mathrm{dLog}^{(k)}(\bar{E}_p(x)^n) = \mathrm{dLog}^{(k)}(\bar{E}_p(x)^a)$, since $\partial^{(k)}(f^{p^m}) = 0$. The general result follows. □

Corollary 4.8. *For $f \in x\mathbb{F}_q[x]$, we have*

$$\mathrm{dLog}^{(k)}(\bar{E}_p(f)^n) \equiv n^k \frac{\bar{\omega}_x^k(f)}{x^k} (\mathrm{dLog}^{(1)} f)^k \mod \overline{M}_{k-1}.$$

Proof. From Lemma 4.7, we see that $\mathrm{dLog}^{(i)}(\bar{E}_p(x)^n) \in \overline{M}_{k-1}$ for $1 \leq i < k$. Note that, for $g \in \overline{M}_{k-1}$ and $h \in x\mathbb{F}_q[x]$, we have $g \circ h \in \overline{M}_{k-1}$, so $\mathrm{dLog}^{(i)}(\bar{E}_p(x)^n) \circ f \in \overline{M}_{k-1}$ for $1 \leq i < k$. The corollary follows from (12) and Lemma 4.7. □

Lemma 4.9. *Let $f \in x\mathbb{F}_q[x]$. Then*

$$\bar{\omega}_x^k(f) \equiv \sum_{\substack{b\in D\\ \deg(b)=k}} c_b^*(f)\overline{w}_b \mod \overline{M}_{k-1}, \quad \text{where } c_b^*(f) = \prod_{i=1}^{k} c_{b(i)}^*(f).$$

Proof. First note that $\bar{\omega}_x^k(f) \equiv \bar{\omega}_x^k(f^*) \bmod \overline{M}_{k-1}$. This can be proven by inducting on k and using (3). We are therefore reduced to the case where $f = f^*$. The result follows from the $\mathbb{F}_p$-linearity of τ modulo p and unraveling the nested τ's. □

Corollary 4.10. *For all $z \in X$, we have $\dot{\omega}_z^k(\bar{\omega}_x^k(f)) = c_z^*(f)^k$.*

Lemma 4.11. *Let $k_1, \dots, k_r \geq 1$ with $k_1 + \cdots + k_r = k$. Then*

$$\dot{\omega}_z^k\big(\bar{\omega}_x^{k_1}(f_1(x)) \cdots \bar{\omega}_x^{k_r}(f_r(x))\big) = \binom{k}{k_1, \dots, k_r} \prod_{i=1}^{r} c_z^*(f_i)^{k_i}.$$

Proof. This follows from Corollaries 4.10 and 3.25. □

Proof of Proposition 4.6. From (11) and Corollary 4.8, we have

$$\begin{aligned} x^k \operatorname{dLog}^{(k)}[\bar{E}_p(f_1)^{n_1} \cdots \bar{E}_p(f_r)^{n_r}] &= \sum_{\substack{k_1,\dots,k_r\geq 0\\ k_1+\cdots+k_r=k}} \prod_{i=1}^{r} \operatorname{dLog}^{(k_i)}(\bar{E}_p(f_i)^{n_i}) \\ &\equiv \sum_{\substack{k_1,\dots,k_r\geq 0\\ k_1+\cdots+k_r=k}} \prod_{i=1}^{r} n_i^{k_i} (\operatorname{dLog}^{(1)}(f_i))^{k_i} \bar{\omega}_x^{k_i}(f_i) \mod \overline{M}_{k-1}. \end{aligned}$$

Applying Lemma 4.11 to $\prod_{i=1}^{r} \bar{\omega}_x^{k_i}(f_i)$ gives

$$\begin{aligned} x^k \dot{\omega}_z^k\big(\operatorname{dLog}^{(k)}[\bar{E}_p(f_1)^{n_1} \cdots \bar{E}_p(f_r)^{n_r}]\big) &= \sum_{\substack{k_1,\dots,k_r\geq 0\\ k_1+\cdots+k_r=k}} \binom{k}{k_1, \dots, k_r} \prod_{i=1}^{s} [n_i \operatorname{dLog}^{(1)}(f_i) c_z^*(f_i)]^{k_i} \\ &= \left(\sum_{i=1}^{r} n_i \operatorname{dLog}^{(1)}(f_i) c_z^*(f_i) \right)^k. \end{aligned}$$

□

5. Algebraic independence results

In this section we prove Theorems 1.3 and 1.7.

5.1. ***Iterative differential Galois theory and transcendence.*** We will make use of iterative differential (ID for short) Galois theory, as expounded on by Matzat and van der Put [2003] (in particular, Sections 3–4 therein). Let K be the algebraic closure of $\mathbb{F}_q(x)$ in $\overline{\mathbb{F}}_p((x))$. The higher derivatives $\partial^{(k)}$ make K into an ID-field. For any $f \in x\mathbb{F}_q[x]$ we recursively define a sequence $A_{f,0}, A_{f,1}, \dots \in K$ by

$$A_{f,0} = 1 \quad \text{and} \quad A_{f,k} = -\sum_{i=0}^{k-1} A_{f,i} \operatorname{dLog}^{(k-i)}(\bar{E}_p(f)).$$

We then define an ID-module $N_f = Ke_f$ over K of rank one by the rule

$$\partial^{(k)}(e_f) = A_{f,k}e_f.$$

Note that N_f trivializes over the ring $K[\bar{E}_p(f), 1/\bar{E}_p(f)]$. For $f_1, \dots, f_r \in x\mathbb{F}_q[x]$, we define the rank r ID-module

$$N := \bigoplus_{i=1}^{r} N_{f_1}.$$

Then N has a full system of solutions over the ring

$$R_0 := K\left[\bar{E}_p(f_1), \dots, \bar{E}_p(f_r), \frac{1}{\bar{E}_p(f_1)\cdots\bar{E}_p(f_r)}\right].$$

The Picard–Vessiot ring of N is $R = R_0/I$, where I is a maximal ID-ideal (i.e., I is a maximal element in the ordered set of ideals of R_0 satisfying $\partial^{(k)}(I) \subset I$). The ID-Galois group $\mathcal{G}(N)$ is the group of ID-automorphisms of R that fix K. A key fact is that $\mathcal{G}(N)$ is a reduced algebraic group over the field of constants $\bar{\mathbb{F}}_p$ and that $\mathrm{Spec}(R)$ is a $\mathcal{G}(N)$-torsor over K. In particular, we have

$$\mathrm{tr.deg}_K(\mathrm{Frac}(R_0)) \geq \mathrm{tr.deg}_K(\mathrm{Frac}(R)) = \dim_{\bar{\mathbb{F}}_p}(\mathcal{G}(N)).$$

Thus, to prove the algebraic independence of the $\bar{E}_p(f_i)$, it suffices to show $\mathcal{G}(N)$ has dimension r.

On the other hand, there is a Tannakian interpretation of the ID-Galois group. Let ID_K denote the category of ID-modules over K. Then ID_K is an $\bar{\mathbb{F}}_p$-linear tensor category. Let $[N]$ be the full subcategory of ID_K generated by tensor powers of N and its dual. Then $[N]$ is again an $\bar{\mathbb{F}}_p$-linear tensor category and thus isomorphic to the category of representations for an affine algebraic group $\mathrm{Gal}(N)$ defined over $\bar{\mathbb{F}}_p$. By standard arguments (see [van der Put and Singer 2003] for the characteristic 0 case and [Matzat and van der Put 2003] for our precise situation), we have

$$\mathcal{G}(N) \cong \mathrm{Gal}(N).$$

Note that, since N_{f_i} has rank one, we know $\mathrm{Gal}(N_{f_i})$ is a closed subgroup of $\mathbb{G}_m$. In particular, we see that $\mathrm{Gal}(N)$ is a closed subgroup of $\mathbb{G}_m^r$. To prove that $\mathrm{Gal}(N) \cong \mathbb{G}_m^r$, it is enough to show that, for any $n_1, \dots, n_r \in \mathbb{Z}$ that are not all zero, the ID-module $N_{f_1}^{\otimes n_1} \otimes \cdots \otimes N_{f_r}^{\otimes n_r}$ is nontrivial. This amounts to proving $\bar{E}_p(f_1)^{n_1}\cdots\bar{E}_p(f_r)^{n_r}$ is transcendental over K. Furthermore, we easily reduce to the case where the n_i are not all divisible by p.

5.2. ***Proof of Theorem 1.3.*** Let $f_1, \dots, f_r$ satisfy one of the two conditions from Theorem 1.3. From the discussion in Section 5.1 we must show $\bar{E}_p(f_1)^{n_1}\cdots\bar{E}_p(f_r)^{n_r}$ is transcendental, where not all the n_i are divisible by p. Using Corollary 4.2 and Proposition 4.6, we reduce to showing that, for some $z \in X$, we have

$$\sum_{i=1}^{r} n_i c_z^*(f_i)\,\mathrm{dLog}^{(1)}(f_i) \neq 0.$$

The case where the f_i^* are not all zero and no nontrivial power product of the f_i are contained in $\mathbb{F}_q(x)^p$. We have

$$\sum_{i=1}^{r} n_i c_z^*(f_i)\,\mathrm{dLog}^{(1)}(f_i) = \mathrm{dLog}^{(1)}\Bigg[\prod_{i=1}^{r} f_i^{n_i c_z^*(f_i)}\Bigg].$$

By our assumption, the product in the $\mathrm{dLog}^{(1)}$ is not in $\mathbb{F}_q(x)^p$. The theorem follows by observing that the kernel of $\mathrm{dLog}^{(1)}$ on $\mathbb{F}_q(x)$ is $\mathbb{F}_q(x)^p$.

The case where $f_1^*, \ldots, f_r^*$ are linearly independent. Without loss of generality, assume $p \nmid n_1$. We may also assume that none of the f_i are p-th powers. Let $g \in \mathbb{F}_q[x]$ be an irreducible polynomial dividing f_1 and let v_g denote the valuation associated to g. Write $f_i = g^{b_i} h_i$, where $g \nmid h_i$. We can find g such that $p \nmid b_1$, as otherwise f_1 would be a p-th power. Since $f_1^*, \ldots, f_r^*$ are linearly dependent over $\mathbb{F}_p$,

$$n_1 b_1 f_1^* + \cdots + n_r b_r f_r^* \neq 0.$$

In particular, there exists $z \in X$ such that

$$D_z := n_1 b_1 c_z^*(f_1) + \cdots + n_r b_r c_z^*(f_r) \neq 0.$$

Then

$$\sum_{i=1}^{r} n_i c_z^*(f_i)\,\mathrm{dLog}^{(1)}(f_i) = D_z\,\mathrm{dLog}^{(1)}(g) + \sum_{i=1}^{r} n_i c_z^*(f_i)\,\mathrm{dLog}^{(1)}(h_i).$$

If α is a root of g, we see that $D_z\,\mathrm{dLog}^{(1)}(g)$ has a simple pole at α, while $\mathrm{dLog}^{(1)}(h_i)$ is regular at α. In particular, the right side of this sum has a simple pole at α and thus is nonzero.

5.3. ***Proof of Theorem 1.7.*** We now prove Theorem 1.7. Let ξ be a generator of $\mathbb{F}_p^\times$. Let $[\xi]$ denote the Teichmüller lift of ξ. Set $r = \phi(p-1)$. First, we show that $\bar{E}_p(x), \ldots, \bar{E}_p(\xi^{r-1}x)$ are algebraically independent. By the ID-Galois group argument in Section 5.1, it suffices to show

$$A(x) := \prod_{i=0}^{r-1} \bar{E}_p(\xi^i x)^{n_i}$$

is transcendental, where $n_0, \ldots, n_{r-1}$ are integers not all divisible by p. Indeed, this implies that the ID-Galois group of the ID-module $N_x \oplus N_{\xi x} \oplus \cdots \oplus N_{\xi^{r-1}x}$ is all of $\mathbb{G}_m^r$. From Lemma 2.3, we have

$$A(x) = \bar{E}_p(x)^{n_0 + n_1[\xi] + \cdots + n_{r-1}[\xi]^{r-1}}.$$

As the $1, \ldots, [\xi]^{r-1}$ are independent over $\mathbb{Z}$, we have $A(x) = \bar{E}_p(x)^n$, where n is a nonzero p-adic number. Thus, it suffices to show $\bar{E}_p(x)^n$ is transcendental for any nonzero p-adic number with $p \nmid n$. By Lemma 4.7, we see that $\mathrm{dLog}^{(k)}(\bar{E}_p(x)^n)$ has depth k. It follows from Corollary 4.2 that $\bar{E}_p(x)^n$ is transcendental over $\mathbb{F}_p(x)$. Thus, we have proven

$$\mathrm{tr.deg}_{\mathbb{F}_p(x)}\,\mathbb{F}_p(x)(\bar{E}_p(\xi^i x))_{0 \le i \le r-1} = r.$$

For $j > r-1$, we can write $[\xi]^j = c_0 + c_1[\xi] + \cdots + c_{r-1}[\xi]^{r-1}$, where the c_i are integers. Then Lemma 2.3 gives

$$\bar{E}_p(\xi^j x) = \prod_{i=0}^{r-1} \bar{E}_p(\xi^i x)^{c_i},$$

so

$$\operatorname{tr.deg}_{\mathbb{F}_p(x)} \mathbb{F}_p(x)(\bar{E}_p(\xi^i x))_{0 \le i \le p-2} = r.$$

Acknowledgements

The author wishes to thank Dinesh Thakur for his enthusiasm and comments on some very preliminary versions of this article. We also thank the reviewers for helpful comments and for providing some historical context for this article.

References

[Adolphson and Sperber 1989] A. Adolphson and S. Sperber, "Exponential sums and Newton polyhedra: cohomology and estimates", *Ann. of Math.* (2) **130**:2 (1989), 367–406. MR

[Allouche and Shallit 2003] J.-P. Allouche and J. Shallit, *Automatic sequences: theory, applications, generalizations*, Cambridge Univ. Press, 2003. MR

[Allouche et al. 1988] J.-P. Allouche, M. Mendès France, and A. J. van der Poorten, "Indépendance algébrique de certaines séries formelles", *Bull. Soc. Math. France* **116**:4 (1988), 449–454. MR

[Ax 1971] J. Ax, "On Schanuel's conjectures", *Ann. of Math.* (2) **93** (1971), 252–268. MR

[Christol 1979] G. Christol, "Ensembles presque periodiques k-reconnaissables", *Theoret. Comput. Sci.* **9**:1 (1979), 141–145. MR

[Christol et al. 1980] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, "Suites algébriques, automates et substitutions", *Bull. Soc. Math. France* **108**:4 (1980), 401–419. MR

[Dieudonné 1957] J. Dieudonné, "On the Artin–Hasse exponential series", *Proc. Amer. Math. Soc.* **8** (1957), 210–214. MR

[Kolchin 1968] E. R. Kolchin, "Algebraic groups and algebraic dependence", *Amer. J. Math.* **90** (1968), 1151–1164. MR

[Matzat and van der Put 2003] B. H. Matzat and M. van der Put, "Iterative differential equations and the Abhyankar conjecture", *J. Reine Angew. Math.* **557** (2003), 1–52. MR

[Ostrowski 1946] A. Ostrowski, "Sur les relations algébriques entre les intégrales indéfinies", *Acta Math.* **78** (1946), 315–318. MR

[Papanikolas 2008] M. A. Papanikolas, "Tannakian duality for Anderson–Drinfeld motives and algebraic independence of Carlitz logarithms", *Invent. Math.* **171**:1 (2008), 123–174. MR

[van der Put and Singer 2003] M. van der Put and M. F. Singer, *Galois theory of linear differential equations*, Grundl. Math. Wissen. **328**, Springer, 2003. MR

[Thakur 2020] D. S. Thakur, "Automata methods in transcendence", pp. 351–372 in *t-motives*: *Hodge structures*, *transcendence and other motivic aspects*, edited by G. Böckle et al., Eur. Math. Soc., Berlin, 2020. MR

[Wan 1993] D. Q. Wan, "Newton polygons of zeta functions and L functions", *Ann. of Math.* (2) **137**:2 (1993), 249–293. MR

Communicated by Michael Singer
Received 2024-05-25 Revised 2025-05-05 Accepted 2025-06-27

jjk221@lehigh.edu *Department of Mathematics, Lehigh University, Bethlehem, PA, United States*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Antoine Chambert-Loir
Université Paris-Diderot
France

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Olivier Benoist	Ecole Normale Supérieure, France	Martin Olsson	University of California, Berkeley, USA
Bhargav Bhatt	University of Michigan, USA	Irena Peeva	Cornell University, USA
Frank Calegari	University of Chicago, USA	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Anand Pillay	University of Notre Dame, USA
Brian D. Conrad	Stanford University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Samit Dasgupta	Duke University, USA	Victor Reiner	University of Minnesota, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Benjamin Schraen	Université Claude Bernard Lyon 1, France
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	SUNY Buffalo, USA
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2026 is US $590/year for the electronic version, and $865/year (+$75, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 2000 Allston Way #59, Berkeley, CA 94701-4004, is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2026 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 20 No. 8 2026

Supersymmetric monoidal categories 1479
STEVEN V SAM and ANDREW SNOWDEN

Rational curves and the Hilbert property on Jacobian Kummer varieties 1543
DAMIÁN GVIRTZ-CHEN and ZHIZHONG HUANG

Homological regularities and concavities 1559
ELLEN KIRKMAN, ROBERT WON and JAMES J. ZHANG

Transcendence properties of the Artin–Hasse exponential modulo p 1597
JOE KRAMER-MILLER

Anticyclotomic Euler system over biquadratic fields 1615
KIM TUAN DO

Explicit Hecke descent for special cycles 1649
SYED WAQAR ALI SHAH