David GOSS[†]

Digit permutations revisited

Digit permutations revisited

par David GOSS†

Résumé. Nous considérons ici les fonctions L en caractéristique p ainsi que le groupe $S_{(q)}$ qui se trouve agir comme des symétries de ces fonctions. Nous expliquons diverses actions de $S_{(q)}$ qui apparaissent naturellement dans la théorie ainsi que les extensions de ces actions. En général de telles extensions semblent hautement arbitraires, mais dans le cas où les zéros sont non-ramifiés, l'extension est unique (et il est raisonnable de s'attendre à l'unicité seulement dans ce cas-là). Avoir des zéros non-ramifiés est le mieux que l'on puisse espérer en caractéristique positive, et semble êtere un avatar de l'hypothèse de Riemann dans ce contexte. Voir Section 8 pour des discussions plus détaillées.

Abstract. We discuss here characteristic p L-series as well as the group $S_{(q)}$ which appears to act as symmetries of these functions. We explain various actions of $S_{(q)}$ that arise naturally in the theory as well as extensions of these actions. In general such extensions appear to be highly arbitrary but in the case where the zeroes are unramified, the extension is unique (and it is reasonable to expect it is unique only in this case). Having unramified zeroes is the best one could hope for in finite characteristic and appears to be an avatar of the Riemann hypothesis in this setting; see Section 8 for a more detailed discussion.

1. Introduction

The publication of V. G. Drinfeld's seminal paper *Elliptic modules* [7] in 1974 has lead to the emergence of a true "analytic theory of numbers" involving analysis in finite characteristic. This work, together with previously little known work by L. Carlitz starting in the 1930's (see for instance [8, Chapter 3]), allow one to create very viable analogs of the classical special functions of complex arithmetic. Thus, for instance, we are able to construct analytic characteristic-p valued L-series and zeta functions which possess special values extremely similar to those of classical L-series (such as an

analog, due to Carlitz, of Euler's great formula for $\zeta_{\mathbb{Q}}(2m)$ for m a positive integer). We also present here some new functions originally defined by B. Anglès (Subsection 5.2).

These analogies, along with others not mentioned here, encourage us to look for a deeper theory associated to these functions. In particular, it is completely reasonable to search for a deeper theory of the zeroes of these functions and, as of this writing, such a theory is still very much in its infancy. However, there have been a few notable victories in this regard. For instance, in the 1990's, based on earlier work of D. Wan, J. Sheats [17] was able to establish that the zeroes of $\zeta_{\mathbb{F}_q[\theta]}(s)$ are simple and lie "on the line" $\mathbb{F}_q((1/\theta))$. This clearly is similar to what is *expected* for the Riemann zeta function.

Of course, basic to the study of the Riemann hypothesis, and, indeed, all complex valued L-series are their functional equations which are symmetries under the transformation $s \mapsto m - s$ for some positive integer m. In finite characteristic it was realized very early on that no such simple symmetry would be satisfied. However, in 1995 Dinesh Thakur [19] published some calculations that led the present author to construct a certain huge group $S_{(q)}$ (see Section 7 and [10]) which *appears* to act as symmetries of the characteristic p L-series (but in a way that is still far from clear).

It is our purpose here to revisit $S_{(q)}$ as well as the zeroes in finite characteristic. We will establish the ubiquity of $S_{(q)}$, as well as its naturality, by expressly presenting many different actions of $S_{(q)}$ on spaces (such as $\mathbb{Z}_p$ or $\mathbb{F}_q((1/\theta))$), functions on these spaces and measures on these spaces, see Section 7. In some cases, these actions are remarkably simple; see, for instance, Corollary 7.5 or Proposition 7.10. Along the way, we obtain a new p-adic congruence for binomial coefficients in Proposition 7.6.

It is well-known that every entire function over a nonarchimedean field is determined up to a constant by its zeroes. Using this, it was pointed out in [11] that the best one could hope for, at least in the case where the base ring $A = \mathbb{F}_q[\theta]$ is to have the zeroes lie in a constant field extension of $\mathbb{F}_q((1/\theta))$. In other words, the zeroes should be *unramified*. As we point out in Subsection 8.1, if one views the classical Riemann hypothesis from the viewpoint of the Carlitz module, it also becomes a statement that the zeroes are unramified!

We originally defined the action of $S_{(q)}$ on $\mathbb{F}_q((1/\theta))$. But as mentioned the zeroes will not always be in this field. They will, however, always be algebraic over $\mathbb{F}_q((1/\theta))$ and so, with a choice of basis of an finite algebraic extension, we show how to further extend the action of $S_{(q)}$ (in an extremely noncanonical fashion). It is expected that this action is indeed *highly* dependent on the choice of basis chosen. However, when the extension is given by a constant field extension (that is the zero lies in an unramified extension),

the action can be chosen to be just the usual extension by scalars (via the tensor product). The constant field extension can then be obtained as the commutator algebra of this extension.

In other words, the action of $S_{(q)}$ appears to allow us to precisely detect unramified zeroes.

In the final section of [5], A. Connes quotes Galois to support his contention that the classical Riemann hypothesis should somehow be the beginning and not the end of the understanding of zeta zeroes. It is precisely in this optic that we view the potential action of $S_{(q)}$ (presented here and in [11]) on the zeroes in characteristic p as it seems to portend a much deeper understanding of these zeroes.

2. Review of basic Carlitz theory

We recall here some basic ideas of L. Carlitz that can be found in [8].

2.1. The Carlitz factorial. As mentioned, we have $A = \mathbb{F}_q[\theta]$ where $q = p^{m_0}$ and p is prime and $k = \mathbb{F}_q(\theta)$ its quotient field.

Definition 2.1. Let i be a positive integer. We set $[i] := \theta^{q^i} - \theta$.

Clearly $\frac{\mathrm{d}[i]}{\mathrm{d}\theta} = -1$ and so $[i]$ is separable. Standard theory of finite fields then readily establishes

$$(2.1) \qquad\qquad [i] = \prod_f f \,,$$

where f runs over the monic prime polynomials whose degree divides i.

Definition 2.2.
   (1) We set $D_0 := 1$, and for $i > 0$, $D_i := [i][i-1]^q \cdots [1]^{q^{i-1}}$.
   (2) We set $L_0 := 1$, and for $i > 0$, $L_i := [i][i-1] \cdots [1]$.

Notice that $L_i = [i]L_{i-1}$ and $D_i = [i]D_{i-1}^q$. The next result follows directly using (2.1).

Proposition 2.3. *We have D_i is the product of all monic polynomials in θ of degree i. Moreover, L_i is the least common multiple of all such monic polynomials.*

Let j be a nonnegative integer written q-adically as $j = \sum_{t=0}^m c_t q^t$ where $0 \le c_t < q$ for all t.

Definition 2.4. We set

$$\Pi(j) := \prod_{t=0}^m D_t^{c_t} \,.$$

Notice, of course, that $\Pi(q^e) = D_e$.

Proposition 2.5. *We have*

$$\Pi(q^j - 1) = (D_0 \cdots D_{j-1})^{q-1} = \frac{D_j}{L_j} = (-1)^j \prod_\alpha \alpha \,,$$

where α runs over all nonzero polynomials in A of degree $< j$.

Proof. The first product is simply the definition of $\Pi(q^j - 1)$. The second equality follows from repeatedly using $D_i = [i]D_{i-1}^q$ and the third equality follows upon expressing the product over *all* nonzero elements of degree $< j$ as a corresponding product over the monic polynomials of degree $< j$. $\square$

2.1.1. *A determinant formula.* Here we will explain how the special factorials $\Pi(\frac{q^m-1}{q-1})$ can be obtained as a determinant of Vandermonde type. We begin with a very clever observation of F. Voloch [20] relating differentiation and q-th powers. Let $f(\theta) \in A$ be a polynomial in θ and let $\partial_j = \partial_{\theta,j}$ be the j-th divided derivative in θ of $f(\theta)$. So one has $f(x) = \sum_j \partial_j f(\theta)(x - \theta)^j$ upon expanding about $x = \theta$.

Proposition 2.6. *With $f(\theta)$ as above, and i a nonnegative integer, we have*

$$f^{q^i}(\theta) = \sum_j \partial_j f(\theta)[i]^j \,.$$

Proof. One simply uses the above Taylor expansion, substitutes θ^{q^i} for x, and notes that $f(\theta^{q^i}) = f^{q^i}(\theta)$. $\square$

Now let m be a fixed positive integer and $\{x_0, \ldots, x_m\} \subset A$ have degree $\leq m$. Set

$$M = M(x_0, \ldots, x_m) := \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & \ldots & x_m \\ x_0^q & x_1^q & x_2^q & x_3^q & \ldots & x_m^q \\ x_0^{q^2} & x_1^{q^2} & x_2^{q^2} & x_3^{q^3} & \ldots & x_m^{q^2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_0^{q^m} & x_1^{q^m} & x_2^{q^m} & x_3^{q^m} & \ldots & x_m^{q^m} \end{pmatrix},$$

$$V = V(0, [1], \ldots, [m]) := \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ 1 & [1] & [1]^2 & [1]^3 & \ldots & [1]^m \\ 1 & [2] & [2]^2 & [2]^3 & \ldots & [2]^m \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & [m] & [m]^2 & [m]^3 & \ldots & [m]^m \end{pmatrix},$$

and,

$$W = W(x_0, \ldots, x_m) := \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & \ldots & x_m \\ \partial_1 x_0 & \partial_1 x_1 & \partial_1 x_2 & \partial_1 x_3 & \ldots & \partial_1 x_m \\ \partial_2 x_0 & \partial_2 x_1 & \partial_2 x_2 & \partial_2 x_3 & \ldots & \partial_2 x_m \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \partial_m x_0 & \partial_m x_1 & \partial_m x_2 & \partial_m x_3 & \ldots & \partial_m x_m \end{pmatrix}.$$

Notice, of course, that M is an example of a Moore matrix, V a matrix of Vandermonde type and W a Wronskian. As M. Papanikolas has communicated to the author [13], Proposition 2.6 immediately implies the next result relating these three famous types of matrices.

Proposition 2.7. *With the above notations, we have*

$$M = VW.$$

Now choose $x_j = \theta^j$, for $j = 0, \ldots, m$.

Corollary 2.8. *We have*

$$\Pi\left(\frac{q^m - 1}{q - 1}\right) = \det V(0, [1], \ldots, [m]).$$

Proof. Note that the Wronskian for our choice of functions is now unipotent. So from Proposition 2.7 we obtain, with the obvious notation, $\det M = \det V$. But Moore's result (Section 1.3 of [8]) now establishes that

$$\Pi\left(\frac{q^m - 1}{q - 1}\right) = \det M(1, \theta, \ldots, \theta^m). \qquad \square$$

Remarks 2.9. Corollary 2.8 is quite remarkable in that it shows that for arbitrary choices of $\{x_i\}$ the Wronskian determinant and the Moore determinant always differ by $\Pi((q^m - 1)/(q - 1))$. Moreover, we also deduce that our matrix V is invertible. Therefore, and more remarkably, we see that one can always express the divided derivatives of elements in $A_{<m+1}$ in terms of their q^j-th powers with denominator at most $\Pi((q^m - 1)/(q - 1))$.

2.2. The Carlitz polynomials. Classically, one passes from $n!$ to the binomial coefficient functions $\binom{s}{n}$ defined, as usual, by $\binom{s}{n} := \frac{s(s-1)\cdots(s-n+1)}{n\cdot(n-1)\cdots1}$. Clearly $\binom{s}{n}$ is a polynomial of degree n in s and is well-known to take on integer values for integer arguments.

As $\binom{s}{n}$ has degree n, the collection $\{\binom{s}{n}\}$ forms a basis for the vector space of polynomials in s over any field of characteristic 0. Let $p(s)$ be a polynomial of degree d which we write as $p(s) = \sum_{k=0}^{d} a_{p,k} \binom{s}{k}$. It is further well known that

$$a_{p,k} = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} p(j).$$

The Carlitz polynomials, recalled here, play the role for the Carlitz factorial that is played by $\binom{s}{n}$ for $n!$. It will be convenient to begin with some definitions.

Definition 2.10.
  (1) Let A_d be the polynomials in A of degree d.
  (2) Let A_+ be the monic polynomials of A and $A_{d,+}$ the monic polynomials in A of degree d.
  (3) Let $A_{<d}$ be the polynomials in A of degree strictly less than d.

Definition 2.11. We set $e_0(x) := x$ and, for an integer $t > 0$,

$$(2.2) \qquad e_t(x) := \prod_{\alpha \in A_{<t}} (x - \alpha).$$

Since the roots of $e_j(x)$ are a finite dimensional $\mathbb{F}_q$-vector space of dimension t, and it is separable, it is well-known that is therefore an $\mathbb{F}_q$-linear function of degree q^t in x.

Proposition 2.12. *Let h be any monic polynomial of degree t. Then $e_t(h) = D_t$.*

Proof. This follows immediately from (2.2) and Proposition 2.3. $\qquad \square$

Let j be a nonnegative integer written q-adically as $j = \sum_{t=0}^{m} c_t q^t$, as above.

Definition 2.13.
  (1) We set $g_j(x) := \prod_t e_t(x)^{c_t}$.
  (2) We set

$$G_j(x) := \prod_t \left(\frac{e_t(x)}{D_t} \right)^{c_t} = \frac{g_j(x)}{\Pi(j)}.$$

Notice that both $g_j(x)$ and $G_j(x)$ have degree j in x. Moreover, if $\zeta \in \mathbb{F}_q$, then $g_j(\zeta x) = \zeta^j g_j(x)$ and $G_j(\zeta x) = \zeta^j G_j(x)$ for all j.

Proposition 2.14. *Let $\alpha \in A$. Then $G_j(\alpha) \in A$ for all $\alpha \in A$.*

Proof. The values $\{G_{q^t}(\alpha) = \frac{e_t(\alpha)}{D_t}\}$ occur as the coefficients of the Carlitz module $C_\alpha(\tau)$ where τ is the q-th power mapping; as such they are in A. Consequently, $G_j(\alpha) \in A$ for all $\alpha \in A$ also. $\qquad \square$

Let y be another indeterminate. With j as above, we then have

$$(2.3) \qquad (x+y)^j = \sum_{w+v=j} \binom{j}{v} x^v y^w = (x+y)^{\sum c_t q^t} = \prod_t (x^{q^t} + y^{q^t})^{c_t}.$$

Notice, obviously, that $e_t(x+y) = e_t(x) + e_t(y)$. The *addition formulas* now follow from (2.3) and are given by our next result.

Proposition 2.15. *We have:*

$$g_j(x+y) = \sum_{w+v=j} \binom{j}{v} g_v(x) g_w(y),$$

and

$$G_j(x+y) = \sum_{w+v=j} \binom{j}{v} G_v(x) G_w(y).$$

In other words, both $\{g_j(x)\}$ and $\{G_j(x)\}$ satisfy the binomial theorem. We call them "the Carlitz polynomials," and we will now define their duals.

Definition 2.16.

(1) Let $0 \leq v < q$ and $t \geq 0$. We set

$$\hat{g}_{vq^t}(x) := \begin{cases} e_t(x)^v & \text{if } v < q-1 \\ e_t(x)^{q-1} - D_t^{q-1} & \text{if } v = q-1. \end{cases}$$

We set $\hat{G}_{vq^t}(x) := \frac{\hat{g}_{vq^t}(x)}{D_t^v}$ for all v and t.

(2) Now let $c = \sum c_t q^t$ with $0 \leq c_t < q$ for all t. We set $\hat{g}_c(x) := \prod_t \hat{g}_{c_t q^t}(x)$ and $\hat{G}_c(x) := \prod_t \hat{G}_{c_t q^t}(x)$.

Remarks 2.17. Note that $G_j(x) = \frac{g_j(x)}{\Pi(j)}$ and $\hat{G}_j(x) = \frac{\hat{g}_j(x)}{\Pi(j)}$ for all j. Note also that both $\hat{g}_{(q-1)q^t}(x)$ and $\hat{G}_{(q-1)q^t}(x)$ vanish on all polynomials of degree t.

Proposition 2.18. *Let* $j = \sum c_t q^t$ *be as above.*

(1) *Let* $\zeta \in \mathbb{F}_q$. *Then* $\hat{g}_j(\zeta x) = \zeta^j \hat{g}_j(x)$ *and* $\hat{G}_j(\zeta x) = \zeta^j \hat{G}_j(x)$.

(2) *Let* $\alpha \in A$. *Then* $\hat{G}_j(\alpha) \in A$ *also.*

(3) *Let* m *be a positive integer. Then*

$$\frac{e_m(x)}{x} = \hat{g}_{q^m-1}(x).$$

Proof. Part (1) follows directly from the definitions. Part (2) follows from Proposition 2.14. Finally, by the remark just above, one sees that both $e_m(x)/x$ and $\hat{g}_{q^m-1}(x)$ are monic of the same degree and with the same zeroes; thus they are equal. $\qquad\square$

Proposition 2.19. *We have for* $j \geq 0$

$$\hat{g}_j(x+y) = \sum_{e+f=j} \binom{j}{e} g_e(x) \hat{g}_f(y) = \sum_{e+f=j} \binom{j}{e} \hat{g}_e(x) g_f(y),$$

and

$$\hat{G}_j(x+y) = \sum_{e+f=j} \binom{j}{e} G_e(x) \hat{G}_f(y) = \sum_{e+f=j} \binom{j}{e} \hat{G}_e(x) G_f(y).$$

Proof. The proof of Proposition 2.15 works here also. □

The following simple lemma is, of course, very well-known.

Lemma 2.20. *Let m be a positive integer. Then for any $0 \leq j \leq q^m - 1$, we have*

$$\binom{q^m - 1}{j} \equiv (-1)^j \pmod{p}.$$

Proof. Note that in characteristic p, $(1 + z)^{q^m - 1} = (1 + z)^{q^m}(1 + z)^{-1} = (1 + z^{q^m})(1 + z)^{-1}$. Now use the geometric series to expand $(1 + z)^{-1}$. □

As an immediate corollary, we obtain the next result.

Corollary 2.21. *Let m be a positive integer. We then have:*

(1) $g_{q^m-1}(x + y) = \displaystyle\sum_{e+f=q^m-1} (-1)^e g_e(x) g_f(y)$.

(2) $g_{q^m-1}(x - y) = \displaystyle\sum_{e+f=q^m-1} g_e(x) g_f(y)$.

(3) $G_{q^m-1}(x + y) = \displaystyle\sum_{e+f=q^m-1} (-1)^e G_e(x) G_f(y)$.

(4) $G_{q^m-1}(x - y) = \displaystyle\sum_{e+f=q^m-1} G_e(x) G_f(y)$.

Proof. Recall that $g_j(-y) = (-1)^j g_j(y)$ and $G_j(-y) = (-1)^j G_j(y)$ and the result follows immediately. □

The same argument immediately establishes the next essential result.

Corollary 2.22. *Let m be a positive integer. Then*

$$\hat{g}_{q^m-1}(x - y) = \sum_{e+f=q^m-1} g_e(x) \hat{g}_f(y) = \sum_{e+f=q^m-1} \hat{g}_e(x) g_f(y).$$

Let L be any field containing A and let $f(x) \in L[x]$ be a polynomial of degree d. Since $g_j(x)$ and $\hat{g}_j(x)$ have degree j in x, we deduce two expressions for $f(x)$ in terms of these polynomials:

$$(2.4) \qquad f(x) = \sum_{i=0}^{d} a_{f,i} g_i(x) = \sum_{i=0}^{d} \hat{a}_{f,i} \hat{g}_i(x).$$

We will now deduce two "integrals" (actually finite sums) for the coefficients $\{a_i\}$ and $\{\hat{a}_i(x)\}$.

Choose m such that $q^m > d$.

Theorem 2.23. *We have*

$$(2.5) \qquad (-1)^m \frac{D_m}{L_m} f(x) = \sum_{\alpha \in A_{<m}} f(\alpha) \frac{e_m(x)}{x - \alpha}.$$

Proof. Let $h(x)$ be the sum on the right hand side of (2.5). Note that since $e_m(\alpha) = 0$ for $\alpha \in A_{<m}$, we deduce $e_m(x)/(x - \alpha)$ is a polynomial in x of degree $q^m - 1$. Thus $h(x)$ has degree in x at most $q^m - 1$. Moreover, for $\alpha \in A_{<m}$ we have $h(\alpha) = f(\alpha)\frac{e_m(x)}{x-\alpha}|_{x=\alpha}$.

But

$$\frac{e_m(x)}{x - \alpha}|_{x=\alpha} = \frac{e_m(x - \alpha)}{x - \alpha}|_{x=\alpha} = \frac{e_m(x)}{x}|_{x=0}.$$

Moreover by Proposition 2.5, $\frac{e_m(x)}{x}|_{x=0} = (-1)^m \frac{D_m}{L_m}$. Now both $h(x)$ and $(-1)^m \frac{D_m}{L_m} f(x)$ are polynomials of degree at most $q^m - 1$ that agree on the q^m points in $A_{<m}$; thus they are equal. $\qquad\square$

Theorem 2.24. *Let $f(x)$ and $\{a_{f,i}\}$ be as in (2.4). Let $q^m > d$ where d is the degree of $f(x)$. Then we have*

$$(-1)^m \frac{D_m}{L_m} a_{f,i} = \sum_{\alpha \in A_{<m}} f(\alpha)\hat{g}_{q^m-1-i}(\alpha).$$

Proof. Theorem 2.23 assures us that

$$(-1)^m \frac{D_m}{L_m} f(x) = \sum_{\alpha \in A_{<m}} f(\alpha)\frac{e_m(x)}{x - \alpha} = \sum_{\alpha \in A_{<m}} f(\alpha)\frac{e_m(x - \alpha)}{x - \alpha}.$$

By the third part of Proposition 2.18 we can rewrite this last sum as

$$\sum_{\alpha \in A_{<m}} f(\alpha)\hat{g}_{q^m-1}(x - \alpha),$$

But by Corollary 2.22, we have

$$\hat{g}_{q^m-1}(x - \alpha) = \sum_{e+f=q^m-1} g_e(x)\hat{g}_f(\alpha).$$

The result follows upon collecting terms. $\qquad\square$

The same proof also gives the following *dual* result.

Theorem 2.25. *With the hypotheses of Theorem 2.24 we have*

$$(-1)^m \frac{D_m}{L_m} \hat{a}_{f,i} = \sum_{\alpha \in A_{<m}} f(\alpha)g_{q^m-1-i}(\alpha).$$

Our next result presents the compatibility between the various expressions for the coefficients given in Theorem 2.24.

Proposition 2.26. *Let $q^{m_1} > i$ and $q^{m_2} > i$. Then*

$$(2.6) \quad (-1)^{m_1} \frac{L_{m_1}}{D_{m_1}} \sum_{\alpha \in A_{<m_1}} \hat{g}_{q^{m_1}-1-i}(\alpha)f(\alpha)$$

$$= (-1)^{m_2} \frac{L_{m_2}}{D_{m_2}} \sum_{\alpha \in A_{<m_2}} \hat{g}_{q^{m_2}-1-i}(\alpha)f(\alpha).$$

Proof. Write i q-adically as $\sum_{t=0}^{e} c_t q^t$ with $c_e \neq 0$. We will show that both sides of (2.6) are equal to

$$(-1)^{e+1} \frac{L_{e+1}}{D_{e+1}} \sum_{\alpha \in A_{<e+1}} \hat{g}_{q^{e+1}-1-i}(\alpha)f(\alpha).$$

Without loss of generality, set $m = m_1$. Now, by definition, $\hat{g}_{q^m-1-i}(\alpha) = 0$ for all α of degree $> e$ and $< m$. Thus

$$(-1)^m \frac{L_m}{D_m} \sum_{\alpha \in A_{<m}} \hat{g}_{q^m-1-i}(\alpha)f(\alpha) = (-1)^m \frac{L_m}{D_m} \sum_{\alpha \in A_{<e+1}} \hat{g}_{q^m-1-i}(\alpha)f(\alpha).$$

Now notice that, by definition,

$$\hat{g}_{q^m-1-i}(\alpha) = (-1)^{m-e-1}(D_{e+1} \cdots D_{m-1})^{q-1}\hat{g}_{q^{e+1}-1-i}(\alpha).$$

The result follows upon noticing that $\Pi(q^m - 1) = \frac{D_m}{L_m}$. □

Remarks 2.27. The above compatibility formula, Proposition 2.26, has some important corollaries. In particular, we can give formulae for the coefficients $\{a_{f,j}\}$ which are independent of d. Indeed, let $f(x)$ be a polynomial of degree d, and write $f(x) = \sum_{i=1}^{d} a_{f,i}g_i(x)$, also as before. Let i be a fixed integer $\leq d$ which we write q-adically, as $\sum_{t=0}^{e} c_t q^t$ with $c_e \neq 0$ as above. Notice then the values of $f(x)$ on the points $x \in A_{<e}$ depends *only* on the truncation of the expansion of $f(x)$ given by $\sum_{i=0}^{q^{e+1}-1} a_{f,i}g_i(x)$ simply because the other elements in the sum vanish on these values. Proposition 2.26 implies that $a_{f,i} = (-1)^{e+1}\frac{L_{e+1}}{D_{e+1}} \sum_{\alpha \in A_{<e+1}} f(\alpha)\hat{g}_{q^{e+1}-1-i}(\alpha)$ which does *not* depend on d in any fashion. It does not appear possible to present similar formulae for the dual coefficients.

Next we present a formula for the coefficients $\{a_{f,i}\}$ and $\{\hat{a}_{f,i}\}$ that involves summing over monics of a given degree. We begin with an analog of Theorem 2.23. As before, let $f(x)$ be a polynomial of degree d and let m be chosen so that $q^m > d$.

Theorem 2.28. *With the above hypotheses, we have*

$$(2.7) \qquad (-1)^m \frac{D_m}{L_m}f(x) = \sum_{h \in A_{m,+}} f(h)\frac{e_m(x) - D_m}{x - h}.$$

Proof. The sum on the right of (2.7) is a polynomial of degree at most $q^m - 1$. As before we see that it, and $(-1)^m f(x)$, have the same values at the points in $A_{m,+}$. Thus they must be equal. □

Let $f(x)$ of degree d be written in terms of the $g_j(x)$ and their duals as in (2.4) and let $q^m > d$.

Theorem 2.29. *We have*

$$(-1)^m \frac{D_m}{L_m} a_{f,i} = \sum_{h \in A_{m,+}} f(h)\hat{g}_{q^m - 1 - i}(h),$$

and

$$(-1)^m \frac{D_m}{L_m} \hat{a}_{f,i} = \sum_{h \in A_{m,+}} f(h)g_{q^m - 1 - i}(h).$$

Proof. The result follows as before upon noting that, for $h \in A_{m,+}$, we have $e_m(x) - D_m = e_m(x - h)$. □

Expanding the Carlitz polynomial $g_j(x)$ leads to the following *orthogonality formulae*.

Theorem 2.30.

(1) *For $l < q^m$ and j arbitrary*

$$\sum_{\alpha \in A_{<m}} \hat{g}_l(\alpha)g_j(\alpha) = \begin{cases} 0 & \text{if } l + j \neq q^m - 1 \\ (-1)^m \frac{D_m}{L_m} & \text{if } l + j = q^m - 1. \end{cases}$$

(2) *For $l < q^m$, $j < q^m$*

$$\sum_{h \in A_{m,+}} \hat{g}_l(h)g_j(h) = \begin{cases} 0 & \text{if } l + j \neq q^m - 1 \\ (-1)^m \frac{D_m}{L_m} & \text{if } l + j = q^m - 1. \end{cases}$$

We now pass to the corresponding formulae for $G_i(x)$ and $\hat{G}_i(x)$ which are, in fact, simpler than those given for $g_i(x)$ and $\hat{g}_i(x)$.

Recall that in (2.4) we expressed a polynomial $f(x)$ in terms of both $\{g_i(x)\}$ and $\{\hat{g}_i(x)\}$ as

$$f(x) = \sum_{i=0}^d a_{f,i} g_i(x) = \sum_{i=0}^d \hat{a}_{f,i} \hat{g}_i(x).$$

We now write

$$(2.8) \qquad f(x) = \sum_{i=0}^d A_{f,i} G_i(x) = \sum_{i=0}^d \hat{A}_{f,i} \hat{G}_i(x).$$

From the definitions, we immediately conclude that

$$\Pi(i)a_{f,i} = A_{f,i} \quad \text{and} \quad \Pi(i)\hat{a}_{f,i} = \hat{A}_{f,i}.$$

Now recall that by Proposition 2.5 we have $\frac{D_m}{L_m} = \Pi(q^m - 1)$. But notice $\Pi(q^m - 1) = \Pi(i)\Pi(q^m - 1 - i)$. Thus from Theorem 2.24, Theorem 2.25, and Theorem 2.29, we obtain the next fundamental theorem.

Theorem 2.31. *With the hypotheses of Theorems 2.24, 2.25 and 2.29 we have:*

(1) $(-1)^m A_{f,i} = \sum_{\alpha \in A_{<m}} f(\alpha)\hat{G}_{q^m-1-i}(\alpha)$,

(2) $(-1)^m \hat{A}_{f,i} = \sum_{\alpha \in A_{<m}} f(\alpha)G_{q^m-1-i}(\alpha)$,

(3) $(-1)^m A_{f,i} = \sum_{h \in A_{m,+}} f(h)\hat{G}_{q^m-i-1}(h)$,

(4) $(-1)^m \hat{A}_{f,i} = \sum_{h \in A_{m,+}} f(h)G_{q^m-1-i}(h)$.

Corollary 2.32. *Both $\{G_i(x)\}$ and $\{\hat{G}_i(x)\}$ are bases for the A-module of elements $f(x) \in k[x]$ such that $f(\alpha) \in A$ for all $\alpha \in A$.*

Proof. Just express $f(x)$ using the theorem. $\qquad\square$

We leave the obvious orthogonality formulae for $G_i(x), \hat{G}_i(x)$, which follow immediately from Theorem 2.30 to the reader.

3. $\mathfrak{v}$-adic continuous functions

3.1. Basic notions. We begin with some notation that we will use throughout the paper. Let X, Y be two topological spaces. Then we denote the set of continuous functions $f\colon X \to Y$ by $\mathcal{C}(X, Y)$.

The binomial theorem implies that the binomial polynomials $\{\binom{s}{j}\}$ take the nonnegative integers to themselves as was mentioned above. Let p be a prime number. Since the p-adic integers, $\mathbb{Z}_p$, form a compact (and therefore closed) algebra, continuity implies that the binomial polynomials also map $\mathbb{Z}_p$ into itself. It is a fundamental result, due to K. Mahler, [12] that the set $\{\binom{s}{j}\}$ forms an *orthogonal basis* for the nonarchimedean Banach space $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. In this section we will briefly recall the theorem of C. G. Wagner [21] which establishes a similar result for the Carlitz polynomials.

In keeping with the theme of this paper, we will sketch a "modern" proof of this result following the excellent paper [6] by K. Conrad. We begin by recalling a well known result of J.-P. Serre [16]. Let $\{K, |\cdot|\}$ be a local field with ring of integers O (i.e., a finite extension of $\mathbb{Q}_p$ for some prime p or a formal Laurent series field over a finite field), and maximal ideal M. Let $(E, \|\cdot\|)$ be a Banach space over K and we assume that $\|\cdot\|$ and $|\cdot|$ have the same value group. We set $E_0 := \{x \in E\colon \|x\| \leq 1\}$, which is an O-module, and set $\bar{E} := E_0/ME_0$. Clearly $\bar{E}$ is a vector space over the field $\mathbb{F} := O/M$.

Examples 3.1.

(a) Let $E_c = \mathcal{C}(O, K)$ equipped with the norm

$$\|f\| := \sup_{x \in O}\{|f(x)|\}.$$

Clearly both E_c and K have the same value groups. Moreover, $E_{c,0} = \mathcal{C}(O, O) \subset \mathcal{C}(O, K)$ and thus $\bar{E}_{c,0} \simeq \mathcal{C}(O, \mathbb{F})$ where $\mathbb{F}$ has the discrete topology.

(b) Let K have positive characteristic and let $\mathbb{F}$ be its field of constants (and so we identify $\mathbb{F}$ and O/M in the usual fashion) where the cardinality of $\mathbb{F}$ is q. Let $E_l := \mathrm{Hom}_{\mathbb{F}}(O, K)$ be the $\mathbb{F}$-vector space of $\mathbb{F}$-linear, continuous functions from O to K equipped with the sup norm as in Part (a). Clearly E_l is a closed sub Banach space of E_c and one sees readily that $\bar{E}_{l,0} = \mathrm{Hom}_{\mathbb{F}}(O, \mathbb{F})$, the vector space of continuous $\mathbb{F}$-linear functions from O to $\mathbb{F}$ with $\mathbb{F}$ again having the discrete topology.

As usual, given E, as above, and a sequence $\mathfrak{E} := \{\mathfrak{e}_0, \mathfrak{e}_1, \ldots\}$ of elements of E, we say that $\mathfrak{E}$ is an *orthonormal basis* for E if and only if every $x \in E$ can be written $x = \sum_{i=0}^{\infty} c_i \mathfrak{e}_i$ with $\{c_i\} \subset K$, $c_i \to 0$ as $i \to \infty$ and $\|x\| = \sup_i\{|c_i|\}$. If $\mathfrak{E}$ is an orthonormal basis, a moment's reflection assures one that the above expansion for x is unique.

The following basic and well-known result is due to J.-P. Serre [16].

Lemma 3.2. *Let $\{K, E, \|\cdot\|\}$ be as in Part (a) of Examples 3.1. Let $\mathfrak{E} = \{\mathfrak{e}_0, \mathfrak{e}_1, \ldots\}$ be a sequence of elements in E. Then a necessary and sufficient condition for $\mathfrak{E}$ to be an orthonormal basis for E is that $\mathfrak{e}_i \in E_0$ for all i and the reductions $\{\bar{\mathfrak{e}}_i\} \subset \bar{E}$ form a basis for $\bar{E}$ as an $\mathbb{F}$-vector space.*

The import of Lemma 3.2 is that it allows us to find orthonormal bases for a Banach space E by finding vector space bases of $\bar{E}$.

3.2. The basic construction. Let K be our local field of characteristic $p > 0$ and let $E_c = \mathcal{C}(O, K)$ all as in Examples 3.1. Let $q = p^{n_0}$ be the order of $\mathbb{F}$ and let $\mathfrak{E} = \{\mathfrak{e}_0, \mathfrak{e}_1 \ldots\}$ be an orthonormal basis for E_l. Our next definition is based on the construction of the Carlitz polynomials given in Definition 2.13.

Definition 3.3. Let j be a nonnegative integer written q-adically as $j = \sum_{t=0}^{\alpha} c_t q^t$ with $0 \leq c_t < q$ all t. We set $\mathfrak{g}_j := \prod_{t=0}^{\alpha} \mathfrak{e}_t^{c_t}$ and we put $\mathfrak{G} = \{\mathfrak{g}_j\}$.

We say that $\mathfrak{G}$ is *the extension of $\mathfrak{E}$ via q-adic digits*.

The next basic result is due to Conrad [6].

Theorem 3.4. *With the above definitions, $\mathfrak{G}$ is an orthonormal basis for $E_c = \mathcal{C}(O, K)$.*

Sketch of proof. Note first that by continuity $\mathcal{C}(O, \mathbb{F}) = \varinjlim \operatorname{Maps}(O/M^j, \mathbb{F})$ and $\operatorname{Hom}_{\mathbb{F}}(O, \mathbb{F}) = \varinjlim \operatorname{Hom}_{\mathbb{F}}(O/M^j, \mathbb{F})$ where O/M^j has the discrete topology.

Now let $\mathfrak{E} = \{\mathfrak{e}_0, \mathfrak{e}_1, \ldots\}$ be our orthonormal basis for $\operatorname{Hom}_{\mathbb{F}}(O, K)$ with reductions $\bar{\mathfrak{e}}_i$ and set $H_i = \cap_{c=0}^{i} \ker \bar{\mathfrak{e}}_c$; one sees readily that H_i has codimension i. Since the $\{H_i\}$ give a basis for the topology at the origin in O, we further deduce that $\mathcal{C}(O, \mathbb{F}) = \varinjlim \operatorname{Maps}(O/H_i, \mathbb{F})$ and $\operatorname{Hom}_{\mathbb{F}}(O, \mathbb{F}) = \varinjlim \operatorname{Hom}_{\mathbb{F}}(O/H_i, \mathbb{F})$.

We are thus reduced to the following combinatorial problem: Let V be a vector space over $\mathbb{F}$ of dimension n and let ϕ_i be a basis for the dual space of V. Let Φ be the set of functions on V created out of $\{\phi_i\}$ via digit expansions (as above) for $0 < j < q^n - 1$. We need to show that Φ is then an $\mathbb{F}$-basis for $\operatorname{Maps}(V, \mathbb{F})$. It is sufficient to show that Φ spans $\operatorname{Maps}(V, \mathbb{F})$. To see this, let $v \in V$. Then Conrad explicitly constructs an element h_v in $\operatorname{Span}(\Phi)$ with the property that $h_v(v) = 1$ but $h_v(w) = 0$ for $w \neq v$. These elements clearly span all maps from V to $\mathbb{F}$ and the proof is complete. $\square$

We also have the following generalization of the above theorem which is established in a similar fashion.

Theorem 3.5. *Let K, $\mathbb{F}$ be as above and let $\mathbb{F}_0 \subseteq \mathbb{F}$ be a subfield of cardinality q_0 (so that $q = q_0^{n_0}$). Let $\mathfrak{E} = \{\mathfrak{e}_0, \mathfrak{e}_1, \ldots\}$ be an orthonormal basis of $\operatorname{Hom}_{\mathbb{F}_0}(O, K)$ such that $\cap_{j=0}^{in_0 - 1} \ker \bar{\mathfrak{e}}_j$ has codimension in_0 for all $i \geq 1$. Let $\mathfrak{G}$ be the extension of $\mathfrak{E}$ using q_0-adic digits. Then $\mathfrak{G}$ is an orthonormal basis for $\mathcal{C}(O, K)$.*

3.3. Applications to *v*-adic continuous functions.
We now return to the case of the Carlitz polynomials of Subsection 2.2 and use the results of the previous subsection to obtain orthonormal bases.

As in Subsection 2.2 we let $A = \mathbb{F}_q[\theta]$ and $k = \mathbb{F}_q(\theta)$. Let $K = k_{(\theta)}$ be the completion of k at the prime (θ) and let $O \subset K = \mathbb{F}_q[\![\theta]\!]$ be the ring of integers. Let $\{e_t(x)\}$ be as in Definition 2.11 and set $\mathfrak{E} := \{e_t(x)/D_t\}$.

Proposition 3.6. *The set $\mathfrak{E}$ forms an orthonormal basis for $\operatorname{Hom}_{\mathbb{F}_q}(O, K)$.*

Proof. By Lemma 3.2, it suffices to show that the reductions $\{\overline{e_t(x)/D_t}\}$ form a vector space basis of the continuous $\mathbb{F}_q$-linear maps from O to $\mathbb{F}_q$ equipped with the discrete topology. Notice that $e_t(x)/D_t$ vanishes at θ^i for $i < t$ and $e_t(\theta^t)/D_t = 1$. Thus $\{e_i(x)/D_i\}_{i=0}^{t-1}$ forms a basis for the dual of $\mathbb{F}_q[\![\theta]\!]/(\theta^t)$ and the result is established. $\square$

Let $\mathfrak{G} := \{G_j(x)\}$ where $G_j(x)$ is the Carlitz polynomial of Definition 2.13.

Corollary 3.7. *The Carlitz polynomials $\mathfrak{G}$ form an orthonormal basis for $\mathcal{C}(O, K)$.*

Proof. This is exactly the content of Theorem 3.4. □

Let $\mathfrak{v}$ now be any prime of A with completions $O := A_{\mathfrak{v}}$ and $K = k_{\mathfrak{v}}$. Very similar arguments give the following essential result.

Theorem 3.8. *The sequence $\mathfrak{E}$ forms an orthonormal basis for the space* $\mathrm{Hom}_{\mathbb{F}_q}(O, K)$. *The sequence $\mathfrak{G}$ forms an orthonormal basis for $\mathcal{C}(O, K)$.*

Theorem 3.8 is the direct analog of Mahler's theorem for binomial coefficients.

Let $\hat{\mathfrak{G}}$ be the sequence of dual Carlitz polynomials of Definition 2.16.

Corollary 3.9. *The sequence $\hat{\mathfrak{G}}$ is an orthonormal basis for $\mathcal{C}(O, K)$.*

Proof. Notice that $G_t(x)$ and $\hat{G}_t(x)$ have the same degree and both sets of polynomials are bases for the space of A-valued polynomials with coefficients in k. Thus the result follows from Lemma 3.2 and Theorem 3.8. □

Let $f \in \mathcal{C}(O, K)$. By Corollaries 3.7 and 3.9 we can write

$$f(x) = \sum_{i=0}^{\infty} A_{f,i} G_i(x) = \sum_{i=0}^{\infty} \hat{A}_{f,i} \hat{G}_i(x) \,,$$

as in (2.8) with the coefficients tending to 0 as i goes to infinity.

Write i q-adically as $\sum_{t=0}^{e} c_t q^e$ with $0 \leq c_t < q$ all t and $c_e \neq 0$. Then the discussion of Remarks 2.27 immediately gives the next result.

Proposition 3.10. *We have*

$$(-1)^{e+1} A_{f,i} = \sum_{\alpha \in A_{<e+1}} f(\alpha) \hat{G}_{q^{e+1}-1-i}(\alpha) \,.$$

As remarked before there is no obvious analog of Proposition 3.10 for the dual coefficients.

4. Measure theory

The previous section has equipped us with a good description of continuous functions on the completions of A. Here we will use that to give a dual description of the algebra of measures on these completions. We begin by recalling the corresponding theory of p-adic measures on subsets of $\mathbb{Z}_p$.

4.1. Distributions and measures. Let X be any compact open subset of the p-adic numbers such as $\mathbb{Z}_p$ or $\mathbb{Z}_p^*$.

Definition 4.1. A p-adic distribution ν on X is a finitely additive $\mathbb{Q}_p$-valued function on the compact-open subsets of X.

More precisely, let $\{U_1, \ldots, U_m\}$ be a collection of pair-wise disjoint compact-open subsets of X. Then we have

$$\mu \left(\bigcup_{j=1}^{m} U_j \right) = \sum_{j=1}^{m} \mu(U_j) \,.$$

Definition 4.2. Let μ be a p-adic distribution. If the values $\mu(U) \in \mathbb{Q}_p$ are bounded for all compact-open subsets $U \subset X$ (i.e., all such values lie in a compact subset of $\mathbb{Q}_p$), then we say that μ is a *p-adic measure*.

Example 4.3. Let $\alpha \in X$ and let $U \subseteq X$ be a compact-open. We define

$$\delta_\alpha(U) = \begin{cases} 1, & \text{if } \alpha \in U \\ 0, & \text{otherwise} \,. \end{cases}$$

Clearly δ_α is a measure called the *Dirac measure at α*.

4.2. Integration. Let μ be a measure on X as in our previous subsection and let $f \colon X \to \mathbb{Q}_p$ be a continuous function. For each $a + p^j \mathbb{Z}_p \subseteq X$ choose a point $x_{a,j} \in a + p^j \mathbb{Z}_p$ and let $X_j := \{x_{a,j}\}$. We can then form the *Riemann sum*

$$S_{X_j} := \sum_{a + p^j \mathbb{Z}_p \subseteq X} f(x_{a,j}) \mu(a + p^j \mathbb{Z}_p) \,.$$

Recall that, as X is compact, every continuous function on X is automatically uniformly continuous. Using this, one can directly prove the next basic result.

Theorem 4.4. *As $j \to \infty$, the Riemann sums converge to an element $\int_X f(x) \, d\mu(x) \in \mathbb{Q}_p$ which does not depend upon the choice of X_j.*

Examples 4.5.

(a) Let $\alpha \in X$ and let δ_α be the Dirac measure at α. Then

$$\int_X f(x) \, d\delta_\alpha(x) = f(\alpha) \,.$$

(b) Let $U \subseteq X$ be a compact open with characteristic function 1_U (with values 1 on U and 0 elsewhere). Note that 1_U is continuous on all of X and that $\int_X 1_U \, d\mu(x) = \mu(U)$.

For now we restrict $X = \mathbb{Z}_p$. Let $f \colon \mathbb{Z}_p \to \mathbb{Q}_p$ be a continuous function. As mentioned above, the classical Theorem of Mahler tells us that $f(x)$ may be expressed as

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i} \,,$$

where $\{a_i\} \subset \mathbb{Q}_p$ and $a_i \to 0$ as $i \to \infty$. Let μ be a measure on $\mathbb{Z}_p$ and let B_μ be an upper bound for $|\mu(U)|$ where U runs over the compact-open subsets of X. One easily checks that

$$\left| \int_{\mathbb{Z}_p} f(x)\,\mathrm{d}\mu(x) \right| \le B_\mu \|f\|.$$

Now put for all $i \ge 0$

$$v_{\mu,i} := \int_{\mathbb{Z}_p} \binom{x}{i} \mathrm{d}\mu(x),$$

and notice that $\{v_{\mu,i}\}$ is bounded since one knows, by Mahler, that $\{\binom{x}{i}\}$ is an orthonormal basis for the Banach space of continuous functions. We therefore deduce that

$$\int_{\mathbb{Z}_p} f(x)\,\mathrm{d}\mu(x) = \sum_{i=0}^{\infty} a_i v_{\mu,i},$$

which converges as $a_i \to 0$ as $i \to \infty$. Conversely, let $V := \{v_i\} \in \mathbb{Q}_p$ be a bounded sequence. Set $\int_{\mathbb{Z}_p} f(x)\,\mathrm{d}\mu_V(x) := \sum_i a_i v_i$. As the characteristic functions of compact open subsets are continuous on all of $\mathbb{Z}_p$ and the locally constant functions are dense in $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$, we obtain a measure by setting $\mu_V(U) = \int 1_U \,\mathrm{d}\mu_V(u)$. We thus obtain the next result.

Proposition 4.6. *The mapping $\mu \mapsto \{\int \binom{x}{i} \mathrm{d}\mu(x)\}$ is a vector space isomorphism between the space of $\mathbb{Q}_p$-valued measures and the vector space of bounded sequences $\{v_i\}_{i=0}^{\infty}$.*

Note that as the locally constant functions are dense in the space of continuous functions, if μ is a $\mathbb{Q}_p$-valued measure and $f \colon X \to \mathbb{Q}_p$ is continuous then $f(x)\mu(x)$ is also a $\mathbb{Q}_p$-valued measure.

4.3. Convolutions. We continue with the p-adic set-up of the previous two subsections and we now restrict to having $X = \mathbb{Z}_p$. Let μ and ν be two $\mathbb{Q}_p$-valued measures on X.

Definition 4.7. We define the convolution $\mu * \nu$ of μ and ν by

$$\int_{\mathbb{Z}_p} f(x)\,\mathrm{d}\mu * \nu(x) := \int_{\mathbb{Z}_p} \int_{\mathbb{Z}_p} f(x+y)\,\mathrm{d}\mu(x)\,\mathrm{d}\mu(y),$$

for continuous $\mathbb{Q}_p$-valued functions on $\mathbb{Z}_p$.

One checks readily that the convolution of two measures is also a measure and that with this definition the vector space $\mathcal{M}_{\mathbb{Z}_p, \mathbb{Q}_p}$ of $\mathbb{Q}_p$-valued measures on $\mathbb{Z}_p$ forms a $\mathbb{Q}_p$-algebra. We want to identify this algebra. The first thing to notice is that $\mathcal{M}_{\mathbb{Z}_p, \mathbb{Q}_p} = \mathcal{M}_{\mathbb{Z}_p, \mathbb{Z}_p} \otimes \mathbb{Q}_p$ where the latter is the space of $\mathbb{Z}_p$-valued measures on $\mathbb{Z}_p$.

Let T be an indeterminate and $\mathbb{Z}_p[\![T]\!]$ be the formal power series algebra in T.

Definition 4.8. Let $\mu \in \mathcal{M}_{\mathbb{Z}_p,\mathbb{Z}_p}$. We define the *Mahler transform* $T_M(\mu) \in \mathbb{Z}_p[\![T]\!]$ of μ by

$$T_M(\mu) := \int_{\mathbb{Z}_p} (1+T)^x \, \mathrm{d}\mu(x) := \sum_{i=0}^{\infty} \left(\int_{\mathbb{Z}_p} \binom{x}{i} \mathrm{d}\mu(x) \right) T^i \,.$$

Proposition 4.9. *The Mahler transform T_M is an algebra isomorphism between $\mathcal{M}_{\mathbb{Z}_p,\mathbb{Z}_p}$ and $\mathbb{Z}_p[\![T]\!]$.*

Proof. This follows from the definition of the convolution product and the addition formula for binomial coefficients. Indeed, the addition formula precisely corresponds, via convolution, to the product of the associated power series. □

Let $t_M \colon \mathbb{Z}_p[\![T]\!] \to \mathcal{M}_{\mathbb{Z}_p,\mathbb{Z}_p}$ be the inverse of T_M.

Proposition 4.10. *Let $g(T) \in \mathbb{Z}_p[\![T]\!]$ and put $\mu_g = t_M(g)$. We then have for $k \geq 0$*

$$T_M(x^k \mu_g) = D^k g(T) \,,$$

where D is the continuous operator $(1+T)\frac{\mathrm{d}}{\mathrm{d}T}$ on $\mathbb{Z}_p[\![T]\!]$.

Proof. Note that $D^k(1+T)^x = x^k(1+T)^x$. Now by definition we have

$$\int_{\mathbb{Z}_p} (1+T)^x \, \mathrm{d}\mu_g(x) = g(T) \,.$$

Now applying D^k gives

$$\int_{\mathbb{Z}_p} D^k(1+T)^x \, \mathrm{d}\mu_g(x) = D^k g(T) \,,$$

or

$$\int_{\mathbb{Z}_p} (1+T)^x \, x^k \, \mathrm{d}\mu_g(x) = D^k g(T) \,.$$

and the result follows. □

Proposition 4.10 is obviously the analog of well-known results in the classical Fourier transform.

4.4. The $\mathfrak{v}$-adic theory. We now return to the case where $A = \mathbb{F}_q[\theta]$ and $\mathfrak{v}$ is a prime of A with completion $A_{\mathfrak{v}}$. Let X now be a compact open subset of $A_{\mathfrak{v}}$. The basic definitions of $\mathfrak{v}$-adic measures etc., on X follow directly *mutatis mutandis* from the theory of Subsections 4.1 and 4.2. We therefore focus here on the $\mathfrak{v}$-adic version of Subsection 4.3.

Therefore let $X = A_{\mathfrak{v}}$ and let $f\colon A_{\mathfrak{v}} \to k_{\mathfrak{v}}$ be a continuous function. By the theorem of Wagner, Corollary 3.7, we have an expression

$$f(x) = \sum_{i=0}^{\infty} a_j G_j(x)\,,$$

where $\{a_j\} \subset k_{\mathfrak{v}}$ and $a_j \to 0$ as $j \to \infty$. If μ is a $\mathfrak{v}$-adic measure then μ is determined by the bounded sequence $\{\int_{A_{\mathfrak{v}}} G_j(x)\,\mathrm{d}\mu(x)\}_{j=0}^{\infty}$. Conversely any such bounded sequence determines a $\mathfrak{v}$-adic measure. Under convolution of measures, such sequences form a $k_{\mathfrak{v}}$-algebra denoted $\mathcal{M}_{A_{\mathfrak{v}},k_{\mathfrak{v}}}$ and we would like to identify this algebra. As in the p-adic case, we immediately reduce to identifying the algebra $\mathcal{M}_{A_{\mathfrak{v}},A_{\mathfrak{v}}}$ of $A_{\mathfrak{v}}$-valued measures on $A_{\mathfrak{v}}$.

Let $\left\{\frac{u^i}{i!}\right\}_{i=0}^{\infty}$ be the divided power elements. These are formal symbols with the usual multiplication rule

$$\frac{u^i}{i!} \cdot \frac{u^j}{j!} := \binom{i+j}{i}\frac{u^{i+j}}{(i+j)!} = \binom{i+j}{j}\frac{u^{i+j}}{(i+j)!}\,,$$

so that the multiplication is well defined in any characteristic.

Definition 4.11. We define $A_{\mathfrak{v}}\{\{u\}\}$ to be the algebra of formal divided power series

$$\sum_{i=0}^{\infty} a_i \frac{u^i}{i!}$$

with the obvious addition and with multiplication given above.

Definition 4.12. Let $\mu \in \mathcal{M}_{A_{\mathfrak{v}},A_{\mathfrak{v}}}$. We set

$$T_W(\mu) := \sum_{j=0}^{\infty} \left(\int_{A_{\mathfrak{v}}} G_j(x)\,\mathrm{d}\mu(x)\right)\frac{u^j}{j!} \in A_{\mathfrak{v}}\{\{u\}\}\,.$$

We call $T_W(\mu)$ the *Wagner transform* of μ.

The addition formula for $G_j(x)$ given in Proposition 2.15 immediately gives our next result which is the analog of Proposition 4.9.

Proposition 4.13. *The Wagner transform* $T_W\colon \mathcal{M}_{A_{\mathfrak{v}},A_{\mathfrak{v}}} \to A_{\mathfrak{v}}\{\{u\}\}$ *is an algebra isomorphism.*

Remarks 4.14.
  (a) The present author had used the addition formula to calculate the convolution of measures which Greg Anderson realized was isomorphic to the algebra of formal divided series.
  (b) There is another equivalent representation of the above algebra. Let $R = A_{\mathfrak{v}}[z]$ be the polynomial ring in z. Let $\partial_j = \partial_{z,j}\colon R \to R$ be the *j-divided derivative* operator defined, as usual, by $\partial_j z^i := \binom{i}{j}z^{i-j}$.

Note that $\partial_i \partial_j = \binom{i+j}{i} \partial_{i+j}$. Let $A_{\mathfrak{v}}\{\{\partial\}\}$ be the algebra of formal divided derivatives formed in the obvious fashion (which obviously acts on R). One then readily sees that $A_{\mathfrak{v}}\{\{\partial\}\}$ is isomorphic to $A_{\mathfrak{v}}\{\{u\}\}$.

Definition 4.15. Let $f \in \mathcal{C}(A_{\mathfrak{v}}, k_{\mathfrak{v}})$ and let $\mu \in \mathcal{M}_{A_{\mathfrak{v}}, k_{\mathfrak{v}}}$. we set

$$\mu * f(x) := \int_{A_{\mathfrak{v}}} f(x+y) \, \mathrm{d}\mu(y) \in \mathcal{C}(A_{\mathfrak{v}}, k_{\mathfrak{v}}) \,.$$

As in [9], we can now present an analog of Proposition 4.10 in the finite characteristic theory. Let z be a variable, as above, and let $k_{\mathfrak{v}}\langle\langle z \rangle\rangle$ be the *Tate algebra* of $k_{\mathfrak{v}}$ power series $\sum_i a_i z^i$ where $a_i \in k_{\mathfrak{v}} \to 0$ as $i \to \infty$. Such power series converge on those $z \in k_{\mathfrak{v}}$ with $\mathfrak{v}$-adic absolute value $|z|_{\mathfrak{v}} \leq 1$ (i.e., $z \in A_{\mathfrak{v}}$). The algebra $A_{\mathfrak{v}}\{\{\partial\}\}$ acts on $k_{\mathfrak{v}}\langle\langle z \rangle\rangle$ in the natural fashion.

Definition 4.16. Let $z \in A_{\mathfrak{v}}$ and let μ_z be the measure whose Wagner transform is $\sum_i z^i \frac{u^i}{i!}$. If $f \in \mathcal{C}(A_{\mathfrak{v}}, k_{\mathfrak{v}})$ we set

$$\hat{f}(z) := \int_{A_{\mathfrak{v}}} f(t) \, \mathrm{d}\mu_z(t) \in k_{\mathfrak{v}}\langle\langle z \rangle\rangle \,.$$

Thus if $f(x) = \sum a_i G_i(x)$ then $\hat{f}(z) = \sum a_i z^i$. Moreover, the map $f \mapsto \hat{f}$ is a Banach space isomorphism between $\mathcal{C}(A_{\mathfrak{v}}, k_{\mathfrak{v}})$ and $k_{\mathfrak{v}}\langle\langle z \rangle\rangle$.

Finally, by a small abuse of notation, let us also denote by "$\frac{u^i}{i!}$" the measure whose Wagner transformation is $\frac{u^i}{i!}$. The following, which is an analog of Proposition 4.10, also follows directly from the addition formula in Proposition 2.15.

Proposition 4.17. *Let f be a continuous $k_{\mathfrak{v}}$-valued function on $A_{\mathfrak{v}}$. With the above definitions, we have*

$$\widehat{\frac{u^i}{i!} * f} = \partial_i \hat{f} \,.$$

In other words, convolution transforms into differentiation.

Remarks 4.18. The very important work of B. Anglès, F. Pellarin and others (see [3] for instance) uses Tate algebras in many variables $t_1, \ldots, t_m$ to study L-series, where m can be an arbitrary positive integer and this suggests that one might need a multi-variable transform. On the other hand, while we have not stressed it here, it is well-known that the convolution algebra of p-adic measures on $\mathbb{Z}_p$ is isomorphic to the completed group algebra $\mathbb{Z}_p[\![\mathbb{Z}_p]\!]$. Similarly the algebra of $\mathfrak{v}$-adic measures on $A_{\mathfrak{v}}$ is isomorphic to the completed group ring $A_{\mathfrak{v}}[\![A_{\mathfrak{v}}]\!]$, etc.

However, as a topological group $A_{\mathfrak{v}}$ is isomorphic to the infinite product of $\mathbb{F}_q$ with itself equipped with the product topology. As such, $A_{\mathfrak{v}}$ is therefore isomorphic to $A_{\mathfrak{v}}^m$ as topological groups, and this isomorphism

clearly extends to the complete group rings. This *suggests*, therefore, that one should be able to construct versions of Propositions 4.13 and 4.17 for many variables $\{z_1, \ldots, z_m\}$ and probably in many different ways.

5. *L*-series

In this section we review the definitions of *L*-series for $A = \mathbb{F}_q[\theta]$, and $k = \mathbb{F}_q(\theta)$. Let ∞ be the infinite prime of k with normalized absolute value $|?|_\infty$ and completion k_∞. We set $\mathbb{C}_\infty$ to be the completion of a fixed algebraic closure $\bar{k}_\infty$ equipped with the canonical extension of $|?|_\infty$.

5.1. Exponentiation. In order to define exponentiation of elements, we must begin with a notion of "positivity" in k_∞. Let $\pi \in k_\infty$ with $|\pi|_\infty = 1$. Let $x \in k_\infty^*$ be expressed as $\sum_{i=e}^{\infty} c_i \pi^i$ where $\{c_e\} \subseteq \mathbb{F}_q$, e is an integer (positive, negative or 0), and $c_e \neq 0$.

Definition 5.1. We set $\mathrm{sgn}(x) := c_e$ and say that x is *positive* (or monic) if and only $c_e = 1$ We call $-e$ the *degree* of x and denote it $\deg x$.

Remarks 5.2.
  (1) It is easy to see that sgn is a homomorphism from $k_\infty^* \to \mathbb{F}_q{}^*$ which is the identity on $\mathbb{F}_q{}^*$ and 1 on principal units (elements of the form $1 + c\pi + \cdots$, with $c \in \mathbb{F}_q$). This mapping sgn is called a *sign function*.
  (2) Conversely given a homomorphism sgn as in Part (1), we deduce an associated notion of positivity.
  (3) Notice that the positive elements $k_{\infty,+}$ form a subgroup of k_∞^*, but are obviously not closed under addition.
  (4) The notion of degree given above agrees with the usual notion of degree in A.

Convention. For simplicity we now fix the unique sign function sgn with $\mathrm{sgn}\, \theta = 1$.

Definition 5.3. We let $\pi \in k_\infty$ be a fixed positive uniformizing element at ∞.

As an example, one could choose $\pi := 1/\theta$; in general, of course, $|\pi|_\infty = |1/\theta|_\infty$.

Let $\alpha \in k_{\infty,+}$. With the above definitions we then deduce a canonical decomposition

$$(5.1) \qquad \alpha = \pi^{-\deg \alpha} \langle \alpha \rangle,$$

where $\langle \alpha \rangle \equiv 1 \pmod{\pi}$. Of course $\langle \alpha \rangle$ depends on π but we shall not explicitly mention this for simplicity once π is chosen.

Now let $s = (x, y)$ where $x \in \mathbb{C}_\infty^*$, and $y \in \mathbb{Z}_p$.

Definition 5.4. We set

$$\alpha^s := x^{\deg \alpha} \langle \alpha \rangle^y \,,$$

where $\langle \alpha \rangle^y$ is defined, as usual, via the binomial theorem.

The elements s form a group under the obvious definitions whose operation will be written additively. One then sees that, as usual, $(\alpha\beta)^s = \alpha^s \beta^s$ and $\alpha^{s_0+s_1} = \alpha^{s_0} \alpha^{s_1}$.

Definition 5.5. We set $\mathbb{S}_\infty := \mathbb{C}_\infty^* \times \mathbb{Z}_p$ with the obvious structure as a topological additive group.

Remarks 5.6. Let $i \in \mathbb{Z}$ and set $s_i := (1/\pi^i, i) \in \mathbb{S}_\infty$. Let $\alpha \in k_{\infty,+}$. Then by definition one sees that $\alpha^{s_i} = \alpha^i$ where α^i has its usual meaning.

Definition 5.7. We call a formal sum $L(s) := \sum_{a \in A_+} c_a a^{-s}$, where $\{c_a\} \subset \mathbb{C}_\infty$ and $s \in \mathbb{S}_\infty$ a *Dirichlet series*.

The convergence properties of such a Dirichlet series $L(s)$ are determined by the $x \in \mathbb{C}_\infty^*$ coordinate. In practice one ends up with a family of entire power series in x^{-1} which is continuous on all of $\mathbb{S}_\infty$; see, for example, [8, Section 8] or [9] for more details.

Example 5.8. We set $\zeta_A(s) := \sum_{a \in A_+} a^{-s}$ and call it the *zeta function of A*. It is a standard exercise to express $\zeta_A(s)$ as an Euler product over all the monic irreducible elements in A.

Let $L(s) = \sum_{a \in A_+} c_a a^{-s}$ be a Dirichlet series. By definition we have

$$L(s) = \sum_{d=0}^{\infty} x^{-d} \left(\sum_{\deg a = d} c_a \langle a \rangle^{-y} \right)$$

where $s = (x, y) \in \mathbb{S}_\infty$. The convergence properties of $L(s)$ are then determined by the convergence properties of the above family of power series in x^{-1}. In all known cases, these power series are shown to be entire.

Remarks 5.9.

   (a) Our theory starts with a choice of a positive uniformizer π_0. Given another uniformizer π_1, clearly $u = \pi_1/\pi_0$ is a 1-unit at ∞. Conversely, given a 1-unit u the element $u\pi_0$ is another positive uniformizer. Moreover $\pi_1^{\deg \alpha} \alpha = (\pi_1/\pi_0)^{\deg \alpha} \pi_0^{\deg \alpha} \alpha$ so that the "gauge" π_1/π_0 tells us how to pass between the various choices of positive uniformizer [10].
   (b) The general theory of Drinfeld modules is defined for all rings A given as the algebra of regular functions outside a fixed point ∞ on a smooth projective geometrically connected curve over $\mathbb{F}_q$. In this case, just exponentiating elements is not sufficient but in fact

our definitions may be readily extended to exponentiating general nonzero ideals of A, see for instance [10].

5.2. A generalization due to B. Anglès. We briefly present here a remarkable generalization of the zeta function of Example 5.8 recently communicated to us by Anglès [1] (see also [2]) which we follow rather closely with his permission.

Therefore let F be a field containing $\mathbb{F}_q$ which is complete for a valuation $v\colon F \to \mathbb{R} \cup \{+\infty\}$.

Definition 5.10. Let n be a positive integer. We set

$$\mathbb{S}_{F,n} := F^* \times \mathbb{Z}_p^n\,,$$

with the obvious structure as an additive topological group.

Clearly $\mathbb{S}_{\mathbb{C}_\infty,1} = \mathbb{S}_\infty$ where the latter is defined in Definition 5.5.

Now let t be a variable and put $\mathcal{A} := \mathbb{F}_q[t]$ with $\mathcal{A}_+$ being the subset of monics and $\mathcal{A}_{+,d}$ being those of degree d. Mimicking our earlier constructions for $A = \mathbb{F}_q[\theta]$ (and $\pi = 1/\theta$) for $a(t) \in \mathcal{A}_+$

$$\langle a \rangle = t^{-\deg a} a\,.$$

Definition 5.11.

(a) Let $\{z_1, \ldots, z_n\} \subset F$ with $v(z_i) < 0$ for all i (so that $\langle a(z_i) \rangle = \langle a \rangle|_{t=z_i}$ converges to an element of F). Let $s = (x, y_1, \ldots, y_n) \in \mathbb{S}_{F,n}$. We set

$$a^s(z_1, \ldots, z_n) = x^{\deg a} \langle a(z_1) \rangle^{y_1} \cdots \langle a(z_n) \rangle^{y_n}\,.$$

(b) We set

$$\zeta(s)(z_1, \ldots, z_n) := \sum_{a \in \mathcal{A}_+} a^{-s}(z_1, \ldots, z_n)\,.$$

Example 5.12. With $F = \mathbb{C}_\infty$, $n = 1$, and $z_1 = \theta$, we recover $\zeta_A(s)$.

Notice that by definition $\zeta(s)(z_1, \ldots, z_n)$ converges for all s with $v(x) < 0$ (as before). Note also that we have

$$\zeta(s)(z_1, \ldots, z_n) = \sum_{d \geq 0} x^{-d} \left(\sum_{a \in \mathcal{A}_{+,d}} \langle a(z_1) \rangle^{-y_1} \cdots \langle a(z_n) \rangle^{-y_n} \right).$$

Proposition 5.13. *The function $\zeta(s)(z_1, \ldots, z_n)$ converges (in F) for all $s \in \mathbb{S}_{F,n}$.*

Proof. Let $\{t_1, \ldots, t_j\}$ be $j \geq 1$ indeterminates. Standard estimates ([8, Chapter 8]) show that for $k < d(q-1)$ we have $\sum_{a \in A_{+,d}} \prod_{i=1}^{k} a(t_i) = 0$ (which is sometimes referred to as *Simon's Lemma*). Notice, of course, that we are free to substitute $t_i^{q^{e_i}}$ for t_i. Now let $m = \sum_i c_i q^i$ be a positive integer

written q-adically (so that $0 \le c_i < q$ all i) with $\ell_q(m) := \sum_i c_i$ the sum of its q-adic digits. We then conclude that if $m_1, \ldots, m_n$ are positive integers with $\sum_{i=1}^n \ell_q(m_i) < d(q-1)$ then

$$(5.2) \qquad \sum_{a \in \mathcal{A}_{+,d}} a(z_1)^{m_1} \cdots a(z_n)^{m_n} = 0 \,.$$

Now let $\{y_i\}_{i=1}^n \subset \mathbb{Z}_p$ and express $-y_i$ q-adically as $-y_i = \sum_j u_{i,j} q^j$

Pick a positive integer l and write $-y_i = m_i + r_i$ where $m_i = \sum_{j=0}^l u_{i,j} q^j$. Notice that

$$\langle a(z_i) \rangle^{r_i} = c z_i^{-q^{l+1}} + \{\text{higher terms}\} \,,$$

where $c \in \mathbb{F}_q$. Note also that $\ell_q(m_i) \le (l+1)(q-1)$ so that $\sum \ell_q(m_i) \le n(l+1)(q-1)$. Thus, using the definition of $\langle a(t) \rangle$ and (5.2), we conclude that

$$\sum_{a \in A_{+,d}} \langle a(z_1) \rangle^{m_1} \cdots \langle a(z_n) \rangle^{m_n} = 0$$

for d such that $n(l+1)(q-1) < d(q-1)$ or $d > (l+1)n$. Moreover in this case we conclude that

$$v \left(\sum_{a \in \mathcal{A}_{+,d}} \langle a(z_1) \rangle^{-y_1} \cdots \langle a(z_n) \rangle^{-y_n} \right) \ge q^{l+1} \inf\{-v(z_i)\} \,.$$

Let $[x]$ be the greatest integer of a real number x and choose l so that $l = [d/n] - 2$ (which ensures $d > (l+1)n$). We then conclude

$$v \left(\sum_{a \in \mathcal{A}_{+,d}} \langle a(z_1) \rangle^{-y_1} \cdots \langle a(z_n) \rangle^{-y_n} \right) \ge q^{[d/n]-1} \inf\{-v(z_i)\} \,,$$

which is much stronger than what is needed to conclude everywhere convergence. □

As a corollary, one immediately obtains the analytic continuation of $\zeta_A(s)$. But there are other, higher order, corollaries of Proposition 5.13 that we now turn to.

Definition 5.14. Let $\mathbb{T}_n(\mathbb{C}_\infty)$ be the *Tate algebra* of power series in $t_1, \ldots, t_n$ converging in the unit polydisc in $\mathbb{C}_\infty^n$.

In other words, let $J = \{j_1, \ldots, j_n\}$ be a multi-index; set $t^J := \prod_i t_i^{j_1}$ and $\|J\| := \sum j_i$. Then $\mathbb{T}_n(\mathbb{C}_\infty)$ consists of those power series $f(t) = \sum_J c_J t^J$ with $|c_J|_\infty \to 0$ as $\|J\| \to \infty$. We set $\|f\| = \max_J\{|c_J|_\infty\}$ which is the *Gauss norm*.

Definition 5.15. Let $a \in \mathcal{A}_{+,d}$. We set

$$\langle a(t_i + \theta) \rangle_\circ := \frac{a(t_i + \theta)}{\theta^{\deg a}} \,.$$

Notice that $\langle a(t_i + \theta) \rangle_\circ$ is a deformation of the definition of $\langle a(\theta) \rangle$ given in (5.1) with $\pi = 1/\theta$. Indeed,

$$\langle a(t_i + \theta) \rangle_\circ |_{t_i=0} = \langle a(\theta) \rangle.$$

Notice also that $\langle a(t_i + \theta) \rangle_\circ \in 1 + \frac{1}{\theta} \mathbb{F}_q[t_i][\frac{1}{\theta}]$.

As in Subsection 2.1.1, we let $\partial_j = \partial_{\theta,j}$ be the j-th divided derivative in θ of $f(\theta)$ and set $f^{(m)} = \partial_m f(\theta)$. Therefore if $a \in \mathcal{A}_+$, then $a(t_i + \theta) = \sum_m a^{(m)} t_i^m$ (as usual from calculus).

Let $s = (x, y_1, \ldots, y_n) \in \mathbb{S}_{\mathbb{C}_\infty, n}$ and let $a \in \mathcal{A}_+$.

Definition 5.16.

(1) We set

$$a_\circ^s := x^{\deg a} \langle a(t_1 + \theta) \rangle_\circ^{y_1} \cdots \langle a(t_n + \theta) \rangle_\circ^{y_n}.$$

Note that $a_\circ^s \in \mathbb{T}_n(\mathbb{C}_\infty)$.

(2) We set

$$L_n^\circ(s) := \sum_{a \in \mathcal{A}_+} a_\circ^{-s}.$$

Unwinding the definition gives immediately

$$L_n^\circ(s) = \sum_{d=0}^\infty x^{-d} \left(\sum_{a \in \mathcal{A}_{+,d}} \langle a(t_i + \theta) \rangle_\circ^{-y_1} \cdots \langle a(t_n + \theta) \rangle_\circ^{-y_n} \right).$$

The Gauss norm gives an absolute value on the quotient field of $\mathbb{T}_n(\mathbb{C}_\infty)$ and we now let F be the completion under this norm.

Lemma 5.17. *As functions on $\mathbb{S}_{F,n}$ we have*

$$(5.3) \qquad L_n^\circ(s) = \zeta \left(x \cdot \prod_{i=1}^n (1 + t_i/\theta)^{-y_i}, y_1, \ldots, y_n \right) (t_1 + \theta, \ldots, t_n + \theta).$$

Proof. Note that $\|t_i + \theta\| = |\theta|_\infty > 1$ so that under the additive valuation v associated to the Gauss norm, we have $v(t_i + \theta) < 0$. The rest of the proof involves unraveling the definitions. $\square$

We then have the following extremely important corollary.

Corollary 5.18. *Let n be a positive integer and let $\{m_i\}_{i=1}^n$ and $\{k_j\}_{j=1}^n$ be two collections of n nonnegative integers. Then the following function on $\mathbb{S}_\infty$ (defined via the uniformizer $\pi := 1/\theta$)*

$$(5.4) \qquad \sum_{d=0}^\infty \sum_{a \in A_{+,d}} a^{-s} (a^{(m_1)})^{k_1} \cdots (a^{(m_n)})^{k_n}$$

is entire (i.e., is a continuous family of entire power series in x^{-1}).

Proof. Notice that

$$L_{n+1}^{\circ}(\theta^{-n}x, -1, \ldots, -1, y)|_{t_{n+1}=0}$$

$$= \sum_{i_1,\ldots,i_n} \left(\sum_{d=0}^{\infty} x^{-d} \sum_{a\in A_{+,d}} \langle a\rangle^{-y} a^{(i_i)} \cdots a^{(i_n)} \right) t_1^{i_1} \cdots t_n^{i_n}.$$

The result now follows from Lemma 5.17 and Proposition 5.13. $\qquad\square$

Remarks 5.19.

(1) Note also that

$$L_{n+1}^{\circ}(\theta^{-n}x, -1, \ldots, -1, y)|_{t_{n+1}=0} = \sum_{d} \sum_{a\in A_{+,d}} a(t_1 + \theta) \cdots a(t_n + \theta) a^{-s}$$

for $s = (x, y) \in \mathbb{S}_{\infty}$. This is similar to certain L-series previously discussed in [14] and [3].

(2) The fundamental estimates of [8, Chapter 8], show that the sum in (5.3) is "essentially algebraic." Indeed, let $\mathfrak{v}$ be a prime of A. Then variants of the arguments given here establish that the series in (5.4) can also be interpolated to entire $\mathfrak{v}$-adic functions on the appropriate $\mathfrak{v}$-adic analog of $\mathbb{S}_{\infty}$.

6. Continuous functions on $\mathbb{Z}_p$ into finite characteristic complete algebras

Let L be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$ equipped with the canonical topology. Let $f\colon \mathbb{Z}_p \to \mathcal{O}$ be a continuous function. As mentioned f has a canonical expansion $f(y) = \sum_{j=0}^{\infty} a_j \binom{y}{j}$ where $\{a_j\} \subset \mathcal{O}$ and $a_j \to 0$ as $j \to \infty$; conversely any such sequence $\{a_j\}$ uniquely defines a continuous function. As $\mathbb{Z}_p$ is compact, one readily deduces Mahler expansions for all continuous L-valued functions on $\mathbb{Z}_p$.

In [8, Section 8.4] it is shown that the obvious variant of Mahler's Theorem also holds true if $\mathcal{O}$ is a complete algebra over $\mathbb{Z}/(p)$ where now $\binom{y}{j}$ is reduced modulo p to obtain a function from $\mathbb{Z}_p$ to $\mathcal{O}$.

6.1. Dirichlet series on $\mathbb{Z}_p$. Let $s = (x, y) \in \mathbb{S}_{\infty}$ and let

$$L(s) = \sum_{a\in A_+} c_a a^{-s}$$

be an L-series as in the previous section. Write $\langle a\rangle = 1 + v_a$ where $v_a \equiv 0$ (mod $1/\theta$) so that $(1+v_a)^{-1} = 1 + w_a$ where $w_a = -v_a + v_a^2 + \cdots$. Therefore $\langle a\rangle^{-y} = (1 + w_a)^y$ and its Mahler expansion is then immediate from the binomial expansion. In this fashion the Mahler coefficients of $L(x, y)$ can be computed in terms of $\{c_a\}$ and powers of x.

Definition 6.1. Let L be a finite extension of $k_\infty = \mathbb{F}_q((1/\theta))$ with ring of integers $\mathcal{O} := \mathcal{O}_L$. Let $\mathcal{D} := \mathcal{D}(\mathbb{Z}_p, \mathcal{O})$ be the closure in the Banach space $\mathcal{C}(\mathbb{Z}_p, L)$ (of continuous functions from $\mathbb{Z}_p$ to L) of $\mathcal{O}$-linear combinations of functions of the form $y \mapsto u^y$ for $u \in \mathcal{O}_L$ a principal unit. Following W. Sinnott [18], we call the elements of $\mathcal{D}$ *Dirichlet series on $\mathbb{Z}_p$ with values in $\mathcal{O}_L$*.

The following three fundamental results are then established in [18] and we refer the reader there for details. To begin, let $U_1 \in \mathcal{O}$ be the group of principal units u; i.e., $u \equiv 1 \pmod{M}$ where $M \subset \mathcal{O}$ is the maximal ideal. As in Subsection 4.4, one has the now obvious notion of L-valued measures on U_1 equipped with the standard notion of convolution (using the *multiplicative* group action on U_1). Let $\mathcal{M}(U_1, L)$ (respectively, $\mathcal{M}(U_1, \mathcal{O})$) the space of measures with coefficients in L (respectively, $\mathcal{O}$).

Definition 6.2. Let $\mu \in \mathcal{M}(U_1, \mathcal{O})$. We define its Γ-*transform* $\Gamma_\mu \colon \mathbb{Z}_p \to \mathcal{O}$ by

$$\Gamma_\mu(y) := \int_{U_1} u^y \, \mathrm{d}\mu(u) \,.$$

Theorem 6.3. *The Gamma-transform is an isomorphism of topological $\mathcal{O}$-modules between $\mathcal{M}(U_1, \mathcal{O})$ and $\mathcal{D}(\mathbb{Z}_p, \mathcal{O})$.*

Theorem 6.4. *The L-span of $\mathcal{D}$ is dense in $\mathcal{C}(\mathbb{Z}_p, L)$.*

The next, and last result of [18] we mention, is remarkable because it shows that, in some sense, the elements of $\mathcal{D}$ exhibit behavior similar to that of analytic functions.

Theorem 6.5. *Let $f, g \in \mathcal{D}$. Suppose that f and g coincide in a neighborhood of a point in $\mathbb{Z}_p$. Then $f = g$.*

7. The group $S_{(q)}$

The analogy with the complex theory leads one to look for functional equations (i.e., symmetries) of our L-series. Looking at the special values of the special case $\zeta_A(s) = \sum_{a \in A_+} a^{-s}$, it is apparent that if there are symmetries, they will not be of the classical form $s \mapsto 1 - s$.

In [19], D. Thakur presented some calculations related to trivial zeroes of zeta functions for some non-polynomial base rings. Based on these calculations we were led to the following construction.

Definition 7.1. Let ρ be a permutation of $\{0, 1, \ldots\}$ and let $y \in \mathbb{Z}_p$ be written q-adically as $\sum_{j=0}^\infty c_j q^j$, $0 \leq c_j < q$ all j. We set

$$\rho_* y := \sum_{j=0}^\infty c_j q^{\rho j} \,.$$

Clearly $y \mapsto \rho_* y$ is a bijection of $\mathbb{Z}_p$; the set of these bijections forms a group denoted $S_{(q)}$ with the cardinality of continuum.

In [10] the following result is established.

Proposition 7.2.

(1) *The map $y \to \rho_* y$ is a homeomorphism of $\mathbb{Z}_p$.*

(2) *The mapping $y \to \rho_* y$ stabilizes both the nonnegative and nonpositive integers.*

(3) *Let y_0, y_1 be two p-adic integers such that $y_0 + y_1$ has no carryover of q-adic digits. Then $\rho_*(y_0 + y_1) = \rho_*(y_0) + \rho_*(y_1)$.*

(4) *Let n be a nonnegative integer with sum of q-adic digits $\ell_q(n)$. Then $\ell_q(n) = \ell_q(\rho_* n)$.*

(5) *Let n be an integer. Then $n \equiv \rho_* n \pmod{q-1}$.*

(6) *Let n, j be two nonnegative integers. Then $\binom{n}{j} \equiv \binom{\rho_* n}{\rho_* j} \pmod{p}$.*

Note that the last statement of the proposition follows directly from Lucas' congruence.

7.1. The first action of $S_{(q)}$ on continuous $\mathcal{O}$-valued functions. As the action of $S_{(q)}$ on $\mathbb{Z}_p$ consists of homeomorphisms, we obtain a natural action on the space of continuous functions $\mathcal{C}(\mathbb{Z}_p, \mathcal{O})$.

Definition 7.3. Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathcal{O})$ and $\rho_* \in S_{(q)}$. We define $f^{\rho_1} \in \mathcal{C}(\mathbb{Z}_p, \mathcal{O})$ by $f^{\rho_1}(y) := f(\rho_*^{-1} y)$.

Note that this action is an automorphism of the algebra $\mathcal{C}(\mathbb{Z}_p, \mathcal{O})$.

Proposition 7.4. *As functions from $\mathbb{Z}_p$ to $\mathcal{O}$, we have $\binom{y}{j}^{\rho_1} = \binom{y}{\rho_* j}$.*

Proof. By Part (6) of Proposition 7.2 we have, as functions from $\mathbb{Z}_p$ to $\mathcal{O}$, $\binom{\rho_*^{-1} y}{\rho_*^{-1} j} = \binom{y}{j}$. Now substitute $\rho_* j$ for j. □

Corollary 7.5. *Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathcal{O})$ have Mahler expansion $f(y) = \sum_j c_j \binom{y}{j}$. Then*

$$f^{\rho_1}(y) = \sum_j c_j \binom{y}{\rho_* j}.$$

7.2. An associated congruence. We begin here by considering binomial coefficients as taking values in $\mathbb{Z}_p$. Let a, b be two nonnegative integers. Then the function $y \mapsto \binom{y}{a}\binom{y}{b}$ is also a continuous function from $\mathbb{Z}_p$ to itself and therefore has a well-known associated Mahler expansion (see Section 1.4 in [15], or the Wikipedia page on binomial coefficients, etc.):

(7.1)
$$\binom{y}{a}\binom{y}{b} = \sum_{k=0}^{a} \binom{a+b-k}{k, a-k, b-k}\binom{y}{a+b-k}.$$

Proposition 7.6. *Let $\rho_* \in S_{(q)}$. Let n, m be nonnegative integers and $y \in \mathbb{Z}_p$. Set*

$$s_1 := \sum_{k=0}^{m} \binom{m+n-k}{k, m-k, n-k} \binom{y}{\rho_*(m+n-k)},$$

and

$$s_2 := \sum_{k=0}^{\rho_* m} \binom{\rho_* m + \rho_* n - k}{k, \rho_* m - k, \rho_* n - k} \binom{y}{\rho_* m + \rho_* n - k}.$$

Then $s_1 \equiv s_2 \pmod{p}$.

Proof. The first sum, s_1, arises from applying ρ to the reduction modulo p of (7.1). Next, note that, as functions from $\mathbb{Z}_p$ to $\mathcal{O}$, we have

$$\left(\binom{y}{m} \binom{y}{n} \right)^{\rho_1} = \binom{y}{m}^{\rho_1} \binom{y}{n}^{\rho_1} = \binom{y}{\rho_* m} \binom{y}{\rho_* n},$$

using Proposition 7.4. Now substituting $\rho_* n$ for b and $\rho_* m$ for a in (7.1). As both sums represent the same function modulo p, we are finished. $\square$

In general, the sums in Proposition 7.6 do not have the same number of elements. Indeed, the reader can easily construct examples where the difference between $\rho_* m$ and m is arbitrarily large.

7.3. The space $\mathcal{D}$ is not stable under the first action of $S_{(q)}$. Recall that in Definition 6.1 we presented Sinnott's space $\mathcal{D}$ of Dirichlet series on $\mathbb{Z}_p$ with values in $\mathcal{O}$. By example we show here that the space $\mathcal{D}$ is *not* stable under $S_{(q)}$.

Example 7.7. Let ρ be the permutation of $\{0, 1, \ldots\}$ obtained by exchanging 0 and 1 and fixing all other integers. Let $\mathcal{O} = \mathbb{F}_q[\![1/\theta]\!]$, $u = 1 + 1/\theta$ and $f(y) := u^y \in \mathcal{D}$. Let $g(y) := f^{\rho_1}(y) = f(\rho_* y)$ (as $\rho^2 = 1$). Clearly $f(y) = g(y)$ for $y \equiv 0 \pmod{q^2}$. Thus if $g \in \mathcal{D}$, we would have $f = g$ by Theorem 6.5 which is easily seen to be false.

In Subsection 7.6 we will present an action of $S_{(q)}$ which *does* preserve the space $\mathcal{D}$.

7.4. The first action of $S_{(q)}$ on measures. Recall that in Proposition 4.13 we showed that the Wagner transform gave an isomorphism between the algebra of measures on $A_{\mathfrak{v}}$ and the $A_{\mathfrak{v}}$ algebra of divided power series. Here we establish a natural action of $S_{(q)}$ on the algebra of formal divided power series over a ring R of characteristic p.

Let u be an indeterminate. Let i be a nonnegative integer and $\rho_* \in S_{(q)}$.

Definition 7.8. We set

$$\rho_* u^i := u^{\rho_* i}.$$

Clearly ρ_*, as just defined, extends to an R-module automorphism of $R[\![u]\!]$. Note that if i, j are two nonnegative integers with no carryover of q-adic digits in $i + j$, then $\rho_* u^{i+j} = \rho_* u^i \cdot \rho_* u^j$ by Part (3) of Proposition 7.2. This is easily seen to be false in general when there is carryover.

Now let $u^i/i!$ be the divided power element and $R\{\{u\}\}$ the R-algebra of formal divided power series over R.

Definition 7.9. We set

$$\rho_* \left(\frac{u^i}{i!} \right) := \frac{u^{\rho_* i}}{(\rho_* i)!} \, ,$$

and extend linearly to all of $R\{\{u\}\}$.

Proposition 7.10. *The map $h \mapsto \rho_* h$ of Definition 7.9 is an R-algebra automorphism of $R\{\{u\}\}$.*

Proof. Let i, j be two nonnegative integers. Suppose first that $i + j$ has no carryover of q-adic digits. Then $\binom{i+j}{i} \equiv \binom{\rho_*(i+j)}{\rho_* i} \pmod{p}$ by Lucas. As such, by the argument given after Definition 7.8, we see

$$(7.2) \qquad \rho_* \left(\frac{u^i}{i!} \cdot \frac{u^j}{j!} \right) = \rho_* \left(\frac{u^i}{i!} \right) \cdot \rho_* \left(\frac{u^j}{j!} \right) .$$

If there is carryover of digits, then

$$\binom{i+j}{i} \equiv \binom{\rho_* i + \rho_* j}{\rho_* i} \equiv 0 \pmod{p} .$$

As such we again deduce the equality in (7.2) as both sides now vanish. $\square$

If μ is a measure on $\mathcal{O}$, we denote the measure $T_W^{-1} \rho_* T_W(\mu)$ by μ^{ρ_1}; we shall describe another action of $S_{(q)}$ on measures in Subsection 7.6.

7.5. The action of $S_{(q)}$ on k_∞. Let $a \in A_+$ and let $s = (x, y) \in S_\infty$. Recall that in Definition 5.4 we defined a^{-s} through the use of the choice of positive uniformizer π. Also, as mentioned in Part (2) of Proposition 7.2, the elements of $S_{(q)}$ stabilize both the nonnegative and nonpositive integers. This allows us to make the next definition.

Definition 7.11. Let $x \in k_\infty$ be written π-adically as $x = \sum_{j \gg -\infty} c_j \pi^j$ with $c_j \in \mathbb{F}_q$. Let $\rho_* \in S_{(q)}$. Then we set

$$\rho_* x := \sum_{j \gg -\infty} c_j \pi^{\rho_* j} .$$

It is readily seen that $x \mapsto \rho_* x$ is a continuous automorphism of k_∞ as $\mathbb{F}_q$-vector space.

7.6. Further actions on measures and functions. We will present here a number of other actions on functions and measures. As of this writing we do not know how they are related.

Let $\mathcal{O} = \mathbb{F}_q[\![\pi]\!]$ and $U \subset \mathcal{O}$ be the group of units and $U_1 \subseteq U$ the group of units $\equiv 1 \pmod{(\pi)}$. Let $\rho_* \in S_{(q)}$. Note that by definition $\rho_* 0 = 0$. The next result is then obvious.

Proposition 7.12. *As sets, $\mathcal{O}$, U and U_1 are stable under ρ_*.*

Let X be one of $\{\mathcal{O}, U, U_1\}$. Let $f \colon X \to k_\infty$ be a continuous function. We then set $f^{\rho_1}(x) := f(\rho_*^{-1} x)$ (in analogy with our definition for functions on $\mathbb{Z}_p$); as before this is an action on the space of continuous functions and is an automorphism of the algebra of such continuous functions.

One can use the Carlitz polynomials in $\mathbb{F}_q[\pi]$ (as in Subsection 2.2) to obtain a Banach basis for the continuous functions on $\mathcal{O}$. However, unlike the simple Corollary 7.5, we do not know how to easily compute $G_i^{\rho_1}(x)$ as of this writing.

As we have an action on the spaces of continuous functions, we deduce associated actions on the space of measures. Again, let X be as above and let μ be an $\mathcal{O}$-valued measure on X.

Definition 7.13. We let μ^{ρ_2} be the measure defined by

$$\int_X f(x) \, \mathrm{d}\mu^{\rho_2}(x) := \int_X f(\rho_*^{-1} x) \, \mathrm{d}\mu(x).$$

Let $f \colon \mathbb{Z}_p \to \mathcal{O}$ be a Dirichlet series on $\mathbb{Z}_p$. In Example 7.7 we established that, in general, $f^{\rho_1}(y) = f(\rho_*^{-1} y)$ will not be a Dirichlet series on $\mathbb{Z}_p$. On the other hand, by Theorem 6.3 we are guaranteed that $f(y) = \int_U u^y \, \mathrm{d}\mu(u)$ for some measure μ.

Definition 7.14. We set

$$f^{\rho_2}(y) := \int_U u^y \, \mathrm{d}\mu^{\rho_2}(u).$$

Clearly $f \mapsto f^{\rho_2}(y)$ is an $\mathcal{O}$-linear automorphism of the space $\mathcal{D}$ of Dirichlet series on $\mathbb{Z}_p$.

Now let $X = \mathcal{O}$ and let $\mu \in \mathcal{M}(\mathcal{O}, \mathcal{O})$.

Proposition 7.15. *The map $\mu \mapsto \mu^{\rho_2}$ is an automorphism of the convolution algebra of measures.*

Proof. This follows because the map $x \mapsto \rho_* x$ on $\mathcal{O}$ is $\mathbb{F}_q$-linear. $\qquad\square$

We have no idea of any relationship between the above action and the action $\mu \mapsto \mu^{\rho_1}$ arising from the Wagner transform and Proposition 7.10.

There is an obvious third action of $S_{(q)}$ on $\mathcal{C}(\mathbb{Z}_p, \mathcal{O})$ (including the above action on Dirichlet series) by $f^{\rho_3}(y) := \rho_* f(y)$. If $f(y) = \sum_{j=0}^{\infty} c_j \binom{y}{j}$ then

$$(7.3) \qquad f^{\rho_2}(y) = \sum_{j=0}^{\infty} \rho_*(c_j) \binom{y}{j}.$$

Let $f \in \mathcal{C}(\mathcal{O}, \mathcal{O})$ be continuous. We obtain a second action of $S_{(q)}$ by $f^{\rho_2}(x) := \rho_* f(x)$. Further let $f : \mathcal{O} \to \mathcal{O}$ have the Wagner expansion $\sum c_j G_j(x)$ where $c_j \to 0$ as $j \mapsto \infty$. We obtain $f^{\rho_2}(x) = \sum \rho_* c_j G_j(x)$. However, we obtain yet a third $\mathbb{F}_q$-linear action on $\mathcal{C}(\mathcal{O}, \mathcal{O})$ by

$$(7.4) \qquad f^{\rho_3}(x) := \sum \rho_*(c_j) G_j(x),$$

which is guaranteed to converge as $\rho_* c_j \to 0$ as $j \to \infty$ (and compare (7.3) and (7.4)).

We leave to the reader the appropriate definitions for actions on the subspaces of $\mathbb{F}_q$-linear functions.

Finally let $\mu \in \mathcal{C}(\mathcal{O}, \mathcal{O})$ have expansion $\sum d_j \frac{u^j}{j!}$ dual to the above Wagner expansions of continuous functions. We set

$$\mu^{\rho_3} := \sum \rho_*(d_j) \frac{u^j}{j!}.$$

The map $\mu \to \mu^{\rho_3}$ is again $\mathbb{F}_q$-linear.

As of this writing, we do not know how these various actions interact.

7.7. The action on $S_{(q)}$. In [10] we defined an action of $S_{(q)}$ on $\mathbb{S}_{\infty}$ which we recall here.

Definition 7.16. Let $y \in \mathbb{Z}_p$ and $\rho_* \in S_{(q)}$. Then we set

$$\hat{\rho}_*(y) := -\rho_*(-y).$$

Clearly, Part (2) of Proposition 7.2 implies that $\hat{\rho}_*$ also stabilizes both the nonnegative and nonpositive integers.

Recall that by definition $\mathbb{S}_{\infty} = \mathbb{C}_{\infty}^* \times \mathbb{Z}_p$. Let $L \subseteq \mathbb{C}_{\infty}$ be a subfield.

Definition 7.17. We define

$$\mathbb{S}_{L,\infty} = L^* \times \mathbb{Z}_p \subseteq \mathbb{S}_{\infty}.$$

Definition 7.18. Let $s = (x, y) \in \mathbb{S}_{k_{\infty}, \infty}$. We set

$$\rho_* s = (\rho_* x, \hat{\rho}_* y) \in \mathbb{S}_{k_{\infty}, \infty}.$$

Recall (see Remarks 5.6) that, for an integer i, we set $s_i = (\pi^{-i}, i) \in \mathbb{S}_{k_{\infty}, \infty}$ with the property that $a^{s_i} = a^i$. From Definition 7.17 we obtain

$$\rho_* s_{-i} = s_{-\rho_* i}.$$

In particular, if $i \equiv 0 \pmod{q-1}$ then so is $\rho_* i$ (by Part (5) of Proposition 7.2).

In [17], J. Sheats established that the zeroes of $\zeta_A(s) = \sum_{a \in A_+} a^{-s}$ all lie in k_∞ and are simple. The remarks just given imply, in particular, that our action on $\mathbb{S}_{k_\infty, \infty}$ permutes the *trivial zeroes* of $\zeta_A(s)$. For a further discussion of the interaction of $S_{(q)}$ and the zeroes of $\zeta_A(s)$ we refer the reader to [10].

In general (for arbitrary A) there will be zeroes of L-functions which do not lie in k_∞ and, as such, we need to extend the action of $S_{(q)}$ further. On the other hand, one knows that *all* zeroes will be algebraic over k_∞ and one *suspects* that, for a fixed $y \in \mathbb{Z}_p$, the zeroes will lie in a finite extension of k_∞.

Therefore let $L \subset \mathbb{C}_\infty$ be a finite extension of k_∞ and set $m = [L : k_\infty]$. We do not as yet have any procedure to continuously extend the action of $S_{(q)}$ $\mathbb{F}_q$-linearly to L, L arbitrary, in a canonical way (or in a way that produces only finitely many extensions such as with Galois theory). Nevertheless one can always get continuous extensions in the following fashion. Let $B = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be a k_∞-basis of L where we always assume $\alpha_1 = 1$. Via B, note that L is isomorphic to k_∞^m.

Definition 7.19. Let $\beta \in L$ be written $\sum_{e=1}^m k_e \alpha_e$ with $\{k_e\} \subset k_\infty$. We set

$$\rho_* \beta := \sum_e \rho_*(k_e) \alpha_e \,.$$

We call this *the extended action of $S_{(q)}$ on L given by B.*

The reader will note that Definition 7.19 is essentially the coordinatewise action of ρ_* on k_∞^m.

If, however, L is a totally unramified extension of k_∞ obtained by a finite field extension, $\mathbb{F}/\mathbb{F}_q$, we *can* $\mathbb{F}$-linearly canonically extend the action of $S_{(q)}$. The next example explains the connection with Definition 7.19.

Example 7.20. Let $\mathbb{F} \simeq \mathbb{F}_{q^m} \subset \mathbb{C}_\infty$ be the finite field of q^m elements. Let $L := k_\infty(\mathbb{F}_{q^m})$ so that $L \simeq \mathbb{F}_{q^m} \otimes_{\mathbb{F}_q} k_\infty$. Choose a basis $B = \{1, \ldots\}$ for L/k_∞ consisting of elements in $\mathbb{F}_{q^m}$. Then the extension to L of ρ_* given in Definition 7.19 is just the obvious $\mathbb{F}_{q^m}$-linear extension of ρ_*. As such it is independent of the basis $B \subset \mathbb{F}_{q^m}$.

Note, again, that the class of constant field extensions is precisely the class of unramified extensions of k_∞.

Let $L \subset \mathbb{C}_\infty$ be a finite extension of k_∞ as above equipped with *some* continuous extension ρ of $S_{(q)}$ to $\mathbb{F}_q$-linear automorphisms of L.

Definition 7.21. Let $L_\rho \subset L$ be the set of those $\alpha \in L$ which commute with the action of $S_{(q)}$ given by ρ.

Proposition 7.22. *The set $L_\rho \subset L$ is an $\mathbb{F}_q$-subfield.*

8. The Riemann Hypothesis as a ramification statement.

Let $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ be, as usual, Riemann's zeta function with its meromorphic continuation to the complex plane $\mathbb{C}$. Let $\Gamma(s)$ be Euler's gamma function and, again as usual, put

$$\Xi(s) := 1/2\pi^{-s/2}s(s-1)\Gamma(s/2)\zeta(s)\,.$$

Riemann showed that $\Xi(s)$ is entire and satisfies the functional equation $\Xi(s) = \Xi(1-s)$. The *Riemann Hypothesis* states that all zeroes of $\Xi(s)$ are of the form $s = 1/2 + it$ for some real number t. Following Riemann, put $\hat{\Xi}(t) := \Xi(1/2 + it)$, so that the functional equation becomes $\hat{\Xi}(t) = \hat{\Xi}(-t)$ and the Riemann Hypothesis becomes the statement that the zeroes of $\hat{\Xi}(t)$ are real. This "reality" statement is precisely echoed by the Theorem of Sheats [17] mentioned above and underlies this section.

8.1. The Riemann Hypothesis from the viewpoint of the Carlitz module. Let $\exp(z) = \sum_{i=0}^{\infty} \frac{x^i}{i!}$ be the exponential function with period $2\pi i$. Note simply that

$$\mathbb{C} = \mathbb{R}(2\pi i)\,.$$

Now let $\exp_C(x)$ be the exponential of the Carlitz module with period $\bar{\xi} \in \mathbb{C}_\infty$. Let $K = k_\infty(\bar{\xi})$. As is well-known K/k_∞ is Galois with Galois group isomorphic to $\mathbb{F}_q{}^* = A^*$ (much as the Galois group of $\mathbb{C}/\mathbb{R}$ is isomorphic to $\mathbb{Z}^* = \{\pm 1\}$). More importantly for our purposes, K is *totally ramified* over k_∞.

This analogy between $\mathbb{C}$ and K suggests very strongly that we view (morally at least!) $\mathbb{C}$ as being totally ramified over $\mathbb{R}$. Thus, from the optic of the Carlitz module, the Riemann Hypothesis becomes the statement "the zeros of $\hat{\Xi}(t)$ are unramified."

8.2. The Riemann Hypothesis in Characteristic p. Here we will be somewhat speculative as the subject is still far from mature. First of all, as noted, unramified extensions of k_∞ are precisely the constant field extensions. Moreover, on the one hand, we know from Sheats that the zeroes of $\zeta_{\mathbb{F}_q[\theta]}(s)$ are simple and in k_∞; on the other, we know from Böckle [4] that there are other base rings A where the zeroes are not all in k_∞ (but for a given $y \in \mathbb{Z}_p$ in fact almost all of those computed are).

Therefore, in general, we should *not* expect that the zeroes lie in k_∞.

Suppose now that $\mathfrak{k}$ is a finite abelian extension of k and for simplicity suppose that $[\mathfrak{k}: k]$ is prime to p. Let $\mathfrak{O} \subset \mathfrak{k}$ be the ring of A-integers. Let I be a nontrivial ideal of $\mathfrak{O}$ and let $nI \in A_+$ be the monic generator of the ideal theoretic norm of I. In the classical fashion we define

$$\zeta_{\mathfrak{O}}(s) := \sum_{I \subset \mathfrak{O}} nI^{-s}\,.$$

Furthermore, exactly as in classical theory, one has the factorization

$$
\tag{8.1} \zeta_{\mathfrak{O}}(s) = \prod_{\psi} L(\psi, s) \,,
$$

where ψ runs over all $\mathbb{C}_{\infty}$-valued characters of $\mathrm{Gal}(\mathfrak{k}/k)$ and $L(\psi, s)$ is defined in the obvious fashion. Note that (Chapter 8, [8]) all functions in (8.1) can be shown to be entire on $\mathbb{S}_{\infty}$. Let $k_{\infty}(\psi)$ be the finite unramified (constant field) extension obtained by adjoining the values of ψ.

If the zeroes of $L(\psi, s)$ were all in k_{∞} then, by completeness, all the coefficients of $L(\psi, s)$ would be also and this is *not* true in general. That is, the best one might hope for is that all the roots lie in $k_{\infty}(\psi)$; i.e. are unramified.

Remark 8.1. Let $\alpha \subset \mathbb{C}_{\infty}$ be algebraic and let $L = k_{\infty}(\alpha)$; set $n = [L : k_{\infty}]$. If $L \simeq \mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} k_{\infty}$ and ρ is the canonical action of $S_{(q)}$ via extension of scalars, then L_{ρ} (given in Definition 7.21) is $\mathbb{F}_{q^n}$.

It is reasonable to believe that the above Remark precisely characterizes the class of unramified extensions in terms of extensions of the action of $S_{(q)}$.

So to summarize, as a first approximation, it seems that one might expect the roots of general arithmetic L-series to be unramified and this appears to be detectable via the extensions of the action of $S_{(q)}$. We know from examples that for general A this will not be true of all zeroes, but perhaps it does always hold for almost all zeroes for a given $y \in \mathbb{Z}_p$. Of course one wants to ultimately understand the arithmetic properties of *all* zeroes including the ramified ones as well as the zeroes of the $\mathfrak{v}$-adic interpolations of such L-series at the finite primes $\mathfrak{v}$ of A.

References

[1] B. Anglès, 2016, private communication.

[2] B. Anglès, T. Ngo Dac & F. Tavares Ribeiro, "Twisted characteristic p zeta functions", *J. Number Theory* **168** (2016), p. 180-214.

[3] B. Anglès & F. Pellarin, "Functional identities for L-series values in positive characteristic", *J. Number Theory* **142** (2014), p. 223-251.

[4] G. Böckle, "The distribution of the zeros of the Goss zeta function for $A = \mathbb{F}_q[x, y]/(y^2 + y + x^3 + x + 1)$", *Math. Z.* **275** (2013), no. 3-4, p. 835-861.

[5] A. Connes, "An essay on the Riemann Hypothesis", in *Open problems in mathematics*, Springer, 2016, p. 225-257.

[6] K. Conrad, "The digit principle", *J. Number Theory* **84** (2000), no. 2, p. 230-257.

[7] V. G. Drinfeld, "Elliptic modules", *Mat. Sb.* **94(136)** (1974), p. 594-627.

[8] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3, vol. 35, Springer, 1996, xiii+422 pages.

[9] ———, "Applications of non-Archimedean integration to the L-series of τ-sheaves", *J. Number Theory* **110** (2005), no. 1, p. 83-113.

[10] ———, "Zeta phenomenology", in *Noncommutative geometry, arithmetic, and related topics*, Johns Hopkins University Press, 2011, p. 159-182.

[11] ———, "A local field approach to the Riemann Hypothesis", `https://arxiv.org/abs/1206.2040`, 2012.

[12] K. Mahler, "An interpolation series for continuous functions of a p-adic variable", *J. Reine Angew. Math* **199** (1958), p. 23-34, erratum in *ibid.* **208** (1961), p. 70-72.

[13] M. A. Papanikolas, 2013, private correspondence.

[14] F. Pellarin, "Values of certain L-series in positive characteristic", *Ann. Math.* **176** (2012), no. 3, p. 2055-2093.

[15] J. Riordan, *Combinatorial Identities*, Robert E. Krieger Publishing Co., 1979, 256 pages.

[16] J.-P. Serre, "Endomorphismes complètement continus des espaces Banach p-adiques", *Publ. Math., Inst. Hautes Étud. Sci.* **12** (1962), p. 69-85.

[17] J. T. Sheats, "The Riemann hypothesis for the Goss zeta function for $\mathbf{F}_q[T]$", *J. Number Theory* **71** (1998), no. 1, p. 121-157.

[18] W. M. Sinnott, "Dirichlet series in function fields", *J. Number Theory* **128** (2008), no. 7, p. 1893-1899.

[19] D. S. Thakur, "On characteristic p zeta functions", *Compos. Math.* **99** (1995), no. 3, p. 231-247.

[20] J. F. Voloch, "Differential operators and interpolation series in power series fields", *J. Number Theory* **71** (1998), no. 1, p. 106-108.

[21] C. G. Wagner, "Interpolation series for continuous functions on π-adic completions of $\mathrm{GF}(q,x)$", *Acta Arith.* **17** (1971), p. 389-406.

David Goss[†]
Department of Mathematics
The Ohio State University
231 W. 18th Ave.
Columbus, Ohio 43210, USA
E-mail: dmgoss@gmail.com