FRACTIONAL POWER SERIES AND PAIRINGS ON DRINFELD MODULES

BJORN POONEN

May 18, 1995

Abstract. Let C be an algebraically closed field containing $\mathbb{F}_q$ which is complete with respect to an absolute value $|\ |$. We prove that under suitable constraints on the coefficients, the series $f(z) = \sum_{n \in \mathbb{Z}} a_n z^{q^n}$ converges to a surjective, open, continuous $\mathbb{F}_q$-linear homomorphism $C \to C$ whose kernel is locally compact. We characterize the locally compact sub-$\mathbb{F}_q$-vector spaces G of C which occur as kernels of such series, and describe the extent to which G determines the series. We develop a theory of Newton polygons for these series which lets us compute the Haar measure of the set of zeros of f of a given valuation, given the valuations of the coefficients. The "adjoint" series $f^*(z) = \sum_{n \in \mathbb{Z}} a_n^{1/q^n} z^{1/q^n}$ converges everywhere if and only if f does, and in this case there is a natural bilinear pairing

$$\ker f \times \ker f^* \to \mathbb{F}_q$$

which exhibits $\ker f^*$ as the Pontryagin dual of $\ker f$. Many of these results extend to non-linear fractional power series. We apply these results to construct a Drinfeld module analogue of the Weil pairing, and to describe the topological module structure of the kernel of the adjoint exponential of a Drinfeld module.

1. Introduction

Let L be a perfect field of characteristic p. Recall that a polynomial $f(x) \in L[x]$ is called *additive* if $f(x+y) = f(x) + f(y)$ identically. It is easy to see that a polynomial is additive if and only if it is of the form

$$f(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_n x^{p^n}.$$

The set of additive polynomials forms a noncommutative ring in which $(f \circ g)(x) = f(g(x))$. This ring is generated by the scalar multiplications $x \mapsto ax$ for $a \in L$, and

1991 *Mathematics Subject Classification.* Primary 13J05; Secondary 11G09.

Key words and phrases. fractional power series, Pontryagin duality, Newton polygon, Weil pairing, Drinfeld module.

This research was supported by a Sloan Doctoral Dissertation Fellowship and an NSF Mathematical Sciences Postdoctoral Research Fellowship. Research at MSRI is supported in part by NSF grant DMS-9022140.

by $\tau(x) = x^p$. In this ring we can write the f above as $a_0+a_1\tau+a_2\tau^2+\cdots+a_n\tau^n$, and we will denote the ring by $L\{\tau\}$, using braces instead of brackets to remind ourselves that it is a *twisted* polynomial ring in τ. The indeterminate τ does not commute with elements of L (which are acting as scalar multiplications); instead if $a \in L$ then $\tau a = a^p\tau$ as additive polynomials.

Following Ore [17], we define the *adjoint* of f to be the expression

$$f^*(x) = a_0 x + a_1^{1/p} x^{1/p} + a_2^{1/p^2} x^{1/p^2} + \cdots + a_n^{1/p^n} x^{1/p^n}.$$

This defines a function on L (and its algebraic closure) since L is perfect. Goss observed that the kernel of f (the set of zeros of f in a fixed algebraic closure of L) generates the same field extension as the kernel of f^*, by using a formula of Ore [17] which expresses the zeros of f^* explicitly in terms of determinants involving the zeros of f. One might ask whether there is a natural Galois-equivariant isomorphism between $\ker f$ and $\ker f^*$. In general, the answer is no. But, as was discovered independently by the author and N. Elkies [6], there is something which is just as good:

Theorem. *There exists a natural Galois-equivariant pairing*

$$\ker f \times \ker f^* \to \mathbb{F}_p.$$

One of the main results of this paper is the generalization of this theorem to the situation where f is an additive *power series*. Let C be an algebraically closed field of characteristic p which is complete with respect to a (non-archimedean) absolute value $|\ |$. If $f \in C[[z]]$ is an additive power series, its adjoint is a "linear fractional power series" of the form

$$g(z) = b_0 z + b_1 z^{1/p} + b_2 z^{1/p^2} + \cdots$$

It is easy to see that such a series converges for all z when the b_i tend to zero. In this case, we will show that g defines a continuous group homomorphism $C \to C$, which is surjective and open if nonzero. One can see immediately that if $b_0 \neq 0$ then $g(z) = b_0 z + \text{(smaller terms)} \neq 0$ for large z, so $\ker g$ is a closed and bounded subgroup of C. In fact, we prove that $\ker g$ is compact, and if infinitely many b_i are nonzero, it is isomorphic to $\mathbb{F}_p^\omega$ as a topological group. Conversely, if G is any compact subgroup of C, then G is the kernel of such a g if and only if the integral $\int_G v$ of the real-valued function $v(z) = -\log|z|$ with respect to Haar measure on G equals $+\infty$. Also, G essentially determines g. We next develop the theory of Newton polygons for such series. Finally we prove the analogue of our pairing theorem above, namely that for any everywhere convergent additive power series $f \in C[[z]]$, there is a natural pairing

$$\ker f \times \ker f^* \to \mathbb{F}_p$$

which exhibits the compact group $\ker f^*$ as the Pontryagin dual of the discrete group $\ker f$.

Actually we will generalize further by considering $\mathbb{F}_q$-linear power series for any power q of p, and more substantially by considering *bi-infinite series*

$$f(z) = \cdots + a_{-2}z^{1/q^2} + a_{-1}z^{1/q} + a_0 z + a_1 z^q + a_2 z^{q^2} + \cdots .$$

The kernels of these series are locally compact. In fact, many of our results extend to non-linear series for which the set of allowable exponents is

$$E = \{mp^n : m, n \in \mathbb{Z}, m \geq 0\}.$$

We will develop results in this general context, specializing when appropriate.

Finally we give some applications of our results to the theory of Drinfeld modules. We construct a pairing for Drinfeld modules which behaves in many ways like the Weil pairing on abelian varieties. In addition, our results let us describe the topological module structure of the kernel of the adjoint exponential function of a Drinfeld module. We conclude with a few unanswered questions.

2. The rings $\mathcal{P}$ and $\mathcal{F}$ of fractional power series

Let C be an algebraically closed field containing $\mathbb{F}_q$ which is complete with respect to a (non-archimedean) absolute value $|\ |$. Let $V = \{x \in C : |x| \leq 1\}$ be the valuation ring of C, let $\mathfrak{m} = \{x \in C : |x| < 1\}$ be its maximal ideal, and let $k = V/\mathfrak{m}$ be the residue field.

We will consider "fractional power series" in which the exponents belong to

$$E = \{mp^n : m, n \in \mathbb{Z}, m \geq 0\}.$$

Since we have unique p-th roots in C, for any $z \in C$ and $e = mp^n \in E$ we can interpret z^e as $(z^{1/p^n})^m$. Define $\mathcal{P}$ to be the set of series $\sum_{e \in E} a_e z^e$ with coefficients a_e in C, which converge at all $z \in C$. Since E is countable, it is clear what convergence means: for each $z \in C$ and $r > 0$, there must be only finitely many terms in the series of absolute value greater than r. And since we are in the non-archimedean situation, convergence at some z of absolute value r implies uniform convergence on all of Δ_r.

Furthermore, we define the set $\mathcal{F}$ of "$\mathbb{F}_q$-linear fractional power series" as the set of bi-infinite series

$$f(z) = \cdots + a_{-2}z^{1/q^2} + a_{-1}z^{1/q} + a_0 z + a_1 z^q + a_2 z^{q^2} + \cdots$$

which converge for all $z \in C$. Hence $\mathcal{F}$ is a subset of $\mathcal{P}$. For $f \in \mathcal{F}$ we will also write

$$f = \cdots + a_{-2}\tau^{-2} + a_{-1}\tau^{-1} + a_0 + a_1\tau + a_2\tau^2 + \cdots ,$$

thinking of τ as the operator $\tau(z) = z^q$ on C, and thinking of $a \in C$ acting as the scalar multiplication by a. Note that for $a \in C$, $\tau a = a^q \tau$ and $\tau^{-1} a = a^{1/q}\tau^{-1}$, as maps on C. We also define $\mathcal{F}^+$ as the set of $f \in \mathcal{F}$ such that $a_n = 0$ for $n < 0$ (these are just the convergent $\mathbb{F}_q$-linear power series), and $\mathcal{F}^-$ as the set of $f \in \mathcal{F}$ such that $a_n = 0$ for $n > 0$.

There is a simple criterion for the convergence of linear series:

Proposition 1. *Suppose $a_i \in C$ for $i \in \mathbb{Z}$. The bi-infinite series*

$$f(z) = \cdots + a_{-2}z^{1/q^2} + a_{-1}z^{1/q} + a_0 z + a_1 z^q + a_2 z^{q^2} + \cdots$$

converges for all $z \in C$ if and only if the following two conditions hold:

(1) $\lim_{n\to-\infty} |a_n| = 0.$
(2) $\lim_{n\to+\infty} |a_n|^{1/q^n} = 0.$

Proof. By the well-known formula for the radius of convergence of a power series, the right end of the series converges everywhere when $\lim_{n\to+\infty} |a_n|^{1/q^n} = 0$. The left end converges at z when $\lim_{n\to-\infty} |a_n z^{q^n}| = 0$. But for z nonzero, this is equivalent to $\lim_{n\to-\infty} |a_n| = 0$, since $\lim_{n\to-\infty} |z^{q^n}| = 1$. □

For $f, g \in \mathcal{P}$, we define $f + g$ and $f \cdot g$ in the obvious way, by expanding and grouping terms with the same exponent.

Proposition 2. *$(\mathcal{P}, +, \cdot)$ is a commutative ring.*

Proof. The only nontrivial part is to check that the sum and product are actually everywhere convergent. In fact, this is easy as well, since the sum or product of two convergent series is a doubly infinite convergent series, even before grouping terms. □

If $f, g \in \mathcal{F}$, we can still use the definitions of addition and multiplication above, but $f \cdot g$ need not be an element of $\mathcal{F}$, so $\mathcal{F}$ is not a subring of $\mathcal{P}$. Nevertheless, we will make $\mathcal{F}$ into a ring by using composition in place of multiplication. In fact, we will define the composition $f \circ g$ of two general elements $f(z) = \sum_{d\in E} a_d z^d$ and $g(z) = \sum_{e\in E} b_e z^e$ of $\mathcal{P}$. First, for integral $m \geq 0$, let g^m denote g multiplied by itself m times. For $n \in \mathbb{Z}$, define $g^{p^n} = \sum_{e\in E} b_e^{p^n} z^{ep^n}$, which is consistent with the previous sentence. For $d = mp^n \in E$, define $g^d = (g^m)^{p^n}$. Finally define

$$f \circ g = \sum_{d\in E} a_d g^d,$$

in which we expand and group terms of the same exponent. If $f = \sum_{i\in\mathbb{Z}} a_i \tau^i$ and $g = \sum_{j\in\mathbb{Z}} b_j \tau^j$ are elements of $\mathcal{F}$, then the above definition simplifies to $f \circ g = \sum_{n\in\mathbb{Z}} c_n \tau^n$ where

$$c_n = \sum_{i+j=n} a_i b_j^{q^i}.$$

Proposition 3. *For $f, g \in \mathcal{P}$, $f \circ g$ converges to an element of $\mathcal{P}$, and represents the composition of the maps f and g.*

Proof. Fix $r > 0$. Since the series g converges uniformly on Δ_r, we may let $R = \sup|g(\Delta_r)|$. Fix z of absolute value r. Then from the definition of g^d it is clear that all terms in the expansion of g^d (for fixed $d \in E$) are bounded in absolute value by R^d, with only finitely terms of absolute value greater than s, for each $s > 0$. Fix $t > 0$. There are only finitely many d such that $|a_d|R^d > t$ (since f is convergent), so there are only finitely many d such that $a_d g^d$ has terms of absolute value greater than t, and the previous sentence implies that even for such d, there are at most finitely many such terms. Hence even before grouping terms, the series for $f \circ g$ converges at z, and this implies that the grouping gives a convergent series for each coefficient of $f \circ g$ as well. □

Proposition 4. *$(\mathcal{F}, +, \circ)$ is a noncommutative ring containing C. The center of $\mathcal{F}$ is $\mathbb{F}_q$.*

Proof. By the previous proposition and the explicit form of the definition for linear series, if $f, g \in \mathcal{F}$, then $f \circ g \in \mathcal{F}$. Hence the first part is clear. The center of $\mathcal{F}$ clearly contains $\mathbb{F}_q$. On the other hand, if $c \in C$ is transcendental, direct computation shows that its centralizer in $\mathcal{F}$ is C, and the only elements of C which commute with τ are those in $\mathbb{F}_q$. □

Proposition 5. *Any $f \in \mathcal{P}$ defines a continuous function $f : C \to C$. The continuity is uniform on each bounded subset of C.*

Proof. It suffices to show f is uniformly continuous on Δ_R for each $R > 0$. Given $\epsilon > 0$, there are only finitely many terms $a_e z^e$ in f for which $|a_e|R^e > \epsilon$, since f is everywhere convergent. The sum of these is clearly uniformly convergent on Δ_R, and the sum of the rest of the terms is bounded in absolute value by ϵ for all $z \in \Delta_R$, so f is uniformly continuous on Δ_R as well. □

Proposition 6. *If $f \in \mathcal{P}$ is nonzero as a series, then the function it defines on C is not identically zero.*

Proof. Since $f(1)$ converges, there are only finitely many coefficients of f larger than a given size, and by scaling by an element of C, we may assume the largest coefficients have absolute value 1. Then the reduction of f modulo $\mathfrak{m}$ is a fractional *polynomial* over the residue field k, i.e., the p^n-th root of a polynomial. Since k is infinite, this reduction is nonzero at some $\bar{\alpha} \in k$. If $\alpha \in C$ is any lift of $\bar{\alpha}$, then $|f(\alpha)| = 1$, so in particular $f(\alpha) \neq 0$. □

Proposition 7. *If $f \in \mathcal{P}$ considered as a map on C is $\mathbb{F}_q$-linear, then $f \in \mathcal{F}$.*

Proof. Write $f = \sum_{e \in E} a_e z^e$. For each $c \in C$, the function $f(cz + z) - f(cz) - f(z)$ in $\mathcal{P}$ is identically zero, so by Proposition 6 it is zero as a series. Hence for each $e = mp^n$, the coefficient of z^e in it is zero. This coefficient is $a_e\,[(c+1)^e - c^e - 1]$. If e is not a power of p and $a_e \neq 0$, then the p^n-th power of this coefficient will be a nonzero polynomial in c, and hence will not vanish for some value of c. This contradiction shows that $a_e = 0$ for e not a power of p. A similar argument with $f(cz) - cf(z)$ for $c \in \mathbb{F}_q$ shows that $a_e = 0$ for e not a power of q; i.e., $f \in \mathcal{F}$. $\square$

3. The topology and norm on $\mathcal{P}$ and $\mathcal{F}$

We give $\mathcal{P}$ the "bounded-open topology." For real $r > 0$, define

$$\begin{aligned} \Delta_r &= \{ x \in C : |x| \leq r \}, \\ \Delta'_r &= \{ x \in C : |x| < r \}. \end{aligned}$$

If $r, s > 0$ let

$$\mathcal{P}(r,s) = \{ f \in \mathcal{P} | f(\Delta_r) \subset \Delta_s \}.$$

Take these subsets of $\mathcal{P}$ as a subbasis for the neighborhoods of zero. For each $\alpha, \beta \in C$ and $c \in \mathbb{F}_q$, the set of $f \in \mathcal{P}$ such that $f(\alpha+\beta) = f(\alpha) + f(\beta)$ and the set of $f \in \mathcal{P}$ such that $f(c\alpha) = cf(\alpha)$ are closed subsets of $\mathcal{P}$. Hence by Proposition 7, $\mathcal{F}$ is a closed subset of $\mathcal{P}$. We give $\mathcal{F}$ the subspace topology, which is also the bounded-open topology on $\mathcal{F}$.

For $f = \sum_{e \in E} a_e z^e \in \mathcal{P}$, define

$$\|f\| = \sup \{ |a_e| : e \leq 1 \} \cup \{ |a_e|^{1/e} : e \geq 1 \}.$$

The convergence of f implies that this is a finite real number, and that the supremum is attained. If $f = \sum_{n \in \mathbb{Z}} a_n \tau^n \in \mathcal{F}$ this becomes

$$\|f\| = \sup \{ |a_n| : n \leq 0 \} \cup \{ |a_n|^{q^{-n}} : n \geq 0 \}.$$

This norm satisfies an ultrametric triangle inequality: $\|f + g\| \leq \max\{\|f\|, \|g\|\}$ for any $f, g \in \mathcal{P}$. In showing that the norm is consistent with the bounded-open topology on $\mathcal{P}$ we will use the following.

Lemma 1. *Let $f = \sum_{e \in E} a_e z^e \in \mathcal{P}$, and let $r, s > 0$. Then the following are equivalent:*

(1) *$f \in \mathcal{P}(r,s)$.*
(2) *$a_e z^e \in \mathcal{P}(r,s)$ for all $e \in E$.*
(3) *$|a_e| r^e \leq s$ for all $e \in E$.*

Proof. It is clear that (2) and (3) are equivalent, and that they imply (1). In showing (1) implies (3), we can assume r is the absolute value of some element of C, because if not, it is an increasing limit of such r, and the implication follows if it is known for those r. Then we can reduce to the case $r = 1$ by composing f with a scalar multiplication on the right. Now what we must show is that if f is a nonzero element of $\mathcal{P}(1,s)$, a largest coefficient b of f is at most s in absolute value. The mod $\mathfrak{m}$ reduction of $b^{-1}f$ is the p^n-th root of a nonzero *polynomial*, so we can pick $x \in V$ which does not reduce to one of its roots, and find that $|b^{-1}f(x)| = 1$. Hence $|b| = |f(x)| \leq s$, since $f \in \mathcal{P}(1,s)$. $\square$

Proposition 8. *The bounded-open topology on $\mathcal{P}$ is the same as that induced by the norm $\| \ \|$.*

Proof. It is clear from the definitions that if $0 < s < 1 < r$,

$$\|f\| \leq s/r \implies f \in \mathcal{P}(r,s).$$

On the other hand, by Lemma 1, if $0 < s < 1$,

$$f \in \mathcal{P}(1,s) \cap \mathcal{P}(1/s,1) \implies \|f\| \leq s.$$

□

Theorem 1. $(\mathcal{P}, +, \cdot)$ *is a complete topological ring, and the composition map $\mathcal{P} \times \mathcal{P} \to \mathcal{P}$ is continuous. Also, $(\mathcal{F}, +, \circ)$ is a complete topological ring.*

Proof. The triangle inequality for $\| \ \|$ implies that addition is continuous. To check that multiplcation is continuous, we must show that if $f, g \in \mathcal{P}$, and $r, s > 0$, then for f_0, g_0 sufficiently small,

$$(f + f_0) \cdot (g + g_0) - f \cdot g \in \mathcal{P}(r,s).$$

Since f and g are bounded on Δ_R, this follows for $f_0, g_0 \in \mathcal{P}(r, \epsilon)$ for sufficiently small $\epsilon > 0$.

Now let us show that $\mathcal{P}$ is complete. It suffices to show that if $f_1, f_2, \ldots$ is a sequence in $\mathcal{P}$ tending to zero, then $\sum_{i=1}^{\infty} f_i$ converges to another element of $\mathcal{P}$. For each $e \in E$, the coefficients of z^e in f_i tend to zero by Lemma 1, so they sum to some $a_e \in C$. Interchanging the order of summation shows that $\sum_{i=1}^{\infty} f_i$ converges to $f \stackrel{\text{def}}{=} \sum_{e \in E} a_e z^e$ uniformly on bounded subsets, and that $f \in \mathcal{P}$.

For the continuity of composition, we must show that for f_0, g_0 sufficiently small,

$$(f + f_0) \circ (g + g_0) - f \circ g \in \mathcal{P}(r,s). \tag{1}$$

Let $R = \sup |g(\Delta_r)|$. If $g_0 \in \mathcal{P}(r, R)$ and $f_0 \in \mathcal{P}(R, s)$, then

$$f_0 \circ (g + g_0) \in \mathcal{P}(r,s). \tag{2}$$

By Proposition 5, f is uniformly continuous on Δ_R, so if $g_0 \in \mathcal{P}(r, \epsilon)$ for sufficiently small ϵ,

$$f \circ (g + g_0) - f \circ g \in \mathcal{P}(r,s). \tag{3}$$

Adding (2) and (3) yields (1).

By restriction from $\mathcal{P}$ to $\mathcal{F}$, the ring operations on $\mathcal{F}$ are continuous. As remarked earlier, $\mathcal{F}$ is a closed subset of $\mathcal{P}$, so the completeness of $\mathcal{F}$ follows from that of $\mathcal{P}$. □

Although the ring operations for both $\mathcal{P}$ and $\mathcal{F}$ are continuous with respect the topology induced by $\| \|$, it is not true that $\|f \cdot g\| \le \|f\| \cdot \|g\|$ for all $f, g \in \mathcal{P}$; nor is it true that $\|f \circ g\| \le \|f\| \cdot \|g\|$ for all $f, g \in \mathcal{F}$. In fact, these can fail even if $f \in C$. The following proposition shows that this defect of $\| \|$ is unavoidable. (This is different from the theory of Banach algebras, in which if one has a norm for which multiplication is continuous in each variable, one can define a new norm with the sub-multiplicative property. See Section 3.1 of [12].)

Proposition 9. *There is no norm $\| \|'$ on $\mathcal{P}$ inducing the same topology as above and satisfying*

1. $\|f\|' \ge 0$ *with equality if and only if* $f = 0$.
2. $\|f \pm g\|' \le \|f\|' + \|g\|'$
3. $\|1\|' = 1$.
4. $\|f \cdot g\|' \le \|f\|' \cdot \|g\|'$.

Similarly, there is no norm $\| \|'$ on $\mathcal{F}$ inducing the same topology and satisfying (1), (2), (3), and (4) with $\cdot$ replaced by $\circ$.

Proof. Suppose there were such a norm on $\mathcal{P}$. As $\epsilon \to 0$ in C, $\epsilon z \to 0$ in $\mathcal{P}$, so $\|\epsilon z\|' < 1$ for some nonzero $\epsilon \in C$. Then the series $1 + \epsilon z + (\epsilon z)^2 + \cdots$ should converge in $\mathcal{P}$ to an inverse of $1 - \epsilon z$. This is impossible since $1 - \epsilon z$ is zero at $z = 1/\epsilon$.

Similarly, since $1 - \epsilon\tau$ has no inverse (with respect to composition), there cannot be a sub-multiplicative norm on $\mathcal{F}$. $\square$

4. A Class of Locally Compact Subspaces of C

For $z \in C^*$, let

$$v(z) = -\log |z| \in \mathbb{R}$$

be the (additive) valuation associated with $| \, |$. By convention, $v(0) = +\infty$.

If $f \in \mathcal{F}^+$, then as is well-known, $\ker f$ is a discrete sub-$\mathbb{F}_q$-vector space of C, which is "concentrated near infinity" in the sense that if it is infinite, it is countable and its elements tend to infinity. If $f \in \mathcal{F}^-$, it will turn out that $G \stackrel{\text{def}}{=} \ker f$ is a *compact* sub-$\mathbb{F}_q$-vector space of C, this time "concentrated near zero" in the sense that the integral $\int_G v$ of the valuation with respect to Haar measure on G is $+\infty$. The kernel of a general (i.e., possibly infinite in both directions) element of $\mathcal{F}$ will belong to a certain hybrid of these two classes of vector spaces, which we now define.

Definition. Fix a real number $r > 0$. Let $\mathcal{G}$ be the collection of sub-$\mathbb{F}_q$-vector spaces G of C satisfying the following conditions:

1. $G \cap \Delta_r$ is compact.
2. $\int_{G \cap \Delta_r} v = +\infty$. The integral is with respect to (any) Haar measure on $G \cap \Delta_r$.
3. $G \cap \Delta_r$ has finite or countable index in G, and in the latter case, if $g_1, g_2, \dots$ is a system of coset representatives, then $\lim_{n \to \infty} |g_n| = +\infty$.

Definition. Let G be a sub-$\mathbb{F}_q$-vector space of C. Let $\{\lambda_n\}_{n\in\mathbb{Z}}$ be a bi-infinite collection of elements of C, possibly terminating on either side. We say $\{\lambda_n\}_{n\in\mathbb{Z}}$ is a *descending basis* for G if

(1) The λ_n are independent over $\mathbb{F}_q$ and the closure of their span is G.
(2) For each $m \in \mathbb{Z}$ (for which λ_m exists), λ_m is a smallest nonzero element of the $\mathbb{F}_q$-vector space spanned by $\{\, \lambda_n \mid n \le m \,\}$.
(3) The sequence terminates on the left, or $\lim_{n\to-\infty} |\lambda_n| = \infty$.
(4) The sequence terminates on the right, or $\sum_{n=1}^{\infty} v(\lambda_n) q^{-n} = +\infty$.

Proposition 10. *Let G be a sub-$\mathbb{F}_q$-vector space of C. Then*

(1) *The definition of $\mathcal{G}$ does not depend on the choice of $r > 0$.*
(2) *G has a descending basis if and only if $G \in \mathcal{G}$.*
(3) *If $G \in \mathcal{G}$, then G is locally compact.*
(4) *For G discrete, $G \in \mathcal{G}$ if and only if it is finite or countable, with its elements tending to infinity in the latter case.*
(5) *For G compact, $G \in \mathcal{G}$ if and only if $\int_G v = +\infty$.*
(6) *If $G \in \mathcal{G}$, then any closed sub-$\mathbb{F}_q$-vector space H of G also belongs to $\mathcal{G}$.*

Proof.
Proof of (2): Suppose G has a descending basis $\{\lambda_n\}$. Then the λ_n are decreasing in size by condition (2) in the definition, and $G \cap \Delta_r$ is the closure of the span of the $\{\lambda_n : n \ge n_0\}$ where λ_{n_0} is the first λ of absolute value at most r. If the sequence of λ_n after λ_{n_0} terminates, then $G \cap \Delta_r$ is finite, hence compact. Otherwise, these λ_n form a sequence tending to zero by condition (4), and we get a topological isomorphism $\mathbb{F}_q^\omega \to G \cap \Delta_r$ which sends $(a_0, a_1, a_2, \dots)$ to $\sum_{i=0}^{\infty} a_i \lambda_{n_0+i}$. (This, together with Theorem 3, proves the remark in the introduction regarding the topological group structure of the kernel of an element of $\mathcal{F}^-$.) Hence $G \cap \Delta_r$ is compact in any case. Thus condition (1) of the definition of $\mathcal{G}$ is verified for G.

Assume that the Haar measure on G is normalized so that the open subspace $G\cap\Delta_r$ has measure 1. If $G \cap \Delta_r$ is finite, then $\int_{G\cap\Delta_r} v = +\infty$ since 0 has positive measure. Otherwise, under the isomorphism above, the set of $(a_0, a_1, a_2, \dots) \in \mathbb{F}_q^\omega$ such that the first nonzero a is a_i corresponds to a subset of $G \cap \Delta_r$ of measure $q^{-i} - q^{-i-1}$, and the function v takes the value $v(\lambda_{n_0+i})$ everywhere on this subset, since otherwise some nontrivial combination of the λ's of the same size as λ_{n_0+i} would be closer to zero than λ_{n_0+i}, violating condition (2) in the definition of decreasing basis. These sets cover $\mathbb{F}_q^\omega$ (except for the point 0), so

$$\int_{G\cap\Delta_r} v = \sum_{i=0}^{\infty} v(\lambda_{n_0+i})(q^{-i} - q^{-i-1}).$$

This is $+\infty$, since it agrees up to a finite number of terms with

$$(1-q^{-1})q^{n_0}\sum_{n=1}^{\infty} v(\lambda_n)q^{-n}.$$

(Substitute $n = n_0 + i$.) Hence condition (2) of the definition of $\mathcal{G}$ holds.

Also, the finite linear combinations of the λ_n for $n < n_0$ are coset representatives for $G \cap \Delta_r$ in G, so condition (3) of the definition of $\mathcal{G}$ follows from properties (2) and (3) of a decreasing basis. Hence $G \in \mathcal{G}$.

Conversely, suppose $G \in \mathcal{G}$. Since $G \cap \Delta_r$ is compact, only zero can be a limit point of $\{|x| : x \in G \cap \Delta_r\}$. Combined with condition (3) of the definition of $\mathcal{G}$, this implies that the nonzero absolute values of elements of G consist of a decreasing sequence $\{r_n\}_{n\in\mathbb{Z}}$, possibly terminating in either direction. For each r_n, choose an $\mathbb{F}_q$-basis for $(G\cap\Delta_{r_n})/(G\cap\Delta'_{r_n})$, which is finite, by condition (1) in the definition of $\mathcal{G}$ when $r_n \le r$, and by condition (3) when $r_n > r$. We claim that the concatenation of these bases (lifted to C) is a descending basis for G. Properties (1) and (2) of a descending basis are clearly satisfied. Property (3) follows from condition (3) in the definition of $\mathcal{G}$, and property (4) is equivalent to condition (2) in the definition of $\mathcal{G}$, as in the proof of the converse above.

Proof of (1), (3), (4), and (5): Part (1) follows trivially from (2). Part (3) follows since if $G \in \mathcal{G}$, the open subgroup $G \cap \Delta_r$ is compact. For part (4), we may assume by (1) that r is smaller than the absolute value of the smallest nonzero element of G, and see what the conditions in the definition of $\mathcal{G}$ say in this case. Similarly, part (5) follows by assuming r is greater than the absolute value of all elements of G.

Proof of (6): In constructing a descending basis for G as in the proof of (2), we may assume that the chosen basis for $(G\cap\Delta_{r_n})/(G\cap\Delta'_{r_n})$ contains a basis for its subspace $(H\cap\Delta_{r_n})/(H\cap\Delta'_{r_n})$. It is then easy to check that the concatenation of the latter bases (lifted to C) is a descending basis for H, so that $H \in \mathcal{G}$ by (2). $\square$

5. Maps and Fibers

Here we state basic results on the maps on C defined by elements of $\mathcal{P}$ or $\mathcal{F}$, and in particular study their fibers. The proofs will be postponed until the next section. First we have a fractional version of "Picard's Theorem," which in the non-archimedean situation asserts that non-constant everywhere convergent power series are surjective. The openness of the map is a kind of local surjectivity.

Theorem 2. *If $f \in \mathcal{P}$ is not a constant series, then $f : C \to C$ is a surjective open map.*

This theorem has two easy consequences.

Corollary 1. *If $f, g \in \mathcal{P}$ are not constant, then $f \circ g$ is not constant. In particular, the noncommutative ring $\mathcal{F}$ has no zero divisors.*

Corollary 2. *Distinct series of $\mathcal{P}$ yield distinct maps on C.*

Theorem 3. *If $f = \sum_{e \in E} a_e z^e \in \mathcal{P}$ is not constant, then for each $c \in C$, $f^{-1}(c)$ is a locally compact subset of C, and is compact if and only if there is a largest e for which $a_e \neq 0$. If $f = \sum_{n \in \mathbb{Z}} a_n \tau^n \in \mathcal{F}$ is nonzero, then $G \overset{def}{=} \ker f$ is in $\mathcal{G}$. Moreover,*

$$\begin{aligned} G \text{ is discrete} &\iff a_n = 0 \text{ for } n \ll 0. \\ G \text{ is compact} &\iff a_n = 0 \text{ for } n \gg 0. \end{aligned}$$

(The last two statements are dual in the sense of Section 8.) We have a converse for $f \in \mathcal{F}$:

Theorem 4. *Each $G \in \mathcal{G}$ is the kernel of some $f \in \mathcal{F}$. The f is essentially unique: any $g \in \mathcal{F}$ with the same kernel is of the form $\epsilon\tau^n \circ f$ for some $\epsilon \in C^*$ and $n \in \mathbb{Z}$. (In other words, by Corollary 5 below, g differs from f only by a unit of $\mathcal{F}$.)*

Because C is not locally compact, Theorem 3 implies it is not the union of $f^{-1}(0)$ and $g^{-1}(0)$ for nonzero $f, g \in \mathcal{P}$. This proves the following.

Corollary 3. *The commutative ring $\mathcal{P}$ has no zero divisors.*

Recall that for a power series $f(z) = \sum_{i=0}^{\infty} a_i z^i \in C[[z]]$, the Newton polygon is the lower convex hull of the set of points $(i, v(a_i))$ in the plane, and that the Newton polygon gives information on the valuations of the zeros of f. (See [1], [3], [13], [14], or [16].) Similarly, we define the Newton polygon of $f = \sum_{e \in E} a_e z^e \in \mathcal{P}$ to be the lower convex hull of the set of points $(e, v(a_e))$ in the plane. Let v_p denote the p-adic valuation on $\mathbb{Q}$. For $f = \sum_{e \in E} a_e z^e \in \mathcal{P}$, and $n \geq 0$, define

$$f_n = \sum_{v_p(e) \geq -n} a_e z^e. \tag{4}$$

Therefore f_n is the p^n-th root of a power series. Since f is convergent everywhere, we see that the f_n converge to f uniformly on bounded subsets (hence also in $\mathcal{P}$) as n tends to infinity.

Theorem 5. *Suppose $f \in \mathcal{P}$ is not constant, and $c \in C$. Then there is a canonical measure μ on $f^{-1}(c)$, characterized by*

$$\mu\left(f^{-1}(c) \cap (\alpha + \Delta_r)\right) = \lim_{n \to \infty} \frac{\#\text{ zeros of } (f_n - c)^{p^n} \text{ in } (\alpha + \Delta_r)}{p^n},$$

for all $\alpha \in C$, $r > 0$. (Here zeros are to be counted with multiplicity.) The horizontal length of the segment of the Newton polygon of $f - c$ having slope s (if any) equals

$$\mu(\{\, z \in f^{-1}(c) \mid v(z) = -s \,\}).$$

Also,

$$\mu(f^{-1}(c)) = \sup\{\, e \mid a_e \neq 0 \,\}.$$

(Both might be $+\infty$.) If $f \in C[[z]]$, then μ is the "counting measure"; i.e., $\mu(\{x\})$ is the multiplicity of x as a zero of $f - c$. Finally, if $f \in \mathcal{F}$ is nonzero and $c = 0$, then μ is a Haar measure on the locally compact group $\ker f$.

Corollary 4. *If $f \in \mathcal{P}$ vanishes only at 0, then $f(z) = az^e$ where $a \in C^*$ and $e \in E$.*

Proof. By Theorem 5, any series with at least two monomials has a ero of nonzero valuation. □

Corollary 5. *The unit group of $\mathcal{F}$ consists of the elements of the form $a\tau^n$ where $a \in C^*$ and $n \in \mathbb{Z}$.*

Proof. Any unit of $\mathcal{F}$ must have trivial kernel, and so must be of the form in Corollary 4, with the exponent a power of q. On the other hand, it is easy to write down inverses of elements of this form. □

Theorem 6. *Let f, g be nonzero elements of $\mathcal{F}$. Then $\ker g \subseteq \ker f$ if and only if there exists $h \in \mathcal{F}$ such that $f = h \circ g$. In this case, the h is unique, and $\ker h = g(\ker f)$.*

6. Proofs

Here we provide proofs of the theorems stated in the previous section.

Lemma 2. *Suppose $f(z) = \sum_{v_p(e) \geq -n} a_e z^e \in \mathcal{P}$, and $j > 0$ is such that $a_j \neq 0$. Then there exists $x \in C$ such that $f(x) = 0$ and $|x| \leq |f(0)/a_j|^{1/j}$.*

Proof. This follows from looking at the Newton polygon for the (ordinary) power series $f(z)^{p^n}$. □

Let f_n be as in (4).

Lemma 3. *Suppose $f \in \mathcal{P}$ is not a constant series. Fix $r, R \in \mathbb{R}$, with $0 < r < R$, and fix $c \in C$. Then the images of $f^{-1}(c) \cap \Delta_R$ and $f_n^{-1}(c) \cap \Delta_R$ in Δ_R/Δ_r coincide for $n \gg 0$.*

Proof. By considering $f - c$, we may assume $c = 0$. By composing with scalar multiplcations on both sides, we may assume $R = 1$, and that the largest coefficient of f other than the constant coefficient is of absolute value 1. Let $a_e z^e$ be the term of f with largest e for which $|a_e| = 1$. Let $\epsilon_n = \sup |(f_{n+1} - f_n)(\Delta_R)|$. Since $f_n \to f$, $\epsilon_n \to 0$.

Suppose $\lambda_n \in f_n^{-1}(0) \cap \Delta_R$. Then

$$|f_{n+1}(\lambda_n)| = |(f_{n+1} - f_n)(\lambda_n)| \leq \epsilon_n.$$

Provided that $n+1 \geq -v_p(e)$, the coefficient of z^e in $f_{n+1}(z+\lambda_n)$ has absolute value 1, by choice of e and since $|\lambda_n| \leq 1$. Hence by Lemma 2, there exists z_n such that $|z_n| \leq \epsilon_n^{1/e}$ and

$$f_{n+1}(z_n + \lambda_n) = 0.$$

Let $\lambda_{n+1} = z_n + \lambda_n$. Provided n was chosen large enough, we can repeat the argument to construct a sequence $\lambda_n, \lambda_{n+1}, \lambda_{n+2}, \ldots$ with $\lambda_i \in f_i^{-1}(0)$ and

$$|\lambda_{i+1} - \lambda_i| \leq \epsilon_i^{1/e} \leq r.$$

Since $\epsilon_i \to 0$, the λ_i converge to a limit λ_∞ with $|\lambda_\infty - \lambda_n| \leq r$. Also since $f_n \to f$ uniformly on Δ_R,

$$f(\lambda_\infty) = \lim_{i\to\infty} f_i(\lambda_i) = 0.$$

For the other direction, suppose $\lambda \in f^{-1}(0) \cap \Delta_R$. By Lemma 2, for $n \gg 0$, there exists z_n such that $f_n(z_n + \lambda) = 0$ and

$$|z_n| \leq |f_n(\lambda)|^{1/e} \to 0$$

as $n \to \infty$. In particular, for sufficiently large n (and how large does not depend on λ), $|z_n| \leq r$, so $z_n + \lambda \in f_n^{-1}(0)$ is in the same coset of Δ_r as λ. □

From the preceding we can deduce two useful corollaries. First of all, we see that Lemma 2 extends to arbitrary non-constant $f \in \mathcal{P}$.

Corollary 6. *Suppose $f(z) = \sum_{e\in E} a_e z^e \in \mathcal{P}$, and $j > 0$ is such that $a_j \neq 0$. Then there exists $x \in C$ such that $f(x) = 0$ and $|x| \leq |f(0)/a_j|^{1/j}$.*

Next we have a finiteness result, which will be used to prove that fibers are locally compact.

Corollary 7. *If $f \in \mathcal{P}$ is non-constant, $0 < r < R$, and $c \in C$, then the image of $f^{-1}(c) \cap \Delta_R$ in Δ_R/Δ_r is finite.*

Proof. The result with f replaced by f_n is proved by applying the theory of Newton polygons to the power series $f_n^{p^n} - c^{p^n}$. Now apply Lemma 3. □

Proof of Theorem 2. Applying Corollary 6 to $f - c$ where $f \in \mathcal{P}$ is not a constant series and $c \in C$ shows that there is a solution to $f(z) - c = 0$, so f is surjective.

In checking that f defines an open map, we may reduce to proving f is open at 0, by composing f with a translation. Moreover we may assume $f(0) = 0$. If $c \in C$ is small, Corollary 6 applied to $f - c$ shows that $f(z) - c = 0$ has a solution near 0. This is exactly what is needed to prove that f is open at 0. □

Proof of Theorems 3 *and* 5. First let us show that for any $r > 0$, $f^{-1}(c) \cap \Delta_r$ is compact. Suppose $\alpha_1, \alpha_2, \dots$ is a sequence in $f^{-1}(c) \cap \Delta_r$. By Corollary 7, these elements lie in finitely many cosets of $\Delta_{r/2}$, so we can find an infinite subsequence within one coset. Next we can find a subsequence of this subsequence lying within a single coset of $\Delta_{r/3}$, and so on, with the n-th subsequence lying within a coset of $\Delta_{r/n}$. By diagonalization we obtain a convergent subsequence of the original sequence. Since f is continuous, $f^{-1}(c)$ is closed (and so is Δ_r), so the limit lies in $f^{-1}(c) \cap \Delta_r$. Thus $f^{-1}(c) \cap \Delta_r$ is compact. Taking larger and larger r shows that $f^{-1}(c)$ is locally compact.

Before completing the proof of Theorem 3, let us turn to Theorem 5. First we check that the limit in the definition of μ exists. Without loss of generality we may assume $c = 0$. Also we may assume $\alpha = 0$, by considering $f(z + \alpha)$. Let $\ell_r(f)$ denote the total horizontal length of the segments of the Newton polygon of f whose slope is less than $\log r$, which is the largest x-coordinate of a point of contact of the Newton polygon with a supporting line of slope $\log r$. The fact that f is everywhere convergent implies that below any line in $\mathbb{R}^2$ there are at most finitely vertices, so for each r, $\ell_r(f_n) = \ell_r(f)$ for $n \gg 0$.

The Newton polygon for $f_n^{p^n}$ is the dilation of that of f_n by the factor p^n, so $\ell_r(f_n^{p^n}) = p^n \ell_r(f_n)$. The theory of Newton polygons for ordinary power series implies that $\ell_r(f_n^{p^n})$ counts the number of zeros of $f_n^{p^n}$ (with multiplicity) in Δ_r, so the limit in the definition of μ (for $c = \alpha = 0$) converges to $\ell_r(f)$.

To check that μ is truly a measure, it will suffice to check that the definition is consistent in the sense that when $r < R$, its value on $f^{-1}(c) \cap (\beta + \Delta_R)$ equals the sum of its values on $f^{-1}(c) \cap (\alpha + \Delta_r)$ with $\alpha + \Delta_r$ ranging over the cosets of Δ_r contained in $\beta + \Delta_R$. By Lemma 3 and Corollary 7, we need concern ourselves with only finitely many of these cosets. Now the result is clear from the finite additivity of the right hand side of the definition of μ.

By what we have shown so far,

$$\mu(\{\, z \in f^{-1}(0) : |z| \leq r \,\}) = \ell_r(f).$$

Taking this and subtracting the same with r replaced by $r - \epsilon$ (with $s = \log r$, and ϵ sufficiently small) shows that

$$\mu(\{\, z \in f^{-1}(c) \mid v(z) = -s \,\})$$

equals the horizontal length of the Newton polygon segment of slope s.

We now check the final statements of Theorem 5. By what we have shown so far, $\mu(f^{-1}(c))$ is the sum of the horizontal lengths of all the segments, and this is clearly $\sup\{\, e \mid a_e \neq 0 \,\}$. If $f \in C[[z]]$, the theory of Newton polygons for power series tells us that the lengths of the horizontal segments are counting zeros, so μ is the counting measure. Finally, if $f \in \mathcal{F}$ is nonzero and $c = 0$, it is clear from the definition that μ is translation-invariant on the locally compact group $\ker f$. Moreover, $\mu(\ker f) > 0$

by the formula we just derived for the measure of the whole space. Thus μ is a Haar measure on $\ker f$. This completes the proof of Theorem 5.

We now resume the proof of Theorem 3. First, if there is a largest e for which $a_e \neq 0$, then the slopes of the Newton polygon of $f - c$ are bounded above for each $c \in C$, and hence by Theorem 5, $f^{-1}(c) \subset \Delta_r$ for some $r > 0$. Thus $f^{-1}(c) = f^{-1}(c) \cap \Delta_r$, which we showed already was compact. On the other hand, if there is no largest e for which $a_e \neq 0$, then the Newton polygon of $f - c$ has infinitely many segments of increasing slope, so there is a sequence of elements in $f^{-1}(c)$ of decreasing valuation. Such a sequence cannot have a convergent subsequence, so $f^{-1}(c)$ is not compact.

From now on, we assume $f = \sum_{n \in \mathbb{Z}} a_n \tau^n \in \mathcal{F}$, $c = 0$, and $G = \ker f$. By the first paragraph of this proof, $G \cap \Delta_r$ is compact for any $r > 0$, proving that G satisfies condition (1) in the definition of $\mathcal{G}$. Also by Corollary 7, the image of $\ker f \cap \Delta_{nr}$ in Δ_{nr}/Δ_r is finite for all n, so condition (3) in the definition of $\mathcal{G}$ follows.

Now we check condition (2); i.e., that if $r > 0$, then $\int_{G \cap \Delta_r} v = +\infty$. If we integrate only over the subset

$$\{ z \in G \mid v(z) = -s \}$$

we get $-s$ times the Haar measure of this set, which, by what we just proved, is the same as $-s$ times the horizontal length of the segment of the Newton polygon of slope s, which is the *vertical* displacement as one moves along the segment from right to left. If we sum over all the segments of slopes less than $\log r$, we deduce that $\int_{G \cap \Delta_r} v$ equals the vertical displacement as one moves along the section of the Newton polygon to the left, starting at some point depending on r. This vertical displacement is $+\infty$, since $v(a_n) \to +\infty$ as $n \to -\infty$.

Thus $G \in \mathcal{G}$. Finally, we check the last equivalences in Theorem 3. First, G is discrete if and only if there are no zeros of large finite positive valuation. By Theorem 5, this happens if and only if $a_n = 0$ for $n \ll 0$. Lastly, the criterion for G to be compact follows from our earlier criterion for fibers of general elements of $\mathcal{P}$. $\square$

For future reference, we record the following well-known result.

Lemma 4. *If the zeros of a separable polynomial $f(z) \in C[z]$ form a sub-$\mathbb{F}_q$-vector space of C, then $f \in C\{\tau\}$.*

Proof. Proposition 1.3 in [4] proves this for $q = p$, so f is an additive polynomial. Comparing zeros and linear coefficients shows that $f(cz) = cf(z)$ for all $z \in \mathbb{F}_q$, and this forces $f \in C\{\tau\}$. $\square$

Lemma 5. *If $G \in \mathcal{G}$ and $f \in \mathcal{F}$ has kernel $G \cap \Delta_r$ for some $r > 0$, then $f(G)$ is in $\mathcal{G}$ and is discrete.*

Proof. Since f has compact kernel, its coefficient of τ^n is zero for $n \gg 0$ by Theorem 3. Hence in the series for $f(z)$, the last term dominates for large z. Thus $|f(z)| \to \infty$ as $|z| \to \infty$. Let $g_1, g_2, \dots$ be representatives for the cosets of $G \cap \Delta_r$. These form a sequence tending to infinity, by condition (3) in the definition of $\mathcal{G}$. Then

$$f(G) = \{f(g_1), f(g_2), \dots\}$$

also consists of a sequence tending to infinity, so it is in $\mathcal{G}$ and is discrete. $\square$

Proof of Theorem 4, *existence.*
Case 1: G discrete.
Then by Lemma 4, we may take

$$f(z) = z \prod_{g \in G, g \neq 0} (1 - z/g).$$

Case 2: G compact.
We may assume G is infinite, since otherwise we are in Case 1. Without loss of generality suppose $G \subset \Delta_1$. (If for some small $c \in C$ we can get cG as a kernel of f, then we can get G as the kernel of $f(cz)$.)

By Proposition 10, there exists a descending basis $\lambda_1, \lambda_2, \dots$ for G. (It terminates on the left by condition (3) of the definition of a descending basis.) Let V_n be the $\mathbb{F}_q$-vector space generated by $\lambda_1, \dots, \lambda_n$. Define

$$g_n(z) = \prod_{\lambda \in V_n} (z - \lambda), \qquad h_n(z) = g_n(z)^{1/q^n}.$$

By Lemma 4, $g_n \in C\{\tau\}$, so $h_n \in \mathcal{F}^-$, and both have coefficients bounded in absolute value by 1, since $G \subset \Delta_1$. We will eventually show that the h_n converge to the desired $f \in \mathcal{F}^-$.

We have

$$g_{n+1}(z) = g_n(z)^q - g_n(\lambda_{n+1})^{q-1} g_n(z)$$

since both sides are monic $\mathbb{F}_q$-linear polynomials of degree q^{n+1} which vanish on V_{n+1}. Raising to the $1/q^{n+1}$ power yields

$$h_{n+1}(z) = h_n(z) - c_n h_n(z)^{1/q} \tag{5}$$

where $c_n = h_n(\lambda_{n+1})^{1-1/q}$.

We claim that $|c_n| \to 0$ as $n \to \infty$. We have

$$\begin{aligned} v(h_n(\lambda_{n+1})) &= 1/q^n \sum_{\lambda \in V_n} v(\lambda_{n+1} - \lambda) \\ &\geq 1/q^n \sum_{\lambda \in V_n} \min\{v(\lambda_{n+1}), v(\lambda)\} \\ &\geq 1/q^n \sum_{\lambda \in V_n, \lambda \neq 0} v(\lambda), \end{aligned}$$

since $v(\lambda_{n+1}) \geq v(\lambda)$ for all nonzero $\lambda \in V_n$, by the definition of descending basis. As $n \to \infty$, this tends to $⨍_G v = +\infty$. Hence

$$|c_n| = \exp(-(1 - 1/q)v(h_n(\lambda_{n+1}))) \to 0.$$

By (5), we see that

$$\|h_{n+1}(z) - h_n(z)\| = \|c_n h_n(z)^{1/q}\| \leq |c_n| \to 0$$

as $n \to \infty$. Hence the h_n converge to some $f \in \mathcal{F}$.

If $z \in V_n$, then $h_i(z) = 0$ for $i \geq n$, so $f(z) = 0$. Thus $\ker f$ contains $\bigcup_{n=1}^{\infty} V_n$ and its closure, which is G. On the other hand, if $z \notin G$, and we set

$$\delta = \inf_{\lambda \in G} |z - \lambda|,$$

then directly from the definitions of $g_n(z)$ and $h_n(z)$ we get

$$|g_n(z)| \geq \delta^{q^n}, \qquad |h_n(z)| \geq \delta,$$

for all n, so in particular, $f(z) = \lim_{n\to\infty} h_n(z) \neq 0$. Hence $\ker f = G$, as desired.

Case 3: $G \in \mathcal{G}$ arbitrary.
By Case 2, we can find $g \in \mathcal{F}$ with kernel $G \cap \Delta_1$. By Lemma 5, $g(G)$ is in $\mathcal{G}$ and is discrete, so by Case 1, there exists $h \in \mathcal{F}$ with kernel $g(G)$. Let $f = h \circ g$. Then

$$f(x) = 0 \iff h(g(x)) = 0 \iff g(x) \in g(G) \iff x \in G,$$

since $\ker g \subseteq G$. $\square$

Before proving Theorem 6 and the uniqueness part of Theorem 4, let us prove the following "remainder" lemma.

Lemma 6. *If $f \in \mathcal{F}$, then there exists $q \in \mathcal{F}$ such that*

$$f = q \circ (1 - \tau) + f(1).$$

Proof. Suppose $f = \sum_{n\in\mathbb{Z}} a_n \tau^n \in \mathcal{F}$. Without loss of generality, assume $f(1) = \sum_{n\in\mathbb{Z}} a_n = 0$. Then the rate of growth of the a_n imposed by Proposition 1 implies that if

$$b_n \stackrel{\text{def}}{=} \sum_{m=-\infty}^{n} a_m = -\sum_{m=n+1}^{\infty} a_m,$$

then $q \stackrel{\text{def}}{=} \sum_{n\in\mathbb{Z}} b_n \tau^n$ belongs to $\mathcal{F}$. (Use the first definition of b_n to get convergence on the left, and the second for convergence on the right.) Now

$$q \circ (1 - \tau) = \sum_{n\in\mathbb{Z}} (b_n - b_{n-1})\tau^n = \sum_{n\in\mathbb{Z}} a_n \tau^n = f.$$

$\square$

Proofs of Theorem 6 *and the uniqueness in Theorem* 4. In Theorem 6, it is clear that if $f = h \circ g$, then $\ker g \subseteq \ker f$, so we will concern ourselves with converse, that if $\ker g \subseteq \ker f$, then there exists $h \in \mathcal{F}$ such that $f = h \circ g$. Then the uniqueness of h is clear from Corollary 1, and $\ker h$ must be $g(\ker f)$ by the surjectivity of g from Theorem 2.

Step 1: Prove Theorem 6 for $g = \alpha_0 \circ (1-\tau) \circ \alpha_1 \circ (1-\tau) \circ \alpha_2 \cdots (1-\tau) \circ \alpha_d$, where $\alpha_0, \alpha_1, \dots, \alpha_d \in C^*$.

We use induction on d. The base case $d = 0$ is trivial. Suppose $d \geq 1$. Let $\tilde{g} = \alpha_1 \circ (1-\tau) \circ \alpha_2 \cdots (1-\tau) \circ \alpha_d$. Then the inductive hypothesis implies that $f = j \circ \tilde{g}$ for some $j \in \mathcal{F}$. Since f kills $\ker g$, j kills $\tilde{g}(\ker g) = \ker(\alpha_1 \circ (1-\tau)) = \mathbb{F}_q$. In particular j kills 1, so by Lemma 6, $j = q \circ (1-\tau)$ for some q. If we now let $h = q \circ \alpha_0^{-1}$, then $f = h \circ g$.

Step 2: Every separable $g \in C\{\tau\}$ of τ-degree d is of the form in Step 1.

Again we use induction on d. The base case $d = 0$ is trivial. If $d \geq 1$, there exists $c \in \ker g$, $c \neq 0$. Then g kills $\ker((1-\tau) \circ c^{-1})$, so $g = h \circ (1-\tau) \circ c^{-1}$ for some $h \in \mathcal{F}$ by Step 1, and the proof of the existence of h in fact shows that h must be a separable element of $C\{\tau\}$. Applying the inductive hypothesis to h produces the desired factorization.

Step 3: Theorem 6 holds when $g \in C\{\tau, \tau^{-1}\}$.

Let τ^n be the lowest (most negative) power occuring in g. Then by Steps 1 and 2, we can write $f = h' \circ (\tau^{-n} \circ g)$, so we can take $h = h' \circ \tau^{-n}$.

Step 4: If $g_n, h_n \in \mathcal{F}$ are nonzero, $f = h_n \circ g_n$ for each n, and the g_n converge to some nonzero $g \in \mathcal{F}$, then the h_n converge to some $h \in \mathcal{F}$ and $f = h \circ g$.

Fix $x \in C$. We have $h_n(x) = f(g_n^{-1}(x))$ where $g_n^{-1}(x)$ denotes any $y_n \in C$ such that $g_n(y_n) = x$. (By Theorem 2, such y_n exist.) We will construct a sequence of such y_n which *converges*. Fix a nonzero term $a_j \tau^j$ in g. Choose some large $R > 0$, then choose some large $n_0 > 0$. (We'll specify how large as we go along; how large we need n_0 to be depends on how large R was taken to be.) If $n \gg n_0$, the coefficient of τ^j in g_n has the same absolute value as a_j, provided n_0 was chosen large enough. Then by Corollary 6, there exists a solution $y_{n_0} \in \Delta_R$ to $g_{n_0}(y_{n_0}) = x$, if R was chosen large enough. Now inductively define ϵ_n and $y_{n+1} \in \Delta_R$ for $n \geq n_0$ as follows. Pick ϵ_n such that $g_{n+1}(\epsilon_n) = (g_n - g_{n+1})(y_n)$, and set $y_{n+1} = y_n + \epsilon_n$. Since the g_n converge uniformly on Δ_R, and since $y_n \in \Delta_R$ by the inductive hypothesis, $(g_n - g_{n+1})(y_n)$ can be assumed to be arbitrary small, if n_0 was chosen large enough. Then by Corollary 6, $\epsilon_n \in \Delta_R$, $y_{n+1} \in \Delta_R$, and

$$\begin{aligned} g_{n+1}(y_{n+1}) &= g_{n+1}(y_n) + g_{n+1}(\epsilon_n) \\ &= g_{n+1}(y_n) + g_n(y_n) - g_{n+1}(y_n) \\ &= x. \end{aligned}$$

Moreover Corollary 6 guarantees that the ϵ_n can be chosen going to zero, so the y_n converge as desired.

Since f is continuous, we see that the sequence $h_n(x)$ converges. In fact, as is clear from the construction of the y_n, the rate of convergence depends not on x, but only on an upper bound for $|x|$, so the h_n converge uniformly on every bounded subset of C. By Theorem 1, the h_n converge to some $h \in \mathcal{F}$. Taking the limit of $f = h_n \circ g_n$ as $n \to \infty$ yields $f = h \circ g$.

Step 5: Uniqueness holds in Theorem 4 when $G \in \mathcal{G}$ is compact or discrete.

Suppose $G \in \mathcal{G}$ is compact. By the proof of existence part of Theorem 4, there is a sequence of elements $j_n \in C\{\tau, \tau^{-1}\}$ with $\ker j_n \subseteq G$, which converges to an element $j \in \mathcal{F}$ with kernel G. Let f be any other element of $\mathcal{F}$ with kernel G. By Step 3, we may write $f = h_n \circ j_n$, and then by Step 4, we may write $f = h \circ j$. But j is surjective by Theorem 2, so $\ker h = j(\ker f) = 0$ and hence h is a unit by Corollaries 4 and 5.

If $G \in \mathcal{G}$ is discrete, we can find a sequence $j_n \in C\{\tau\}$ with $\ker j_n \subseteq G$, which converges to an element $j \in \mathcal{F}$ with kernel G, so the same proof works.

Step 6: Theorem 6 holds when $\ker g$ is compact or discrete.

Indeed, by Step 5, g must be a limit of elements $g_n \stackrel{\text{def}}{=} h \circ j_n \in C\{\tau, \tau^{-1}\}$ with $\ker g_n = \ker j_n \subseteq \ker g$, and we can then apply Step 4.

Step 7: Theorem 6 holds.

By the existence part of Theorem 4, we can find $g_1 \in \mathcal{F}$ with compact kernel $G \cap \Delta_1$. By Step 6, we can write $g = j \circ g_1$, and $\ker j = g_1(\ker g)$, which is discrete by Lemma 5. By Step 6 again, we can write $f = h_1 \circ g_1$, and

$$\ker j = g_1(\ker g) \subseteq g_1(\ker f) = \ker h_1.$$

By Step 6 yet a third time, we can write $h_1 = h \circ j$. Then

$$f = h_1 \circ g_1 = h \circ j \circ g_1 = h \circ g.$$

Step 8: Uniqueness holds in Theorem 4.

Indeed, suppose f and g are nonzero elements of $\mathcal{F}$ with the same kernel. By Step 7, each of f and g is a left multiple of the other, so they differ by a unit. □

7. Pontryagin duality for A-modules

Here we recall and develop some results on locally compact topological modules to be used later in the paper. Throughout, topological groups, rings, and modules are assumed Hausdorff, and each Hom consists of continuous homomorphisms and is given the compact-open topology. If G is a locally compact abelian topological group (LCA group), its *Pontryagin dual* is $\hat{G} \stackrel{\text{def}}{=} \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{R}/\mathbb{Z})$, which is again an LCA group. The elements of $\hat{G}$ are called *characters* of G. The main theorem of Pontryagin duality is that the natural map $G \to \hat{\hat{G}}$ is an isomorphism. For an account of Pontryagin duality for groups, see [2].

The following technical result on LCA groups is due to Kaplansky (unpublished) and first appears in a paper of Glicksberg [9]. See Chapter 10 of [2] for a proof and discussion.

Proposition 11. *Let G be a group which becomes a LCA group under a topology $\mathfrak{t}$. Let $\mathfrak{t}'$ be a strictly stronger locally compact group topology on G. Then there is a $\mathfrak{t}'$-continuous character γ of G which is not $\mathfrak{t}$-continuous.*

Corollary 8. *If $f : G \to H$ is a surjective continuous homomorphism of LCA groups whose dual $\hat{f} : \hat{H} \to \hat{G}$ is also surjective, then f is a topological isomorphism.*

Proof. Since $\hat{f}$ is surjective, f is injective by P.23(b) in [2]. Thus f is an isomorphism, except that G may have a stronger topology than H. If it were strictly stronger, then by the proposition above, there would be a character of G not coming from a character of H, contradicting the surjectivity of $\hat{f}$. Therefore f is a topological isomorphism. □

Corollary 9. *Suppose G and H are LCA groups, and there is a continuous bilinear pairing*

$$G \times H \to \mathbb{R}/\mathbb{Z}$$

such that the induced maps

$$f_1 : G \to \hat{H} \quad , \quad f_2 : H \to \hat{G}$$

are surjective. Then f_1 and f_2 are topological isomorphisms.

Proof. By a well-known property of the compact-open topology, the induced maps are continuous. By Pontryagin duality (and chasing definitions), f_2 is the dual of f_1, so f_1 is a topological isomorphism by the previous corollary. The symmetric argument works for f_2. □

We will make use of the theory of Pontryagin duality for topological modules developed by Flood [7]. Let A be a locally compact commutative topological ring. Consider the class $\mathcal{A}$ of locally compact topological A-modules. If $M \in \mathcal{A}$, then the Pontryagin dual $\hat{M} \stackrel{\text{def}}{=} \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{R}/\mathbb{Z})$ of M as a topological group has a natural A-module structure, so $\hat{M} \in \mathcal{A}$. Let us restate the main theorem of [7] for this situation:

Theorem 7 (Pontraygin duality for A-modules). *For each $M \in \mathcal{A}$, the topological A-modules $\hat{M}$ and $\operatorname{Hom}_A(M, \hat{A})$ are canonically isomorphic, and the canonical* *map*

$$\begin{array}{rcl} M & \to & \mathrm{Hom}_A(\mathrm{Hom}_A(M,\hat{A}),\hat{A}) \\ m & \mapsto & (f \mapsto f(m)) \end{array}$$

is an isomorphism of topological A-modules.

If $M, N \in \mathcal{A}$, we say N is the Pontryagin dual of M as an A-module, if it is isomorphic to $\mathrm{Hom}_A(M,\hat{A})$ as a topological A-module. The following corollary is an A-module version of Corollary 9. The next corollary is useful in verifying that two elements of $\mathcal{A}$ are Pontryagin duals (as A-modules).

Corollary 10. *Suppose $M, N \in \mathcal{A}$ and there is a continuous A-module pairing $M \times N \to \hat{A}$ such that the induced maps*

$$f_1 : M \to \mathrm{Hom}_A(N,\hat{A}), \qquad f_2 : N \to \mathrm{Hom}_A(M,\hat{A})$$

are surjective. Then f_1 and f_2 are topological A-module isomorphisms.

Proof. If we compose the pairing with the evaluation-at-1 map $\hat{A} \to \mathbb{R}/\mathbb{Z}$, we get a pairing

$$M \times N \to \mathbb{R}/\mathbb{Z}$$

and the induced map $M \to \hat{N}$ is the same as f_1 once we identify $\hat{N}$ with $\mathrm{Hom}_A(N,\hat{A})$ as in Theorem 7. Similarly f_2 is the same as the induced map $N \to \hat{M}$. In particular, these induced maps are surjective, so by Corollary 9, they are topological isomorphisms. But we know that f_1 and f_2 are A-module homomorphism as well, so the result follows. □

Lemma 7. *Suppose M, N are locally compact topological $\mathbb{F}_q$-vector spaces. If there is a continuous $\mathbb{F}_q$-linear pairing*

$$\langle\ ,\ \rangle : M \times N \to \mathbb{F}_q$$

such that the induced maps

$$M \to \mathrm{Hom}_{\mathbb{F}_q}(N,\mathbb{F}_q) \quad , \quad N \to \mathrm{Hom}_{\mathbb{F}_q}(M,\mathbb{F}_q)$$

are surjective, then N is the Pontryagin dual of M as an $\mathbb{F}_q$-vector space.

If furthermore A is a locally compact $\mathbb{F}_q$-algebra and M and N are topological A-modules such that $\langle am, n\rangle = \langle m, an\rangle$ for all $a \in A$, $m \in M$ and $n \in N$, then $\mathrm{Hom}_{\mathbb{F}_q}(A,\mathbb{F}_q) \cong \hat{A}$ as topological A-modules and the map

$$\begin{array}{rcl} [\ ,\ ] : M \times N & \to & \mathrm{Hom}_{\mathbb{F}_q}(A,\mathbb{F}_q) \cong \hat{A} \\ m\ ,\ n & \mapsto & (a \mapsto \langle am, n\rangle) \end{array}$$

is a continuous A-module pairing which exhibits N as the Pontryagin dual of M as an A-module.

Proof. By counting elements, $\hat{\mathbb{F}}_q$ is a one-dimensional $\mathbb{F}_q$-vector space, and we can explicitly identify $\mathbb{F}_q$ with $\hat{\mathbb{F}}_q$ by mapping 1 to the character $\chi = (1/p) \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ of $\mathbb{F}_q$. Thus the first half of the proposition is just the special case of Corollary 10 for the discrete ring $\mathbb{F}_q$.

There is an isomorphism $\mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q) \cong \hat{A}$ of topological $\mathbb{F}_q$-vector spaces by Theorem 7 (with $M = A$, $A = \mathbb{F}_q$), and it is easily checked that it preserves the A-module structure.

As in Corollary 10, the pairing $\langle \ , \ \rangle$ induces a pairing $M \times N \to \mathbb{R}/\mathbb{Z}$ which identifies N with $\hat{M}$. The condition $\langle am, n\rangle = \langle m, an\rangle$ ensures that this isomorphism is an isomorphism of A-modules. Finally, if we identify $N \cong \hat{M}$ with $\mathrm{Hom}_A(M, \hat{A})$ using Theorem 7, we get a pairing

$$M \times N \to \hat{A}$$

exhibiting N as the Pontryagin dual of M as an A-module, and definition chasing shows that this pairing is $[\ ,\ ]$. $\square$

Now let X be a nonsingular projective curve over $\mathbb{F}_q$, let ∞ be a closed point, and let $Y = X \setminus \infty$. Let A be the Dedekind ring of regular functions on the affine curve Y, and give A the discrete topology. Let K be its fraction field, and let K_∞ be the completion of K at ∞. The Kähler differentials of A over $\mathbb{F}_q$ (see [15]), i.e., the differentials on X which are regular away from ∞, form a rank one projective A-module Ω_A inside the one-dimensional K-vector space Ω_K of Kähler differentials of K over $\mathbb{F}_q$. Therefore there is an ideal J of A isomorphic to Ω as an A-module. Let Ω_∞ be the completion of Ω_K at ∞. This is a one-dimensional vector space over K_∞. By Theorem 3 of Chapter II in [19], any nontrivial character of the locally compact field K_∞ can be used to identify K_∞ with its dual, and it follows that the map

$$\begin{aligned} K_\infty \times \Omega_\infty &\to \mathbb{F}_q \\ a\ ,\ \omega &\to \mathrm{Res}_\infty(a\omega) \end{aligned} \tag{6}$$

exhibits K_∞ and Ω_∞ as Pontraygin duals of each other, as topological $\mathbb{F}_q$-vector spaces.

Theorem 8. *Let I be a fractional ideal of A (with the discrete topology). Then the pairing (6) puts I and $\Omega_\infty/(I^{-1}\Omega_A)$ in Pontryagin duality as A-modules, so the Pontryagin dual of I as an A-module is $K_\infty/(I^{-1}J)$.*

Proof. For $\omega \in \Omega_\infty$, we claim that $\omega \in \Omega_A$ if and only if $\mathrm{Res}_\infty(a\omega) = 0$ for all $a \in A$. For $n \geq 0$, let

$$\begin{aligned} L(n\infty) &= \{\, a \in K \mid \mathrm{div}(a) \geq -n\infty \,\} \\ \Omega_{\geq n\infty} &= \{\, \eta \in \Omega_\infty \mid \mathrm{div}(\eta) \geq n\infty \,\}. \end{aligned}$$

(By the divisor of an element of Ω_∞ we mean only the part at ∞, which is the only part that makes sense.) By the Theorem at the bottom of page 160 in [5], with $h = 0$, $\mathfrak{a} = n\infty$, and dw the principal part system which equals an element of Ω_K differing from ω by an element of $\Omega_{\geq n\infty}$ at ∞, and equalling zero at other places, we have that $\operatorname{Res}_\infty(a\omega) = 0$ for all $a \in L(n\infty)$ if and only if $\omega \in \Omega_A + \Omega_{\geq n\infty}$. But $A = \bigcup_{n\geq 0} L(n\infty)$, so $\operatorname{Res}_\infty(a\omega) = 0$ for all $a \in A$ if and only if

$$\omega \in \bigcap_{n\geq 0} (\Omega_A + \Omega_{\geq n\infty}) = \Omega_A,$$

since Ω_A is a discrete subgroup of Ω_∞, and the $\Omega_{\geq n\infty}$ form a decreasing neighborhood base of 0.

Hence $\operatorname{Res}_\infty(a\omega) = 0$ for all $a \in I$ if and only if $\omega \in I^{-1}\Omega_A$. By P.22(d) in [2], the fact that the pairing (6) puts K_∞ and Ω_∞ in Pontryagin duality implies that

$$\hat{I} \cong \operatorname{Hom}_{\mathbb{F}_q}(I, \mathbb{F}_q) \cong \Omega_\infty/(I^{-1}\Omega_A) \cong K_\infty/(I^{-1}J),$$

and it is trivial to check that all our isomorphisms respect the A-module structures. □

Let $A_\mathfrak{q}$, $K_\mathfrak{q}$ denote the completions of A, K, respectively, at a nonzero prime $\mathfrak{q}$ of A.

Theorem 9. *The $A_\mathfrak{q}$-module $\operatorname{Hom}_{\mathbb{F}_q}(K_\mathfrak{q}/A_\mathfrak{q}, \mathbb{F}_q)$ is free of rank one.*

Proof. Let $t \in K$ be a uniformizing parameter at $\mathfrak{q}$. Then $A_\mathfrak{q} \cong \mathbb{F}_\mathfrak{q}[[t]]$, where $\mathbb{F}_\mathfrak{q}$ is the residue field at $\mathfrak{q}$. Now for the residue pairing

$$\begin{array}{rcl} \mathbb{F}_\mathfrak{q}((t)) \times \mathbb{F}_\mathfrak{q}((t))dt & \to & \mathbb{F}_q \\ a \quad , \quad \omega \qquad & \mapsto & \operatorname{Res}_\mathfrak{q}(a\omega) \end{array}$$

which exhibits the locally compact field $K_\mathfrak{q}$ as its own Pontryagin dual, the set of ω which give zero when paired with any $a \in \mathbb{F}_\mathfrak{q}[[t]]$ is exactly $\mathbb{F}_\mathfrak{q}[[t]]dt$, by definition of the residue, so by P.22(d) in [2], the Pontryagin dual of $A_\mathfrak{q} = \mathbb{F}_\mathfrak{q}[[t]]$ is $K_\mathfrak{q}/A_\mathfrak{q} = \mathbb{F}_\mathfrak{q}((t))/\mathbb{F}_\mathfrak{q}[[t]]$. □

8. Adjoints and Pontryagin duality

The *adjoint map* on $\mathcal{F}$ is the map $f \mapsto f^*$ defined by the following proposition.

Proposition 12. *There is a norm-preserving multiplication-reversing involution*

$$\begin{array}{rcl} \mathcal{F} & \to & \mathcal{F} \\ f = \sum_{n\in\mathbb{Z}} a_n \tau^n & \mapsto & f^* = \sum_{n\in\mathbb{Z}} {a_n}^{1/q^n} \tau^{-n}. \end{array}$$

Proof. The map is well-defined by Proposition 1, and it is immediate from the definition that $\|f^*\| = \|f\|$. One can check $f^{**} = f$ and $(f \circ g)^* = g^* \circ f^*$ directly by comparing coefficients, or perhaps more enlighteningly by noting that

$$f^* = \sum_{n \in \mathbb{Z}} \tau^{-n} a_n$$

is obtained from f by interchanging τ and τ^{-1} and reversing the order of multiplication everywhere, and that this preserves the pair of commutation relations $\tau \circ a = a^q \circ \tau$ and $a \circ \tau^{-1} = \tau^{-1} \circ a^q$. □

We now construct an $\mathbb{F}_q$-linear pairing between $\ker f$ and $\ker f^*$, for nonzero $f \in \mathcal{F}$. Suppose $\alpha \in \ker f$ and $\beta \in \ker f^*$. Then $f \circ \alpha$ vanishes on 1 (recall that $f \circ \alpha$ denotes the composition of f with the map $x \mapsto \alpha x$), so by Lemma 6,

$$f \circ \alpha = g_\alpha \circ (1 - \tau) \tag{7}$$

for some $g_\alpha \in \mathcal{F}$, which is uniquely defined, by Corollary 1. Define

$$\langle \alpha, \beta \rangle_f = g_\alpha^*(\beta).$$

Proposition 13. *If $f \in \mathcal{F}$ is nonzero, then*

$$\langle \ , \ \rangle_f : \ker f \times \ker f^* \to \mathbb{F}_q$$

is an $\mathbb{F}_q$-vector space pairing.

Proof. First let us check that the image lands in $\mathbb{F}_q$. Take adjoints of (7):

$$\alpha \circ f^* = (1 - \tau^{-1}) \circ g_\alpha^*. \tag{8}$$

Apply both sides to β:

$$0 = (1 - \tau^{-1}) g_\alpha^*(\beta).$$

So

$$g_\alpha^*(\beta) \in \ker(1 - \tau^{-1}) = \mathbb{F}_q.$$

From the definition (7), $g_{\alpha+\beta} = g_\alpha + g_\beta$, so the pairing is linear on the left. Linearity on the right is obvious. □

We now prove a series of results leading up to Theorem 10 below.

Lemma 8. *If $f \in \mathcal{F}$, then there exists $q \in \mathcal{F}$ such that*

$$f = (1 - \tau) \circ q + f^*(1).$$

Proof. Apply Lemma 6 to f^* to get h such that

$$f^* = h \circ (1-\tau) + f^*(1).$$

Then taking adjoints yields

$$\begin{aligned} f &= (1-\tau^{-1}) \circ h^* + f^*(1) \\ &= (1-\tau) \circ (-\tau^{-1}) \circ h^* + f^*(1), \end{aligned}$$

so we may take $q = -\tau^{-1} \circ h^*$. $\square$

Lemma 9. *If $f, g \in \mathcal{F}$ and $f \circ (1-\tau) = (1-\tau) \circ g$, then $f^*(1) = g(1)$.*

Proof. Use Lemmas 6 and 8 to write

$$\begin{aligned} f &= (1-\tau) \circ q + f^*(1) \\ g &= h \circ (1-\tau) + g(1). \end{aligned}$$

Substitute these into the given relation:

$$(1-\tau) \circ q \circ (1-\tau) + f^*(1) \circ (1-\tau) = (1-\tau) \circ h \circ (1-\tau) + (1-\tau) \circ g(1). \tag{9}$$

Evaluating the given relation at 1 shows $g(1) \in \ker(1-\tau) = \mathbb{F}_q$, so $g(1)$ commutes with $1-\tau$ and we can cancel $1-\tau$ on the right in (9) to obtain

$$(1-\tau) \circ q + f^*(1) = (1-\tau) \circ h + g(1).$$

Taking adjoints and evaluating at 1 gives the desired result. $\square$

Proposition 14. *If $f \in \mathcal{F}$ is nonzero, $\alpha \in \ker f$, and $\beta \in \ker f^*$, then $\langle \alpha, \beta \rangle_f = -\langle \beta, \alpha \rangle_{f^*}$.*

Proof. Write

$$\begin{aligned} f \circ \alpha &= g_\alpha \circ (1-\tau) \\ f^* \circ \beta &= h_\beta \circ (1-\tau). \end{aligned}$$

Multiply the first by β on the left, and take the adjoint of the second and multiply by α on the right:

$$\begin{aligned} \beta \circ f \circ \alpha &= \beta \circ g_\alpha \circ (1-\tau) \\ \beta \circ f \circ \alpha &= (1-\tau^{-1}) \circ h_\beta^* \circ \alpha \\ &= (1-\tau) \circ (-\tau^{-1}) \circ h_\beta^* \circ \alpha. \end{aligned}$$

Equate and apply Lemma 9 to get

$$\begin{aligned}(\beta \circ g_\alpha)^*(1) &= ((-\tau^{-1}) \circ h_\beta^* \circ \alpha)(1) \\ g_\alpha^*(\beta) &= -\tau^{-1}(h_\beta^*(\alpha)) \\ \langle \alpha, \beta \rangle_f &= -\tau^{-1}(\langle \beta, \alpha \rangle_{f^*}) \\ &= -\langle \beta, \alpha \rangle_{f^*},\end{aligned}$$

since $\langle \beta, \alpha \rangle_{f^*} \in \mathbb{F}_q$. $\square$

Theorem 10. *If $f \in \mathcal{F}$ is nonzero, then the pairing*

$$\langle\ ,\ \rangle_f : \ker f \times \ker f^* \to \mathbb{F}_q$$

exhibits $\ker f$ as the Pontryagin dual of $\ker f^*$ as a topological $\mathbb{F}_q$-vector space.

Proof. First we check that the pairing is continuous. Because of Proposition 14, it will suffice to show that given any bounded subset B of $\ker f^*$, there exists a neighborhood U of 0 in $\ker f$ such that $\langle \alpha, \beta \rangle_f = 0$ for $\alpha \in U$, $\beta \in B$. Given $\alpha \in \ker f$, write

$$f \circ \alpha = g_\alpha \circ (1 - \tau)$$

as in the definition of the pairing. As α tends to zero, each coefficient of $f \circ \alpha$ tends to zero, and so does each coefficient of g_α, by the construction in the proof of Lemma 6. Then the same is true for the coefficients of g_α^*. Combined with the knowledge that g_α^* is everywhere convergent for any α, this implies that $g_\alpha^*(\beta)$ tends to zero uniformly for $\beta \in B$ as α tends to zero, as desired. Thus the pairing is continuous.

The map induced by the pairing is

$$\begin{aligned}\Psi : \ker f &\to \operatorname{Hom}_{\mathbb{F}_q}(\ker f^*, \mathbb{F}_q) \\ \alpha &\mapsto g_\alpha^*|_{\ker f^*}\end{aligned}$$

This is well-defined and continuous, since the pairing is.

We now show Ψ is surjective. If $\phi \in \operatorname{Hom}_{\mathbb{F}_q}(\ker f^*, \mathbb{F}_q)$ is nonzero, then $H = \ker \phi$ is some open and closed subspace in $G = \ker f^*$, so $H \in \mathcal{G}$ by (6) in Proposition 10. Thus by Theorem 4, there exists $h \in \mathcal{F}$ such that $\ker h = H$. Since H has codimension 1 in G (as an $\mathbb{F}_q$-vector space), h must map G to a one-dimensional $\mathbb{F}_q$-vector space inside C. By scaling h, we may assume $h(G) = \mathbb{F}_q$. Now $(1 - \tau) \circ h$ has kernel G, so by the uniqueness in Theorem 4,

$$\tau^n \alpha \circ f^* = (1 - \tau) \circ h$$

for some $\alpha \in C^*$ and $n \in \mathbb{Z}$. Take adjoints and multiply on the right by τ^n:

$$\begin{aligned}f \circ \alpha &= h^* \circ (1 - \tau^{-1}) \circ \tau^n \\ &= h^* \circ (-\tau^{n-1}) \circ (1 - \tau).\end{aligned}$$

Evaluating at 1 shows that $\alpha \in \ker f$. Comparing with (7) shows

$$\begin{aligned} g_\alpha &= h^* \circ (-\tau^{n-1}) \\ g_\alpha^* &= -\tau^{1-n} \circ h \\ g_\alpha^*(G) &= -\tau^{1-n}(h(G)) \\ &= \tau^{1-n}(\mathbb{F}_q) \\ &= \mathbb{F}_q. \end{aligned}$$

Thus ϕ and $\Psi(\alpha) = g_\alpha^*|_{\ker f^*}$ are nonzero $\mathbb{F}_q$-homomorphisms from G to $\mathbb{F}_q$ with the same kernel H, so $\phi = c\Psi(\alpha) = \Psi(c\alpha)$ for some $c \in \mathbb{F}_q{}^*$. Therefore Ψ is surjective.

Applying the above argument to f^* and invoking Proposition 14 shows that the other induced map

$$\ker f^* \to \mathrm{Hom}_{\mathbb{F}_q}(\ker f, \mathbb{F}_q)$$

is surjective as well. Now apply Lemma 7. $\square$

Remarks. If $f = \sum_{i=m}^n a_i \tau^i$ is a finite series with a_i in *any* field L of characteristic p, then the construction yields a perfect pairing between the kernels of f and f^* acting on $\overline{L}$. Here, in addition, the pairing will be $\mathrm{Gal}(L^{\mathrm{sep}}/L)$-equivariant, since its construction is canonical. The same will holds for infinite series, when L has a non-archimedean valuation and L^{sep} is replaced by topological Galois closure.

Next we prove a compatibility result.

Proposition 15. *Let f and h be nonzero elements of $\mathcal{F}$. Then for all $\alpha \in \ker(f \circ h)$ and $\beta \in \ker f^* \subseteq \ker(f \circ h)^*$,*

$$\langle \alpha, \beta \rangle_{f \circ h} = \langle h(\alpha), \beta \rangle_f.$$

Similarly, for all $\alpha \in \ker f \subseteq \ker(h \circ f), \beta \in \ker(h \circ f)^*$,

$$\langle \alpha, \beta \rangle_{h \circ f} = \langle \alpha, h^*(\beta) \rangle_f.$$

Proof. For the first part, write

$$\begin{aligned} (f \circ h) \circ \alpha &= G_\alpha \circ (1 - \tau) \\ f \circ h(\alpha) &= g_{h(\alpha)} \circ (1 - \tau) \end{aligned}$$

Subtract to get

$$f \circ (h \circ \alpha - h(\alpha)) = (G_\alpha - g_{h(\alpha)}) \circ (1 - \tau).$$

Since $h \circ \alpha - h(\alpha)$ kills 1,

$$h \circ \alpha - h(\alpha) = q \circ (1 - \tau)$$

for some $q \in \mathcal{F}$, by Lemma 6. Substitute and cancel $1 - \tau$ on the right:

$$f \circ q = G_\alpha - g_{h(\alpha)}.$$

Take adjoints and apply both sides to $\beta \in \ker f^*$ to get

$$\begin{aligned} 0 &= G_\alpha^*(\beta) - g_{h(\alpha)}^*(\beta) \\ &= \langle \alpha, \beta \rangle_{f \circ h} - \langle h(\alpha), \beta \rangle_f \end{aligned}$$

as desired.

For the second part, we have

$$\begin{aligned} \langle \alpha, \beta \rangle_{h \circ f} &= -\langle \beta, \alpha \rangle_{f^* \circ h^*} \quad \text{(by Proposition 14)} \\ &= -\langle h^*(\beta), \alpha \rangle_{f^*} \quad \text{(by what we just showed)} \\ &= \langle \alpha, h^*(\beta) \rangle_f, \end{aligned}$$

by Proposition 14 again. □

Proposition 16. *Suppose $h, g \in \mathcal{F}$ and $f = h \circ g$. Then*

$$\{\, \beta \in \ker f^* : \langle \alpha, \beta \rangle_f = 0 \ \ \forall \alpha \in \ker g \,\} = \ker h^*.$$

Proof. Suppose $\beta \in \ker f^*$. Then, by Proposition 15,

$$\begin{aligned} \langle \alpha, \beta \rangle_f = 0 \ \ \forall \alpha \in \ker g \quad &\iff \quad \langle \alpha, h^*(\beta) \rangle_g = 0 \ \ \forall \alpha \in \ker g \\ &\iff \quad h^*(\beta) = 0 \quad \text{(by Theorem 10).} \end{aligned}$$

□

Below are three more properties of the pairing. These were discovered by Elkies [6] (for the case of additive polynomials), although some of our proofs are new. We will not need these in the sequel, but they are of interest in their own right. First we explain how the pairing changes if we change the underlying finite field.

Proposition 17. *Let $q' = q^m$, for some $m \geq 1$. If $f \in \mathcal{F}$ is actually $\mathbb{F}_{q'}$-linear, then we can define another pairing $\langle \ , \ \rangle'_f$ between $\ker f$ and $\ker f^*$, this time taking values in $\mathbb{F}_{q'}$. (Note that f^* is the same whether f is considered as $\mathbb{F}_q$-linear or $\mathbb{F}_{q'}$-linear.) Then $\langle \alpha, \beta \rangle_f = \operatorname{Tr}_{\mathbb{F}_{q'}/\mathbb{F}_q} \langle \alpha, \beta \rangle'_f$.*

Proof. Write

$$\begin{aligned} f \circ \alpha &= G_\alpha \circ (1 - \tau^m) \\ &= G_\alpha \circ (1 + \tau + \cdots + \tau^{m-1}) \circ (1 - \tau). \end{aligned}$$

By definition of the pairing,

$$\begin{aligned} \langle \alpha, \beta \rangle_f &= (G_\alpha \circ (1 + \tau + \cdots + \tau^{m-1}))^*(\beta) \\ &= (1 + \tau + \cdots + \tau^{m-1})^*(G_\alpha^*(\beta)) \\ &= (1 + \tau^{-1} + \cdots + \tau^{-(m-1)})(\langle \alpha, \beta \rangle'_f) \\ &= \operatorname{Tr}_{\mathbb{F}_{q'}/\mathbb{F}_q} \langle \alpha, \beta \rangle'_f, \end{aligned}$$

since $\mathrm{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q) = \{1, \tau^{-1}, \ldots, \tau^{-(m-1)}\}$. $\square$

Theorem 11. *Suppose $f \in \mathcal{F}$ is nonzero and $f = f^*$. Then*

(1) *$\langle \alpha, \alpha \rangle_f = 0$ for all $\alpha \in \ker f$.*
(2) *If $h \in \mathcal{F}$ and $f = h^* \circ h$, then $\ker h$ is a maximal isotropic closed sub-$\mathbb{F}_q$-vector space of $\ker f$ under $\langle\ ,\ \rangle_f$.*
(3) *Conversely, if H is a maximal isotropic closed sub-$\mathbb{F}_q$-vector space of $\ker f$ under $\langle\ ,\ \rangle_f$, then there exists $h \in \mathcal{F}$ such that $f = h^* \circ h$ and $\ker h = H$.*

Proof. If $p \neq 2$, then part (1) follows already from Proposition 14. Hence assume $p = 2$. Write $f \circ \alpha = g_\alpha \circ (1 - \tau)$ as usual. Multiply by α on the left, and apply Lemma 8 to write

$$\begin{aligned} \alpha \circ f \circ \alpha &= [(1-\tau) \circ q + (\alpha \circ g_\alpha)^*(1)] \circ (1-\tau) \\ &= (1-\tau^{-1}) \circ j \circ (1-\tau) + g_\alpha^*(\alpha) \circ (1-\tau) \quad \text{(where } j = \tau \circ q\text{)}. \end{aligned}$$

Subtract this from its adjoint and use $f = f^*$ and $g_\alpha^*(\alpha) \in \mathbb{F}_q$ to get

$$0 = (1-\tau^{-1}) \circ (j^* - j) \circ (1-\tau) + g_\alpha^*(\alpha) \circ (\tau - \tau^{-1}).$$

Since $\tau - \tau^{-1} = (1-\tau^{-1}) \circ (1-\tau)$ in characteristic 2, we can cancel $1 - \tau^{-1}$ on the left and $1 - \tau$ on the right to obtain

$$0 = (j^* - j) + g_\alpha^*(\alpha).$$

Take coefficients of τ^0 to deduce

$$\langle \alpha, \alpha \rangle_f = g_\alpha^*(\alpha) = 0.$$

This proves part (1).

Now, for part (2), h is continuous, so $\ker h$ is closed. Proposition 16 says that

$$\{\, \beta \in \ker f^* : \langle \alpha, \beta \rangle_f = 0 \ \ \forall \alpha \in \ker h \,\} = \ker h,$$

which proves part (2).

Finally let us prove (3). Assume H is a maximal isotropic closed sub-$\mathbb{F}_q$-vector space of $\ker f$ under $\langle\ ,\ \rangle$. Then $H \in \mathcal{G}$ by (6) in Proposition 10. By Theorem 4 we can find $g \in \mathcal{F}$ with kernel H, and by Theorem 6, we have $f = j \circ g$ for some $j \in \mathcal{F}$. By Proposition 16,

$$\ker j^* = \{\, \beta \in \ker f^* : \langle \alpha, \beta \rangle_f = 0 \ \ \forall \alpha \in H \,\} = H,$$

since H is maximal isotropic. By the uniqueness in Theorem 4, we have $j^* = \epsilon \circ \tau^n \circ g$ where $\epsilon \in C^*$ and $n \in \mathbb{Z}$. Then

$$f = j \circ g = g^* \circ \tau^{-n} \circ \epsilon \circ g.$$

Taking adjoints and using $f = f^*$ shows that

$$f = g^* \circ \epsilon \circ \tau^n \circ g.$$

If we equate and cancel g^* on the left and g on the right, we obtain

$$\tau^{-n} \circ \epsilon = \epsilon \circ \tau^n,$$

which forces $n = 0$. Now simply take $h = \sqrt{\epsilon} \circ g$ where $\sqrt{\epsilon}$ is any square root of ϵ in C. $\square$

Theorem 12. *If $f \in \mathcal{F}$ and $f^* = -f$, then $\langle \alpha, \beta \rangle_f = \langle \beta, \alpha \rangle_f$ for all $\alpha, \beta \in \ker f$.*

Proof. By definition of the pairing, $\langle\ ,\ \rangle_{-f} = -\langle\ ,\ \rangle_f$, so

$$\begin{aligned} \langle \alpha, \beta \rangle_f &= -\langle \beta, \alpha \rangle_{f^*} \quad \text{(by Proposition 14)} \\ &= -\langle \beta, \alpha \rangle_{-f} \\ &= \langle \beta, \alpha \rangle_f. \end{aligned}$$

$\square$

Remarks. (I thank Noam Elkies for these.) The theory of additive polynomials shares much with the theory of differential operators, as pointed out by Ore [17]. In fact the pairing $\langle\ ,\ \rangle_f$ can be obtained an analogue of a known pairing on kernels of differential operators. If f is a differential operator and f^* denotes its formal adjoint, then we have an identity $uf^*(v) - vf(u) = B'$ where B is a bilinear form in $\{u, u', u'', \ldots, u^{(n-1)}\}$ and $\{v, v', v'', \ldots, v^{(n-1)}\}$. (See p. 124 in [11], where B is called a "bilinear concomitant.") If $u \in \ker f$ and $v \in \ker f^*$, then $B(u, v)$ is a constant depending bilinearly on u and v.

Similarly, if $f \in \mathcal{F}$, then one can write $uf^*(v) - vf(u) = B^q - B$ where B is a (potentially infinite) linear combination of terms of the form $u^{q^m} v^{q^n}$ $(m, n \in \mathbb{Z})$. One can check that B converges to a continuous bilinear function on $C \times C$ by writing B explicitly in terms of the coefficients of f, and using Proposition 1. Clearly $B(\alpha, \beta) \in \mathbb{F}_q$ if $\alpha \in \ker f$ and $\beta \in \ker f^*$.

Proposition 18. *If $\alpha \in \ker f$ and $\beta \in \ker f^*$, then $B(\alpha, \beta) = \langle \alpha, \beta \rangle_f$.*

Proof. Let $b_\alpha(v) = B(\alpha, v)$. If we set $u = \alpha$ in the defining equation for B, we have as functions of v,

$$\begin{aligned} \alpha \circ f^* &= (\tau - 1) \circ b_\alpha, \\ f \circ \alpha &= b_\alpha^* \circ (\tau^{-1} - 1) \\ &= b_\alpha^* \circ \tau^{-1} \circ (1 - \tau). \end{aligned}$$

Comparing with equation (7) shows that $g_\alpha = b_\alpha^* \circ \tau^{-1}$, so

$$\begin{aligned} \langle \alpha, \beta \rangle_f &= g_\alpha^*(\beta) \\ &= (\tau \circ b_\alpha)(\beta) \\ &= \tau(B(\alpha, \beta)) \\ &= B(\alpha, \beta), \end{aligned}$$

since $B(\alpha,\beta) \in \mathbb{F}_q$. $\square$

This alternative definition of the pairing could clearly be used to give new proofs of the properties of the pairing. For instance, Proposition 14 would be immediate, as would the first part of Theorem 11.

9. A-module pairings for Drinfeld modules

Let us retain the assumption that A is the affine ring of a nonsingular projective curve over $\mathbb{F}_q$ minus a closed point ∞, and suppose we have an $\mathbb{F}_q$-algebra homomorphism $\iota : A \to C$. The kernel $\mathfrak{p}$ of ι will be called the characteristic.

Let $a \mapsto \phi_a$ and $a \mapsto \psi_a$ be ring homomorphisms from A to $\mathcal{F}$. For example, ϕ and ψ might be Drinfeld A-modules over C. We say that a nonzero $f \in \mathcal{F}$ is an *isogeny* from ϕ to ψ if $\psi_a \circ f = f \circ \phi_a$ for all $a \in A$. If $f : \phi \to \psi$ is an isogeny, then $\ker f$ is an A-module via ϕ and $\ker f^*$ is an A-module via ψ^*.

Proposition 19. *Let $a \mapsto \phi_a$ and $a \mapsto \psi_a$ be ring homomorphisms from A to $\mathcal{F}$. Suppose $f \in \mathcal{F}$ is an isogeny from ϕ to ψ. Then for all $a \in A$, $\alpha \in \ker f$, $\beta \in \ker f^*$, we have*

$$\langle \phi_a(\alpha), \beta\rangle_f = \langle \alpha, \psi_a^*(\beta)\rangle_f,$$

and

$$\begin{array}{rcl} [\ ,\ ]_f : \ker f \times \ker f^* & \to & \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q) \\ \alpha\ ,\ \beta & \mapsto & (a \mapsto \langle \phi_a(\alpha), \beta\rangle) \end{array}$$

is a pairing of A-modules which exhibits $\ker f^*$ as the Pontryagin dual of $\ker f$ as an A-module.

Furthermore, if $\Psi : A \to \mathcal{F}$ is a third ring homomorphism, and $h : \Psi \to \phi$ is another isogeny, then we have the following two compatibility relations: if $\alpha \in \ker(f \circ h), \beta \in \ker f^* \subseteq \ker(f \circ h)^*$, then

$$[\alpha, \beta]_{f\circ h} = [h(\alpha), \beta]_f.$$

Similarly, for all $\alpha \in \ker h \subseteq \ker(f \circ h), \beta \in \ker(f \circ h)^*$,

$$[\alpha, \beta]_{f\circ h} = [\alpha, f^*(\beta)]_h.$$

Proof. Given $a \in A$, $\alpha \in \ker f$, $\beta \in \ker f^*$, we have

$$\begin{array}{rcll} \langle \phi_a(\alpha), \beta\rangle_f & = & \langle \alpha, \beta\rangle_{f\circ\phi_a} & \text{(by Proposition 15)} \\ & = & \langle \alpha, \beta\rangle_{\psi_a\circ f} & \\ & = & \langle \alpha, \psi_a^*(\beta)\rangle_f & \text{(by Proposition 15 again).} \end{array}$$

Apply Lemma 7 to get the duality property of $[\ ,\ ]_f$. The compatibility relations follow from those for $\langle\ ,\ \rangle$ proved in Proposition 15. $\square$

Corollary 11. *Let ϕ be a Drinfeld A-module over a field L. Fix a nonzero $a \in A$. Let $\phi[a]$ be the kernel of ϕ_a on $\overline{L}$, and similarly define $\phi^*[a] = \ker \phi_a^*$. There is a Galois-equivariant perfect pairing of finite A-modules*

$$[\ ,\ ]_a : \phi[a] \times \phi^*[a] \to \widehat{(A/a)} \subset \hat{A}.$$

(Here $\operatorname{Gal}(L^{sep}/L)$ acts trivially on $\hat{A}$ and $\widehat{(A/a)}$.) If we also have a nonzero $b \in A$, then for any $\alpha \in \phi[ab]$, $\beta \in \psi^*[a]$

$$[\alpha, \beta]_{ab} = [\phi_b(\alpha), \beta]_a.$$

Similarly, for $\alpha \in \phi[a]$, $\beta \in \psi^*[ab]$,

$$[\alpha, \beta]_{ab} = [\alpha, \psi_b^*(\beta)]_a.$$

The properties above of $[\ ,\ ]_a$ should remind one of the Weil pairing for abelian varieties. Another proof of the Galois-equivariant duality between $\phi[a]$ and $\phi^*[a]$ was discovered independently by Taguchi. (See the appendix of [10].)

As another application of our pairings, we can describe the kernel of the adjoint of the exponential function associated with a Drinfeld module.

Corollary 12. *Let C be the completion of the algebraic closure of K_∞ with $|\ |_\infty$, and let ϕ be a Drinfeld A-module over C. Let $e(z) \in C[[z]]$ be the associated exponential function. Then there is a natural pairing*

$$\ker e \times \ker e^* \to \hat{A}$$

which exhibits $\ker e^*$ as the Pontryagin dual of $\ker e$ as an A-module. If the lattice $\ker e$ is isomorphic to the direct sum of fractional ideals $I_1 \oplus \cdots \oplus I_r$, then $\ker e^*$ is isomorphic to $K_\infty/(I_1^{-1}J) \oplus \cdots \oplus K_\infty/(I_r^{-1}J)$ as a topological A-module. (Here J is as in Theorem 8.)

Proof. Simply note that e is an isogeny from C with the standard A-module structure to ϕ, and apply Proposition 19. The last assertion follows from Theorem 8. $\square$

Proposition 20. *Let ϕ and e be as in the previous corollary. Then $\ker e^*$ is the closure of $\bigcup_{a \in A} \phi^*[a]$.*

Proof. Taking adjoints of

$$e \circ a = \phi_a \circ e$$

yields

$$a \circ e^* = e^* \circ \phi_a^*,$$

from which it is clear that $\phi^*[a] \subset \ker e^*$.

Corollary 12 says that $\ker e^*$ as a topological A-module via ϕ^* is isomorphic to $K_\infty/C_1 \oplus \cdots \oplus K_\infty/C_r$, for some fractional A-ideals $C_1, \ldots, C_r$. The torsion submodule in this module is $K/C_1 \oplus \cdots \oplus K/C_r$, which is dense, so the result follows. $\square$

10. Tate module pairings

Because of the compatibility relations, we can use our pairings to construct a pairing between Tate modules, just as the Weil pairing gives rise to a pairing between Tate modules. Let $\mathfrak{q}$ be a nonzero prime of A different from the characteristic $\mathfrak{p}$ of the Drinfeld module. Let K be the fraction field of A, and let $A_\mathfrak{q}$, $K_\mathfrak{q}$ be the completions at the prime $\mathfrak{q}$. The Tate module of a Drinfeld A-module over L is

$$T_\mathfrak{q}(\phi) = \mathrm{Hom}_A(K_\mathfrak{q}/A_\mathfrak{q}, \phi(\overline{L}))$$

where $\phi(\overline{L})$ denotes the additive group of $\overline{L}$ with the A-module structure given by ϕ. Similarly we define the Tate module of ϕ^* as

$$T_\mathfrak{q}(\phi^*) = \mathrm{Hom}_A(K_\mathfrak{q}/A_\mathfrak{q}, \phi^*(\overline{L})).$$

These are both free $A_\mathfrak{q}$-modules of rank equal to the rank of the Drinfeld module.

Proposition 21. *There is a Galois-equivariant continuous perfect pairing of $A_\mathfrak{q}$-modules*

$$[\ ,\ ]_\mathfrak{q} : T_\mathfrak{q}(\phi) \times T_\mathfrak{q}(\phi^*) \to \mathrm{Hom}_{\mathbb{F}_q}(K_\mathfrak{q}/A_\mathfrak{q}, \mathbb{F}_q) \cong A_\mathfrak{q}$$

.

Proof. Given $\alpha \in T_\mathfrak{q}(\phi)$, $\beta \in T_\mathfrak{q}(\phi^*)$, define $[\alpha, \beta]_\mathfrak{q} \in \mathrm{Hom}_{\mathbb{F}_q}(K_\mathfrak{q}/A_\mathfrak{q}, \mathbb{F}_q)$ by

$$[\alpha, \beta]_\mathfrak{q}(b) = [\alpha(b), \beta(a^{-1})]_a$$

where $a \in A$ kills b and generates an ideal power of $\mathfrak{q}$. As is well known, A is a Dedekind domain with finite class number, so some power $\mathfrak{q}^h$ of $\mathfrak{q}$ is principal, so it is always possible to find such an a, given b. The definition is independent of the choice of a, by the last compatibility relation in Corollary 11.

If we fix $a \in A$ generating a power of $\mathfrak{q}$, we can also obtain the pairing as the inverse limit of the pairings

$$[\ ,\ ]_{a^n} : \phi[a^n] \times \phi^*[a^n] \longrightarrow \mathrm{Hom}_{\mathbb{F}_q}(A/a^n, \mathbb{F}_q) = \mathrm{Hom}_{\mathbb{F}_q}(a^{-n}A/A, \mathbb{F}_q),$$

with respect to the maps

$$\begin{array}{rcl} \phi[a^{n+1}] & \xrightarrow{a} & \phi[a^n] \\ \phi^*[a^{n+1}] & \xrightarrow{a} & \phi^*[a^n] \\ \mathrm{Hom}_{\mathbb{F}_q}(a^{-(n+1)}A/A, \mathbb{F}_q) & \xrightarrow{\mathrm{res}} & \mathrm{Hom}_{\mathbb{F}_q}(a^{-n}A/A, \mathbb{F}_q). \end{array}$$

The Galois-equivariance, continuity, and perfectness of the pairing then follow from the properties of the pairings $[\ ,\ ]_{a^n}$.

Finally, $\mathrm{Hom}_{\mathbb{F}_q}(K_\mathfrak{q}/A_\mathfrak{q}, \mathbb{F}_q)$ is (non-canonically) isomorphic to $A_\mathfrak{q}$ as an $A_\mathfrak{q}$-module, by Theorem 9. $\square$

As pointed out by Goss, this duality of Tate modules has the following corollary.

Corollary 13. *Suppose the Drinfeld module ϕ is defined over a finite extension L of K. Then*

$$T_{\mathfrak{q}}(\phi^*) \otimes_{A_{\mathfrak{q}}} K_{\mathfrak{q}}$$

is a semi-simple $K_{\mathfrak{q}}[\mathrm{Gal}(L^{sep}/L)]$-module.

Proof. Combine the previous theorem with the main theorem in [18]. □

11. Questions

Our results show that in two cohomological realizations (the period lattice and Tate module), the cohomology of the adjoint of a Drinfeld module is dual to the cohomology of the original Drinfeld module. There is a third cohomological realization of a Drinfeld module, namely the de Rham cohomology [8] developed by Anderson, Deligne, Gekeler, and Yu.

Question 1. Is it possible to give a reasonable definition for the de Rham cohomology of the adjoint of a Drinfeld module and prove that it is dual in some sense to the de Rham cohomology of the original Drinfeld module?

It would also be nice to generalize the applications of this paper to include t-modules, the higher dimensional analogues of Drinfeld modules.

Question 2. Can one prove results similar to those in this paper for fractional power series in more than one variable?

A reasonable approach is to work with the ring $\mathbb{M}_d(\mathcal{F})$ of d-by-d matrices with coefficients in $\mathcal{F}$. Elements of this ring act on C^d in an obvious way. Moreover, there is a multiplication-reversing adjoint map $\mathbb{M}_d(\mathcal{F}) \to \mathbb{M}_d(\mathcal{F})$, which maps a matrix $A = (a_{ij})$ to $A^* = (a_{ji}^*)$, i.e., the transpose of the matrix obtained by taking the adjoint of each entry. Hence, for example, it is possible to define the adjoint of a t-module

$$\begin{aligned} \phi : \mathbb{F}_q[t] &\to \mathbb{M}_d(C\{\tau\}) \subset \mathbb{M}_d(\mathcal{F}) \\ a &\mapsto \phi_a \end{aligned}$$

as

$$\begin{aligned} \phi^* : \mathbb{F}_q[t] &\to \mathbb{M}_d(\mathcal{F}) \\ a &\mapsto \phi_a^*. \end{aligned}$$

For each $A = (a_{ij}) \in \mathbb{M}_d(\mathcal{F})$ it is also possible to define a natural bilinear pairing

$$\langle\ ,\ \rangle_A : \ker A \times \ker A^* \to \mathbb{F}_q$$

by following the differential operator analogy. Let $\cdot$ denote the standard inner product on C^d. As in the remarks at the end of Section 8, for each $f \in \mathcal{F}$, let $B_f(u,v)$ be the bilinear function of $u, v \in C$ such that

$$uf^*(v) - vf(u) = B_f^q - B_f.$$

Then, for $u, v \in C^d$, the bilinear function

$$B_A(u,v) = \sum_{i,j} B_{a_{ij}}(u_i, v_j)$$

satisfies

$$u \cdot A^*(v) - v \cdot A(u) = B_A^q - B_A,$$

and we may define

$$\langle u, v\rangle_A = B_A(u,v).$$

Thus for instance, one has a pairing between the a-torsion of a t-module and the a-torsion of its adjoint.

Acknowledgements

Many thanks go to David Goss, who introduced me to adjoints of polynomials and Drinfeld modules, and asked some of the questions answered by this paper. I thank T. Y. Lam, Hendrik Lenstra, and Ken Ribet for helping me find references for Newton polygons. Thanks also to Noam Elkies for sharing his preprint with me, and to Michael Rosen for suggesting references of use in proving Theorem 8. Finally, I thank the referee for many intelligent and helpful suggestions.

References

1. Y. Amice: *Les nombres p-adiques*, Presses Universitaires de France, 1975.
2. D. Armacost: *The Structure of Locally Compact Abelian Groups*, Marcel Dekker, 1981.
3. E. Artin: *Algebraic Numbers and Algebraic Functions I*, Lecture Notes Princeton Univ./New York Univ., 1950/51.
4. P. Deligne and D. Husemöller: Survey of Drinfeld Modules, *Contemp. Math.* **67** (1987), 25–91.
5. M. Eichler: *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, 1966.
6. N. Elkies: Linearized algebra and finite groups of Lie type, preprint, 1994.
7. J. Flood: Pontryagin Duality for Topological Modules, *Proc. Amer. Math. Soc.* **75** (1979), 329–333.
8. E.-U. Gekeler: De Rham Cohomology for Drinfeld Modules, *Séminaire de Théorie des Nombres, Paris 1988–89*, 57–85.
9. I. Glicksberg: Uniform boundedness for groups, *Can. J. Math.* **14** (1962), 269–277.
10. D. Goss: The adjoint of the Carlitz module and Fermat's Last Theorem, preprint, 1994.
11. E. Ince: *Ordinary Differential Equations*, Dover, 1956.
12. R. V. Kadison and J. R. Ringrose: *Fundamentals of the theory of operator algebras*, Vol. 1, Academic Press, 1983.

13. Kneser, M.: *Algebraische Zahlentheorie*, Vorlesungsausarbeitung Georg-August-Universität Göttingen, 1966.
14. N. Koblitz: *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, 1984.
15. H. Matsumura: *Commutative Algebra*, Second Edition, Benjamin/Cummings Publishing Co., 1980.
16. J. Neukirch: *Algebraische Zahlentheorie*, Springer-Verlag, 1992.
17. Ø. Ore: On a Special Class of Polynomials, *Trans. Amer. Math. Soc.* **35** (1933), 559–584.
18. Y. Taguchi: Semi-simplicity of the Galois Representations Attached to Drinfeld Modules over Fields of "Infinite Characterstics," *J. of Number Th.* **44** (1993), 292–314.
19. A. Weil: *Basic Number Theory*, Springer-Verlag, 1974.

Mathematical Sciences Research Institute, Berkeley, CA 94720-5070, USA
E-mail address: poonen@msri.org