DRINFELD MODULES AND ARITHMETIC IN THE FUNCTION FIELDS

DINESH S. THAKUR

0. Background.

Notation:
q: a power of a prime p;
K: a function field of one variable over its field of constants $\mathbf{F}_q$;
∞: a place of K;
A: the ring of elements of K integral outside ∞;
K_∞: the completion of K at ∞;
Ω: the completion of an algebraic closure of K_∞;
δ: the degree of the place ∞;
h: the class number of K;
g: the genus of K.

Various partial analogies observed between the theory of number fields and the theory of function fields have stimulated the development of both number theory and geometry. At the simplest level, we have the well-known analogies $K \leftrightarrow \mathbf{Q}$, $A \leftrightarrow \mathbf{Z}$, $K_\infty \leftrightarrow \mathbf{R}$, $\Omega \leftrightarrow \mathbf{C}$, and $\infty \leftrightarrow$ the unique archimedean place of $\mathbf{Q}$. We may extend these analogies also to the imaginary quadratic fields and their rings of integers in place of K and A, since they have a unique archimedean place too. (In this case, $\mathbf{C}$ will be an analogue for both K_∞ and Ω.) The imaginary quadratic fields and $\mathbf{Q}$ are precisely the number fields for which there is a well-developed explicit class-field theory (i.e., theory of abelian extensions) using the torsion of the action of integers on the corresponding complex multiplication elliptic curves or the multiplicative group $\mathbf{G}_m$ respectively. Analogous theory was developed by Drinfeld (see [D] and also [C1, H1, H2]), by considering the additive group $\mathbf{G}_a$ (instead of $\mathbf{G}_m$ and various elliptic curves) which admits various possible actions of any A. This led to the concept of Drinfeld module introduced below.

From now on, we assume $\delta = 1$, though a few concepts and results below have straightforward generalizations even when $\delta > 1$. A choice of uniformizer u at ∞ allows us to express $z \in K_\infty^\times$ uniquely as $z = sgn(z) \times \bar{z} \times u^{\deg z}$, where $sgn(z) \in \mathbf{F}_q^\times$, $\bar{z}$ is a one unit at ∞ and $\deg z$ is an integer. We make a choice of such a *sgn* function and call monic the elements of $sgn = 1$. Let A_+ be the set of monic elements of A and let $\mathbf{Z}_+$ be the set of positive integers of $\mathbf{Z}$. Let H be the maximal abelian unramified extension of K split completely at ∞ and let B be the integral closure of A in H. (H is an analogue of Hilbert class field; see [H2, R].)

Received 20 August 1992.
Communicated by Barry Mazur.

Let $B\{F\}$ denote the noncommutative ring generated by elements of B and by a symbol F, satisfying the commutation relation $Fb = b^q F$ for all $b \in B$. (Elements of this ring can be considered as endomorphisms of the additive group, F being identified with the Frobenius.)

Definition. By a Drinfeld A-module ρ (in fact, "*sgn*-normalized of rank one and of generic characteristic over B", but we will drop these words), we will mean an injective homomorphism $\rho: A \to B\{F\}$ (we write image of a by ρ_a) such that, for nonzero $a \in A$,

(1) the degree of ρ_a as a polynomial in F is $\deg a$,
(2) the coefficient of F^0 in ρ_a is a, and
(3) the top-degree coefficient in ρ_a is $sgn(a)$.

Example. Let $A = \mathbf{F}_q[T]$ and choose sgn so that $sgn(T) = 1$. Then T being a generator of A, $\rho_T := T + F$ defines a ρ. One has, e.g., $\rho_{T^2} = T^2 + (T + T^q)F + F^2$. ■

There are h such Drinfeld A-modules and can be obtained from one another by $\mathrm{Gal}(H/K)$ conjugation. We assume that such a ρ is given and drop it from notation when convenient.

The analogy with the classical case is

$$a \in A \mapsto \rho_a \in End\, \mathbf{G}_a \leftrightarrow n \in \mathbf{Z} \mapsto (x \mapsto x^n) \in End\, \mathbf{G}_m .$$

A classical exponential function is just a normalized entire function satisfying $e^{nz} = (e^z)^n$. Similarly, associated to ρ, we have the (Drinfeld) exponential $e(z)$ defined to be the entire function (i.e., the function from Ω to Ω given by an everywhere convergent power series) with the linear term z and satisfying

$$e(az) = \rho_a(e(z)), \qquad a \in A. \tag{1}$$

Various analogies with the usual exponential are described in [T2, T3]. We define (see 3.2 of [T4]) d_i by the expression

$$e(z) = \sum_{i=0}^{\infty} z^{q^i}/d_i . \tag{2}$$

The kernel Λ of the exponential $e(z)$ is an A-lattice (i.e., a discrete A module in Ω) of rank one. We can write $\Lambda = \tilde{\pi}_I I$ for $\tilde{\pi}_I \in \Omega$ and some ideal I of A. For simplicity (see the remarks at the end of the paper), we assume that ρ corresponds to the principal ideal class (i.e., the equality above holds for some principal ideal); we put $\tilde{\pi} = \tilde{\pi}_A$. Note that $\tilde{\pi}$ is then determined up to multiplication by a nonzero element of $\mathbf{F}_q$. It can be considered as an analogue of $2\pi i$.

It is easy to see that

$$e(z) = z \prod_{\lambda \in \Lambda - \{0\}} (1 - z/\lambda). \tag{3}$$

Let *log* be the (multivalued) inverse function of e and let (see 5.8 of [T4])

$$l(z) = \sum_{i=0}^{\infty} z^{q^i}/l_i \tag{4}$$

be the power series, representing the branch of *log* vanishing at zero, convergent in some neighborhood of zero. We have

$$a\, log(z) = log(\rho_a(z)). \tag{5}$$

We also define $\left\{ {t \atop q^i} \right\}$ by

$$e(tl(z)) = \sum_{i=0}^{\infty} \left\{ {t \atop q^i} \right\} z^{q^i}. \tag{6}$$

Then we have

$$\left\{ {t \atop q^i} \right\} = \sum_{k=0}^{i} t^{q^k}/d_k l_{i-k}^{q^k}. \tag{7}$$

Let $A_{i+} := \{a \in A_+ : \deg a = i\}$ and define

$$\frac{1}{L_i} := S_i := \sum_{a \in A_{i+}} \frac{1}{a}, \tag{8}$$

$$e_i(t) := \psi_i(t) := \prod_{\substack{a \in A \\ \deg a < i}} (t - a) \in A[t], \tag{9}$$

$$D_i := \prod_{a \in A_{i+}} a, \tag{10}$$

$$\binom{t}{q^i} := \frac{e_i(t)}{D_i}. \tag{11}$$

THEOREM I (see [C1]). *For $A = \mathbf{F}_q[T]$ and ρ as in our example,*

$$\left\{ {t \atop q^i} \right\} = \binom{t}{q^i}, \qquad D_i = d_i, \qquad L_i = l_i.$$

Note that there are many notation and normalization differences in the literature. The first two quantities in the theorem are analogues of binomial coefficients and factorials respectively. (See [C1, C3, T1].) In general, the equalities do not hold, but D_i are good analogues of factorials. (see [T3]).

As an analogue of Riemann zeta values

$$\zeta_{Riemann}(n) = \sum_{z \in \mathbf{Z}_+} 1/z^n \in \mathbf{R}, \qquad n = 2, 3, \ldots,$$

define

$$\zeta(n) := \sum_{a \in A_+} 1/a^n \in K_\infty, \qquad n = 1, 2, 3, \ldots .$$

Now $A^\times = \mathbf{F}_q^\times \leftrightarrow \mathbf{Z}^\times = \{\pm 1\}$. The cardinalities of $A^\times$ and $\mathbf{Z}^\times$ (i.e., choices of signs) are $q-1$ and 2 respectively. Hence we call the multiples of $q-1$ "even".

THEOREM II (See [C1, G]). *For n even, $\zeta(n)/\tilde{\pi}^n \in H$.*

Proof. Multiplying the logarithmic derivative of both the sides of (3) by z, we get

$$\frac{z}{e(z)} = 1 - \sum_{\lambda \in \Lambda - \{0\}} \frac{z/\lambda}{1 - z/\lambda} = 1 - \sum_{n=1}^{\infty} \sum_{\lambda} \left(\frac{z}{\lambda}\right)^n = 1 + \sum_{n \text{ even}} \frac{\zeta(n)}{\tilde{\pi}^n} z^n$$

since $\sum_{c \in \mathbf{F}_q^\times} c^n = -1$ or 0 according to whether n is even or not. By (1) and (2), $d_i \in H$. This completes the proof.

In particular, by comparing the coefficients of z^{q-1} in the equation above, we get

$$\zeta(q-1)/\tilde{\pi}^{q-1} = -1/d_1 . \tag{12}$$

For more on analogies with Riemann zeta values and interpolations, see [C1, G, T1]. Note that $\zeta(1)$ also makes sense. It is an analogue of Euler's gamma constant (see [T3]).

I. Interrelations. Note that d_i, $l_i \in H$, $\{{t \atop q^i}\} \in H[t]$ and D_i, $L_i \in K$, $({t \atop q^i}) \in K[t]$. (In fact, $D_i \in A$.) We want to generalize Theorem I by relating d_i's to D_i's, l_i's to L_i's, and { }'s to ( )'s. Further motivation will be provided in Sections II and III. See also [C1, AT].

If A has a monic element, say p_i, of degree i (e.g. if $i > g-1$), then $e_{i+1}(t) = \prod_{c \in \mathbf{F}_q} e_i(t + cp_i) = e_i(t)^q - D_i^{q-1} e_i(t)$ since $e_i(p_i) = D_i$. So

$$e_{i+1}(t) = e_i(t)^q - D_i^{q-1} e_i(t) \tag{13}$$

if p_i exists. If p_i does not exist, $e_{i+1}(t) = e_i(t)$. Let

$$\begin{Bmatrix} t \\ q^i \end{Bmatrix} = \sum_{k=0}^{i} a_{ik} t^{q^k}, \qquad \begin{pmatrix} t \\ q^i \end{pmatrix} = \sum A_{ik} t^{q^k}. \tag{14}$$

By the Riemann-Roch theorem, if $i \geqslant 2g$ then $A_{ik} = 0$ if $k > i - g$, since there are g Weierstrass gaps. For the same reason, as a straightforward counting of signs shows, we have for $i \geqslant 2g$,

$$A_{i0} = (-1)^{i-g} \frac{(D_0 D_1 \cdots D_{i-1})^{q-1}}{D_i}. \tag{15}$$

On the other hand, (7) implies that, for any i,

$$a_{i0} = 1/l_i, \qquad a_{ii} = 1/d_i, \qquad A_{i(i-g)} = 1/D_i. \tag{16}$$

Let

$$L_i(n)^{-1} := S_i(n) := \sum_{a \in A_{i+}} \frac{1}{a^n}. \tag{17}$$

Then for i for which p_i exists (e.g., $i > g-1$),

$$1 - \binom{t}{q^i} = -\binom{t-p_i}{q^i} = -\prod_{a \in A_{i+}} \left(\frac{t}{a} - 1\right).$$

Taking the negative of the logarithmic derivative of both the sides, we get

$$\frac{A_{i0}}{1 - \sum_{k=0}^{i} A_{ik} t^{q^k}} = -\sum_{a \in A_{i+}} \frac{1}{t-a} = \sum_{n=0}^{\infty} S_i(n+1) t^n. \tag{18}$$

Remark. Hence $S_i(n)$ is a homogeneous polynomial in A_{ik}'s, with coefficients in $\mathbf{F}_p$, of weight n, if A_{ik} is given weight q^k. In particular,

$$S_i(1) = S_i = \frac{1}{L_i} = A_{i0}. \tag{19}$$

This quantity plays a crucial role in the arithmetic of gamma functions, periods, and zeta functions. See [T3].

THEOREM III. *For $i \geqslant 2g$,*

$$\begin{Bmatrix} t \\ q^i \end{Bmatrix} = \sum_{k=0}^{g} c_{ik} \binom{t}{q^i}^{q^k}, \qquad c_{ik} \in H,$$

$$\sum_{k=0}^{g} c_{ik} = 1, \qquad c_{i0} = \frac{L_i}{l_i}, \qquad c_{ig} = \frac{D_i^{q^g}}{d_i}.$$

Proof. If $t \in A$, then by (1),

$$e(tl(z)) = \rho_t(e(l(z)) = \rho_t(z).$$

Further, if $\deg t < i$, then the degree of the polynomial $\rho_t(z)$ is less than q^i so that, by (6), $\left\{ {t \atop q^i} \right\} = 0$. Hence the $\mathbf{F}_q$-linear polynomial $\left\{ {t \atop q^i} \right\}$ of degree q^i in t has elements of A of degree less than i as its zeros. Now $\binom{t}{q^i}$ has precisely these zeros. By the Riemann-Roch theorem, this accounts for q^{i-g} zeros of $\{\ \}$. Since the zeros of a $\mathbf{F}_q$-linear polynomial form a vector space over $\mathbf{F}_q$, choosing a basis and using the fact that the top-degree coefficient of $\left\{ {t \atop q^i} \right\}$ is $1/d_i$, we see that

$$d_i \left\{ {t \atop q^i} \right\} = \prod_{c_1, \ldots, c_g \in \mathbf{F}_q} e_i(t + c_1 t_{i1} + \cdots + c_g t_{ig}) = \sum_{k=0}^{g} r_{ik} e_i(t)^{q^k}$$

for suitable t_{ij}, r_{ij}'s. This implies the first statement of the theorem. By the conditions (1) and (3) in the definition of ρ, it follows that $\left\{ {p_i \atop q^i} \right\} = 1$. Hence the second statement of the theorem follows by putting $t = p_i$ in the first statement. The rest follows by comparison of the lowest- (resp. top-)degree coefficients in the first statement using (14), (16), and (19). This completes the proof.

Hence one of our goals is to understand c_{ik}'s.

Remark. Theorem III clearly implies Theorem I.

Let

$$f_i := d_i/d_{i-1}^q, \qquad g_i := l_i/l_{i-1}. \tag{20}$$

THEOREM IV. *When $g = 1$, $i \geqslant 2g$, we have*

$$\left\{ {t \atop q^i} \right\} = (1 - \mu_i)\binom{t}{q^i}^q + \mu_i \binom{t}{q^i}, \tag{21}$$

$$D_i^q = (1 - \mu_i)\, d_i, \qquad S_i = \frac{1}{L_i} = \frac{1}{\mu_i l_i}, \tag{22}$$

with

$$\mu_i = \frac{(f_{i+1} - f_i + l_1^{q^i}) g_{i+1}}{(f_{i+1} - f_i) g_{i+1} - f_{i+1} l_1^{q^i}}. \tag{23}$$

Proof. By (15) and (19) we have

$$\frac{D_{i+1}}{L_{i+1}} = -\frac{D_i^q}{L_i}. \tag{24}$$

Let b_i be the coefficient of t^{q^i-2} in $e_i(t)$. Comparing the coefficients of t^{q^i-1} in (13), we get

$$b_{i+1} = b_i^q - D_i^{q-1}. \tag{25}$$

Let $\mu_i = L_i/l_i$; then by Theorem III, we get (21) and (22). We want to show (23). Now comparing the coefficients of $t^{q^{i-1}}$ in (21), using (7), (11), and (22), we get

$$\frac{d_i}{d_{i-1}l_1^{q^{i-1}}} = b_i^q + \frac{d_i L_i}{D_i l_i}. \tag{26}$$

Subtracting qth power of this equation from the same equation, but with i replaced by $i+1$, and using (25), we get

$$\frac{1}{l_1^{q^i}}\left(\frac{d_{i+1}}{d_i} - \frac{d_i^q}{d_{i-1}^q}\right) = -D_i^{q(q-1)} + \left(\frac{d_{i+1}L_{i+1}}{l_{i+1}D_{i+1}} - \frac{d_i^q L_i^q}{l_i^q D_i^q}\right)$$

which equals, by (24),

$$-D_i^{q(q-1)} - \frac{1}{D_i^q}\left(\frac{d_{i+1}L_i}{l_{i+1}} + \frac{d_i^q L_i^q}{l_i^q}\right).$$

By (20), (21), and (22), the above equation reduces, after cancelling the common factor d_i^{q-1}, to

$$\left(\frac{f_{i+1}}{f_i} - 1\right)\frac{f_i}{l_1^{q^i}} = -(1-\mu_i)^{q-1} - \frac{1}{1-\mu_i}\left(\frac{f_{i+1}\mu_i}{g_{i+1}} + \mu_i^q\right).$$

Simple algebraic manipulation now leads to (23). This completes the proof.

Finally, we give an explicit formula for f_i and g_i when $g = 1$. By the Riemann-Roch theorem, we can find monic $x, y \in A$ of degrees 2 and 3 respectively. Put $[i]_x := x^{q^i} - x$ and $[i]_y := y^{q^i} - y$. Let $\rho_x = x + x_1 F + F^2$ and $\rho_y = y + y_1 F + y_2 F^2 + F^3$. (In fact, ρ_x determines ρ.)

THEOREM V. *When $g = 1$, we have*

$$f_i = \frac{[i]_y - (y_2 - x_1^q)[i]_x}{[i-1]_x^q + y_1 - (y_2 - x_1^q)x_1}, \tag{27}$$

$$g_i = \frac{-[i]_y + (y_2 - x_1)^{q^{i-2}}[i]_x}{y_1^{q^{i-1}} - [i-1]_x - (y_2 - x_1)^{q^{i-2}} x_1^{q^{i-1}}}. \tag{28}$$

Proof. Comparing the coefficients of z^{q^i} in (1) with $a = x$ and with $a = y$, we get

$$0 = -\frac{[i]_x}{d_i} + \frac{x_1}{d_{i-1}^q} + \frac{1}{d_{i-2}^{q^2}}, \qquad 0 = -\frac{[i]_y}{d_i} + \frac{y_1}{d_{i-1}^q} + \frac{y_2}{d_{i-2}^{q^2}} + \frac{1}{d_{i-3}^{q^3}}.$$

Denote the right-hand sides of these equations by $x[i]$ and $y[i]$ respectively. Then the equation $y[i] - x[i-1]^q - (y_2 - x_1^q)x[i] = 0$ simplifies to (27).

A similar method, using (5) instead of (1), gives (28). This completes the proof.

II. Examples. We now apply the results of the last section to special zeta values. It was shown in [LMQ] that, apart from the rational function fields (one for each q), there are only seven other function fields of class number one. A simple check of the list given there shows that there are only three possibilities for A with $\delta = h = g = 1$. These possibilities, with the corresponding (unique) ρ's, are listed in [H2] as examples 11.3–11.5. We list them now.

Example A. $A = \mathbf{F}_3[x, y]/y^2 = x^3 - x - 1$.

$$x_1 = y(x^3 - x), \qquad y_1 = y(y^3 - y), \qquad y_2 = y^9 + y^3 + y.$$

Example B. $A = \mathbf{F}_4[x, y]/y^2 + y = x^3 + \theta$, where $\theta \in \mathbf{F}_4$ is a root of $\theta^2 + \theta + 1 = 0$.

$$x_1 = x^8 + x^2, \qquad y_1 = x^{10} + x, \qquad y_2 = x^{32} + x^8 + x^2.$$

Example C. $A = \mathbf{F}_2[x, y]/y^2 + y = x^3 + x + 1$.

$$x_1 = x^2 + x, \qquad y_1 = y^2 + y, \qquad y_2 = x(y^2 + y).$$

THEOREM VI. *For Example A, we have*

$$\sum_{a \in A_{i+}} \frac{1}{a} = \frac{1}{L_i} = \frac{y\left(\frac{1}{y}\right)^{3^i}}{l_i} + \frac{\left(\frac{1}{y}\right)^{3^{i-1}}}{l_{i-1}} + \frac{\left(-\frac{1}{y^6} - \frac{1}{y^8}\right)^{3^{i-2}}}{l_{i-2}} + \frac{\left(-\frac{1}{y^{27}}\right)^{3^{i-3}}}{l_{i-3}}, \tag{29}$$

$$\zeta(1) = yl\left(\frac{1}{y}\right) + l\left(\frac{1}{y} - \frac{1}{y^6} - \frac{1}{y^8} - \frac{1}{y^{27}}\right) = log(y - 1), \tag{30}$$

$$e(\zeta(1)) = y - 1. \tag{31}$$

THEOREM VII. *For Example A, $\zeta(3^n)$ and $\zeta(3^n)/\tilde{\pi}^{3^n}$ are transcendental for all nonnegative integers n.*

THEOREM VIII. *For Example B, we have*

$$\sum_{a \in A_{i+}} \frac{1}{a} = \frac{1}{L_i} = \frac{x^2\left(\frac{1}{x^2}\right)^{4^i}}{l_i} + \frac{\left(\frac{1}{x^2}\right)^{4^{i-1}} + x\left(\frac{1}{x^6}\right)^{4^{i-1}}}{l_{i-1}} + \frac{x\left(\frac{1}{x^{32}}\right)^{4^{i-2}} + \left(\frac{1}{x^{16}}\right)^{4^{i-2}}}{l_{i-2}},$$

$$\zeta(1) = x^2 l\left(\frac{1}{x^2}\right) + l\left(\frac{1}{x^2}\right) + xl\left(\frac{1}{x^6} + \frac{1}{x^{32}}\right) + l\left(\frac{1}{x^{16}}\right) = log(x^8 + x^4 + x^2 + x),$$

$$e(\zeta(1)) = x^8 + x^4 + x^2 + x.$$

THEOREM IX. *For Example B, $\zeta(2^n)$ and $\zeta(2^n)/\tilde{\pi}^{2^n}$ are transcendental for all nonnegative integers n.*

THEOREM X. *For Example C, we have*

$$\sum_{a\in A_{i+}} \frac{1}{a} = \frac{1}{L_i} = \frac{x^2\left(\frac{1}{x^2}\right)^{2^i}}{l_i} + \frac{x\left(\frac{1}{x^3}\right)^{2^{i-1}}}{l_{i-1}} + \frac{x\left(\frac{1}{x^8}\right)^{2^{i-2}} + \left(\frac{1}{x^2}+\frac{1}{x^3}+\frac{1}{x^4}\right)^{2^{i-2}}}{l_{i-2}}$$
$$+ \frac{\left(\frac{1}{x^8}\right)^{2^{i-3}}}{l_{i-3}},$$

$$\zeta(1) = x^2 l\left(\frac{1}{x^2}\right) + xl\left(\frac{1}{x^3}+\frac{1}{x^8}\right) + l\left(\frac{1}{x^2}+\frac{1}{x^3}+\frac{1}{x^4}+\frac{1}{x^8}\right) = log(0),$$

$$e(\zeta(1)) = 0.$$

Remark. For Example C, since $q = 2$, by (12), $\zeta(1) = \tilde{\pi}/d_1$, with $d_1 \in K$. Hence Theorem 5.1 of Jing Yu [Y1] showing the transcendence of $\tilde{\pi}$ takes care of the counterpart of Theorems VII and IX.

We will only prove Theorems VI and VII. The rest are proved similarly.

Proof of Theorem VI. Substituting the data of Example A in (27) and (28), we get

$$f_i = \frac{[i]_y - y[i]_x}{[i]_x - 1}, \qquad g_i = \frac{[i]_y - y^{3^i}[i]_x}{[i+1]_x + 1}.$$

Using the values of g_i, g_{i-1}, and g_{i-2} thus obtained, we can express the right-hand side of (29) as $1/v_i l_i$ where v_i is a rational function with coefficients in $\mathbf{F}_3$ of x, y, $x^{3^{i-2}}$, and $y^{3^{i-2}}$. (See more on this in Section III.) On the other hand, from (23), (27), and (28), we see that μ_i is also such a function. The direct comparison, the details of which we omit, of the complicated expressions thus obtained for these rational functions μ_i, v_i shows that, in fact, $\mu_i = v_i$, thus proving (29). From the formula for g_i given above, we see that $\deg g_i = -3^i$. By induction, (20) then implies that $\deg l_i = -(3/2)(3^i - 1)$. Hence the power series (4) converges when $\deg z < -3/2$. Summing (29) over i running from 0 to ∞, we get the first equality in (30). The second equality of (30) follows by using (5) with $a = y$ and $z = 1/y$. (31) follows from (30) by exponentiating. This completes the proof.

Remark. (29) is not the "simplest" form of the relation between L_i's and l_i's. For example, using the recursion relations for l_i's obtained from (5) with $a = y$, $a = x$, and by evaluation of g_i above respectively, we get the three equalities

$$\frac{1}{L_i} = \frac{1}{l_i} + \frac{y^{3^{i-1}}}{l_{i-1}} + \frac{1}{l_{i-2}} = \frac{1-[i]_x}{l_i} - \frac{y^{3^i}}{l_{i-1}} = \frac{y^{3^i+1} - 1 - [i]_x^2 - [i]_x}{([i+1]_x+1)l_i}.$$

Proof of Theorem VII. According to an analogue (Theorem 5.1 of [Y1]) of the Hermite-Lindemann theorem, $e(z)$ is transcendental if z is nonzero algebraic over K. Hence (31) shows that $\zeta(1)$ is transcendental. Jing Yu has also proved an analogue (Theorems 5.5 and 5.2 of [Y1]) of the Gelfand-Schneider theorem. Let $\alpha = \zeta(1)/\tilde{\pi}$. Then by (31), $e(\alpha\tilde{\pi})$ is algebraic; hence by Theorem 5.2 and Lemma 3.4 of [Y1], to prove that α is transcendental, it is enough to show that α is irrational (i.e., not in K). In fact, we claim that α is not in K_∞: First, note that by the nonarchimedean nature of K_∞, $\zeta(1) \in K_\infty$ has degree 0. Hence (12) implies that $2 \deg \tilde{\pi} = \deg d_1 = 3 \deg x - \deg x_1 = -3$. (The last equality follows by comparing the coefficients of z^q in (1) with $a = x$ and using (2).) Hence $\tilde{\pi}$ is not in K_∞. This proves the claim. We have shown that $\zeta(1)$ and $\zeta(1)/\tilde{\pi}$ are transcendental. On the other hand, it is easy to see that $\zeta(kp^n) = \zeta(k)^{p^n}$. Hence the proof is complete.

III. Generalizations. We now consider the situation where the genus and the class number can be arbitrary. From the list in [LMQ], it follows that apart from rational function fields and the examples of the last section, the only other A with $h = \delta = 1$ is the following example.

Example D (Example 11.6 of [H2]). $A = \mathbf{F}_2[x, y]/y^2 + y = x^5 + x^3 + 1$. This has $g = 2$. We refer to [H2] for values of y_i's.

$$x_1 = (x^2 + x)^2.$$

Conjecture E. For Example D, we have

$$\sum_{a \in A_{i+}} \frac{1}{a} = \frac{1}{L_i} = \frac{x^3\left(\frac{1}{x^3}\right)^{2^i}}{l_i} + \frac{x^2\left(\frac{1}{x^3}+\frac{1}{x^4}\right)^{2^{i-1}}}{l_{i-1}}$$
$$+ \frac{x^2\left(\frac{1}{x^{12}}\right)^{2^{i-2}} + x\left(\frac{1}{x^4}+\frac{1}{x^8}\right)^{2^{i-2}} + \left(\frac{1}{x^4}\right)^{2^{i-2}}}{l_{i-2}}$$
$$+ \frac{\left(\frac{1}{x^4}\right)^{2^{i-3}} + x\left(\frac{1}{x^8}+\frac{1}{x^{12}}\right)^{2^{i-3}}}{l_{i-3}}.$$

We have verified this for $i < 7$. Also, from (15), (16), and the recursion relations for l_i's obtained from (5), it is easy to see that the degrees of both the sides are same.

Further, if we sum both the sides for i from 0 to ∞, we get

$$\zeta(1) = (x^2 + x)\tilde{\pi} = log(0) = x^3 l\left(\frac{1}{x^3}\right) + x^2 l\left(\frac{1}{x^3} + \frac{1}{x^4} + \frac{1}{x^{12}}\right) + xl\left(\frac{1}{x^4} + \frac{1}{x^{12}}\right).$$

This can be directly verified as follows: The first equality follows by (12), the second is clear. If we take $a = x$ and $z = 1/x^3$ in (5), we get $xl(1/x^3) + l(1/x^4 + 1/x^{12}) = a\tilde{\pi}$ for some $a \in A$. Multiplying this equation by $x^2 + x$, the right-hand side of the equation to be verified is seen to be a times the left-hand side. A simple count of degrees shows that $\deg a = 0$ and hence $a = 1$.

Definition. Let $x_1, \ldots, x_n$ be generators of H over $\mathbf{F}_q$. We say that $f(i)$ is an F-function (of i) if there exists $k \in \mathbf{Z}_+$ and $g \in \mathbf{F}_q(X_1, \ldots, X_{2n})$ such that $f(i) = g(x_1^{q^{i-k}}, \ldots, x_n^{q^{i-k}}, x_1, \ldots, x_n)$ for i sufficiently large.

Hypothesis (H). For $k = 0$ to g, (H_k): c_{ik} is a F-function of i.

By Theorems I and IV, (H) holds for $g = 0$ and $g = 1$, respectively.

THEOREM XI. *Assume (H) holds. Then*
(a) $D_i^{q^g}/d_i$ *and* L_i/l_i *and* D_{i+1}/D_i^q *are F-functions of* i;
(b) *for each* k, $A_{ik}l_i^{q^k}$ *is F-function of* i;
(c) $S_i(n) = u(i)/l_i^n = v(i)S_i^n$, *where* $u(i)$ *and* $v(i)$ *are F-functions of* i.

Proof. By Theorem III, the first two claims of (a) are just (H_0) and (H_g). As in Section II, we see that g_i is an F-function, and so the third claim follows from the second by looking at $L_{i+1}l_i/(L_i l_{i+1})$ and using (15) and (19). By (7) and (14), comparing the coefficients of t^{q^k} (for $k = 0, 1, \ldots, k \geqslant g$) in the first formula of Theorem III, we get

$$\frac{1}{l_i} = c_{i0}A_{i0}, \quad \frac{1}{d_1 l_{i-1}^q} = c_{i0}A_{i1} + c_{i1}A_{i0}^q, \ldots, \quad \frac{1}{d_k l_{i-k}^{q^k}} = \sum_{r=0}^{g} c_{ir}A_{i(k-r)}^{q^r} \quad (k \geqslant g).$$

Now g_i is an F-function, and also d_k, being independent of i, is clearly an F-function. Hence (b) easily follows by induction on k using the equations above. (Note that (b) is, in fact, equivalent to (H) by the same reasoning.) By the remark following (18), $S_i(n)l_i^n$ is a polynomial in $A_{ik}l_i^{q^k}$'s with coefficients in $\mathbf{F}_p$, and hence (c) follows from (b), (a), and (8). This completes the proof.

Our conjecture (H) has since been proved (private communication) by Greg Anderson.

Now we explain the motivation behind these investigations. If we guess the "term-by-term" relations (assuming they exist) between the partial zeta sums and logarithms, say as in Theorems VI, VII, X, and conjecture E, and if we know c_{ik}, then we can prove the guessed relation, as in the proof of Theorem VI. Instead of $\zeta(1)$ and $l(z)$, we can also consider $\zeta(n)$ and the "multilogarithm" $l_n(z) := \sum z^{q^i}/l_i^n$ and use (c) of Theorem XI.

In fact, using the notion of tensor products of Drinfeld modules from [A], it was shown in [AT] that, for $A = \mathbf{F}_4[T]$, $\zeta(n)$ is essentially the "last coordinate" of the logarithm of nth tensor power of the Carlitz module (the example of section 0) evaluated at an "algebraic point". ([Y2] contains the relevant transcendence theory.) The "last coordinate" is in some sense a deformation of $l_n(z)$. Now it is clear how to generalize t-motives and their tensor powers of [A] to A-motives and their tensor powers, and so we may expect generalizations of these results. But explicit equations of c_{ik}'s and tensor powers are very complicated, and with an explicit approach looking hopeless, we need a better understanding of the situation.

There is an additional problem when $h > 1$: For example, when $q = 2$, by (12) we have $\zeta(1) = \tilde{\pi}/d_1$. When A has an element, say x, of degree 2, as before we can see that $d_1 = [1]_x/x_1$. But by [H2], $x_1 \in H - K$, so that by Theorem 5.2 of [Y1], $e(\zeta(1))$ is transcendental. On the other hand, $e(d_1\zeta(1)) = 0$ is clearly algebraic. We may expect, in general, that there exists $\theta \in H$ such that $e(\theta\zeta(1))$ lies in A (or, at least, is algebraic). There is no evidence in general. Greg Anderson has suggested the following weaker conjecture: There exist finitely many $h_i \in H$, $k_i \in K$ for i such that $\zeta(1) = \sum h_i l(k_i)$.

Remarks. (I) We have not studied the case when $\delta > 1$. It may be worthwhile to do so. Also, we may generalize by restricting to a in some congruence classes with respect to some ideal I of A (this way, we may be able to handle partial zeta functions) or study singular theory by looking at orders in A.

(II) The connections between zeta values and multilogarithms suggested by [AT] and this paper are quite different in spirit from the relations between the relative classical zeta functions and multilogarithms recently investigated by Zagier. For example, we consider the absolute zeta functions for A, and our logarithms depend on A.

Acknowledgements. I thank Greg Anderson for encouragement and helpful conversations.

References

[A] G. Anderson, *t-motives*, Duke Math. J. **53** (1986), 457–502.

[AT] G. Anderson and D. Thakur, *Tensor powers of the Carlitz module and zeta values*, Ann. of Math. **132** (1990), 159–191.

[C1] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137–168.

[C2] ———, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 167–182.

[C3] ———, *A set of polynomials*, Duke Math. J. **6** (1940), 486–504.

[D] V. Drinfeld, *Elliptic modules*, English translation, Math. USSR-Sb. **23** (1974), 561–592.

[G] D. Goss, *v-adic zeta functions, l-series, and measures for function fields*, Invent. Math. **55** (1979), 107–119.

[H1] D. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[H2] ———, "Explicit class field theory in global function fields" in *Studies in Algebras and Number Theory*, ed. by G. C. Rota, Adv. Math. Suppl. Stud. **6**, Academic Press, New York, 1979, 173–217.

[LMQ] J. LEITZEL, M. MADAN, AND C. QUEEN, *On congruence function fields of class number one*, J. Number Theory **7** (1975), 11–27.

[R] M. ROSEN, *The Hilbert class field in function fields*, Exposition. Math. **5** (1987), 365–378.

[T1] D. THAKUR, *Zeta measure associated to* $\mathbf{F}_q[T]$, J. Number Theory **35** (1990), 1–17.

[T2] ———, *Continued fractions for* $\mathbf{F}_q[T]$, J. Number Theory **41** (1992), 150–155.

[T3] ———, *Gamma functions for function fields and Drinfeld modules*, Ann. of Math. **134** (1991), 25–64.

[T4] ———, *Shtukas and Jacobi sums*, to appear in Invent. Math.

[Y1] J. YU, *Transcendence and Drinfeld modules*, Invent. Math. **83** (1986), 507–517.

[Y2] ———, *Transcendence and special zeta values in characteristic p*, Ann. of Math. **134** (1991), 1–24.

SCHOOL OF MATHEMATICS, TATA INSTITUTE OF FUNDAMENTAL RESEARCH, BOMBAY 5, INDIA