Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 116

Frobenius distributions of Drinfeld modules over finite fields

Ernst-Ulrich Gekeler

Saarbrücken 2004

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 116
submitted: November 19, 2004

Frobenius distributions of Drinfeld modules over finite fields

Ernst-Ulrich Gekeler

Saarland University
Department of Mathematics
Postfach 15 11 50
D–66041 Saarbrücken
Germany
gekeler@math.uni-sb.de

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

FROBENIUS DISTRIBUTIONS OF DRINFELD MODULES OVER FINITE FIELDS

ERNST-ULRICH GEKELER

0. Introduction.

The topic of this article is the variation of characteristic polynomials of Drinfeld modules of rank two over finite fields.

Let $\mathbb{F} = \mathbb{F}_q$ be the finite field with q elements, A the polynomial ring $\mathbb{F}[T]$ and L a finite field provided with a structure of A-algebra. Any Drinfeld A-module ϕ over L (we always suppose that the rank equals two) gives rise to a Frobenius endomorphism $F = F_L$, which satisfies a quadratic equation $F^2 - aF + b = 0$ with $a, b \in A$. The coefficients of the characteristic polynomial $P_{\phi,L}(X) = X^2 - aX + b$ of F (or ϕ) are subject to restrictions similar to those of the characteristic polynomials of Frobenius endomorphisms of elliptic curves over finite fields. For example, P_ϕ is a square or irreducible, in which case its splitting field is "imaginary quadratic", i.e., inert or ramified at the place at infinity of $K = \mathrm{quot}(A)$.

As for elliptic curves, natural questions arise, e.g.:

(A) Which polynomials of the given shape actually come from Drinfeld modules?

(B) How many ϕ over L are there such that $P_{\phi,L}(X) = X^2 - aX + b$, a and b being given?

Whereas (A) is implicitly or explicitly answered in [5], [9], [19], the situation is more involved for (B). On the one hand, (B) is related to class numbers in imaginary quadratic orders over A, and an explicit formula may be given via the analytic class number formula. This is worked out in the case where L is an A-prime field $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$ with a prime ideal $\mathfrak{p}$ of A: see (6.19), which allows fast calculation of the number in question. On the other hand, that formula fails to explain the variation of the corresponding class numbers with the coefficients a, b.

Our main result is Theorem 8.17, which expresses the weighted class number $h^*(a, b, \mathfrak{p})$ of Drinfeld modules ϕ over $\mathbb{F}_\mathfrak{p}$ with $P_{\phi,\mathbb{F}_\mathfrak{p}}(X) = X^2 - aX + b$ as a product of $\mathfrak{l}$-local contributions $v_\mathfrak{l}(a, b)$, where $\mathfrak{l}$ runs through the places of K. For $\mathfrak{l}$ finite, $v_\mathfrak{l}(a,b)$ has an intuitive description as a continuous local density function of $A_\mathfrak{l} \times A_\mathfrak{l}$ (Definition 7.1). We may thus state that $h^*(a,b,\mathfrak{p})$ is "explained" by the frequencies of matrices $M \in \mathrm{Mat}(2, A_\mathfrak{l})$ with the given characteristic polynomial $X^2 - aX + b$, $\mathfrak{l}$ ranging through the finite places. The factor $v_\infty(a,b)$ (which corresponds to the Sato-Tate function $\frac{2}{\pi}\sqrt{1-a^2/4b}$) is of a different nature; its shape distinguishes the cases where char($\mathbb{F}$) is odd or even.

Theorem 8.17 is analogous with Theorem 5.5 of [11], a similar result for elliptic curves over finite prime fields $\mathbb{F}_p$. It is funny to note that the result for elliptic curves was motivated by observations from extensive calculations with Drinfeld modules (see [14]). On the other hand, the results of [11] led to consider the present factors $v_\mathfrak{l}(a,b)$, and to the precise shape of the formula in Theorem 8.17.

Besides the intrinsic interest of these problems and, once again, the flow of information (in both directions) between "Drinfeld modules of rank two" and "elliptic curves", there are relations to Sato-Tate-like questions, and to the construction of curves over finite fields with many rational points, in that the quantities that appear in our formulas also govern the geometry of certain Drinfeld modular curves (see [7], [17]).

It is obvious that most of the questions addressed (and some of the methods used and results obtained) in this paper may be generalized to arbitrary Drinfeld modules without any restriction on the rank or the nature of the base ring A. We restricted to the present setting, rich enough to show all facets of the general problem, in order to avoid technical difficulties that would obscure the overall picture.

We now briefly describe the contents of the different sections. After assembling the framework in section 1, we study in section 2 the behavior of $P_{\phi,L}$ under twists of ϕ and automorphisms of A, and present formulas for the absolute term b of $P_{\phi,L}$ (Theorem 2.11) and the leading coefficient of the Frobenius trace a (Proposition 2.14, due to F. Jung [14]). Theorem 2.11 appears, in much greater generality, in [13]; we fill a gap in the argument *loc. cit.* In section 3 we describe how $P_{\phi,L}$ can be calculated in practice, which is more involved than the corresponding problem for elliptic curves. A highly efficient procedure, based on a Deligne-like congruence between Hasse invariants and Eisenstein series, is given in (3.7). It works for prime fields $L = \mathbb{F}_\mathfrak{p}$ only, an assumption maintained from now on. In section 4 we determine the ratio between the numbers of ϕ/L with Frobenius traces of maximal/non-maximal degree (Theorem 4.2). We show in Theorem 5.2: For $d = \deg\ \mathfrak{p} \leq 3$, the numbers $d(a,\mathfrak{p})$ (resp. $h(a,\mathfrak{p})$) of Drinfeld modules (resp. of isomorphism classes of Drinfeld modules) over $\mathbb{F}_{\mathfrak{p}}$ with Frobenius trace a depend only on d and the degree of a.

In section 6, we relate $h^*(a,b,\mathfrak{p})$ with class numbers of imaginary quadratic orders over A. Section 7 is devoted to the study of $v_{\mathfrak{l}}(a,b)$ for finite $\mathfrak{l}$. We give an explicit expression in Theorem 7.8 and Corollary 7.9 and restrict the proof to the (more elaborate) case of $\mathrm{char}(\mathbb{F}) = 2$, since the proof given in [11] for a similar assertion about elliptic curves easily adapts to the present case of odd characteristics. In section 8 we determine some ingredients of earlier formulas that are associated with the polynomial $X^2 - aX + b$, which leads to the final result Theorem 8.17. As usual, the case of characteristic 2 is the most involved.

Parts of this paper are motivated from the calculations performed in [14]. Along with the author of that thesis, I would like to express my gratitude to Max Gebhardt and Andreas Schweizer for helpful discussions.

1. Background.

Throughout, we use the following notation:
(1.1)

$\mathbb{F}$	$=$	$\mathbb{F}_q$, a finite field with q elements, of characteristic p
A	$=$	$\mathbb{F}[T]$, the polynomial ring over $\mathbb{F}$ in an indeterminate T, with degree function "deg"
K	$=$	$\mathbb{F}(T)$, the quotient field of A
K_∞	$=$	$\mathbb{F}((T^{-1}))$, the completion of K at the infinite place, provided with its normalized absolute value "$\lvert\ .\ \rvert$", where $\lvert T\rvert = q$.

We write $\mathrm{sgn}(a) \in \mathbb{F}$ for the leading coefficient of an element a of A, and extend this notation to $0 \neq a \in K_\infty$.

L	$=$	a field provided with a structure $\gamma:\ A \to L$ as an A-algebra; thus L is an extension either of K or of some $\mathbb{F}_{\mathfrak{p}}$, in which case we write $\mathfrak{p} = \mathrm{char}_A(L)$ for its A-characteristic. Here
$\mathbb{F}_{\mathfrak{p}}$	$=$	$A/\mathfrak{p}$ with a (maximal) prime ideal $\mathfrak{p}$ of A, of degree $d = \deg\ \mathfrak{p}$

By abuse of notation, we also write $\mathfrak{p}$ for the monic irreducible polynomial that generates $\mathfrak{p}$. We identify the copies of $\mathbb{F}$ inside A and $\mathbb{F}_{\mathfrak{p}}$ through the natural map. Places $\mathfrak{l}$ of K either correspond to prime ideals of A, in which case we call $\mathfrak{l}$ finite and use the same symbol $\mathfrak{l}$ for "place" and "prime ideal", or $\mathfrak{l} = \infty$, the infinite place. The symbol $\tau = \tau_q$ denotes the additive polynomial X^q, regarded as an $\mathbb{F}$-linear endomorphism of the additive group scheme $\mathbb{G}_a$ over L. Hence the ring

$$\mathrm{End}_{L,\mathbb{F}}(\mathbb{G}_a) = \{\sum a_i X^{q^i} \mid a_i \in L\}$$

of all $\mathbb{F}$-linear endomorphisms of $\mathbb{G}_a/L$ will be regarded as the skew polynomial ring $L\{\tau\} = \{\sum a_i\tau^i \mid a_i \in L\}$ in the non-commutative indeterminate τ with commutation rule $\tau c = c^q\tau$ $(c \in L)$.

(1.2) A *Drinfeld A-module* over L (see e.g. [12], [21], [16]) is the A-module structure on $\mathbb{G}_a/L$ given through a ring homomorphism

$$\begin{array}{rccl} \phi: & A & \longrightarrow & \mathrm{End}_{L,\mathbb{F}}(\mathbb{G}_a) \\ & a & \longmapsto & \phi_a \end{array}$$

subject to

(i) ϕ is $\mathbb{F}$-linear
(ii) $\phi_a = \gamma(a) + \sum_{i\geq 1} \ell_i(a)\tau^i$ for $a \in A$.

It is uniquely determined through

$$\phi_T = \gamma(T) + \sum_{1\leq i\leq r} \ell_i(T)\tau^i,$$

which may be prescribed arbitrarily. We always assume that $\ell_r(T) \neq 0$, where r is the *rank* of ϕ. In case $r = \mathrm{rank}(\phi) = 2$ (essentially the only case treated in this article), we write $\phi_T = \gamma(T) + g\tau + \Delta\tau^2$, $\Delta \neq 0$, and briefly $\phi = (g, \Delta)$.

A *morphism* from the Drinfeld module ϕ/L to the Drinfeld module ψ/L is some $u \in L\{T\}$ such that $u\phi_a = \psi_a u$ for $a \in A$ (it suffices to require this for $a = T$). Similarly, we define endo-, iso-, and automorphisms. The endomorphism ring $\mathrm{End}_L(\phi)$ of a Drinfeld module ϕ over L of rank $r > 0$ has the following properties:

(1.3)

(i) It contains the subring $A \xrightarrow{\cong} \phi(A) \hookrightarrow L\{T\}$;
(ii) it is a free A-module of dimension a divisor of r^2 ([4], [2]);
(iii) $\mathrm{End}_L(\phi) \otimes_A K_\infty$ is a division algebra over K_∞ (*loc. cit.*).

We define the absolute invariant $j = j(\phi)$ of a rank-two Drinfeld module $\phi = (g, \Delta)$ as $j = g^{q+1}/\Delta$. Then we have the following easily proved criterion:

(1.4) Two rank-two Drinfeld modules $\phi = (g, \Delta)$ and $\phi' = (g', \Delta')$ over L are isomorphic if and only if there exists $c \in L^*$ such that $g' = c^{q-1}g$, $\Delta' = c^{q^2-1}\Delta$. This is also equivalent with

(i) $j(\phi) = j(\phi')$ and
(ii) g'/g is a $(q-1)$-th power in L (if $j = j(\phi) = j(\phi') \neq 0$)
Δ'/Δ is a (q^2-1)-th power in L (if $j = 0$).

Further, the automorphism group of $\phi = (g, \Delta)$ over L is

$$\mathrm{Aut}_L(\phi) = \begin{array}{ll} \mathbb{F}^* & \text{if } j \neq 0 \text{ or } L \text{ doesn't contain } \mathbb{F}^{(2)} \\ \mathbb{F}^{(2)*} & \text{otherwise.} \end{array} \tag{1.5}$$

Here $\mathbb{F}^{(2)}$ is the unique quadratic extension of $\mathbb{F}$ contained in the algebraic closure $\overline{L}$ of L.

From now on, if not stated otherwise, we assume that L is an extension of degree m of $\mathbb{F}_{\mathfrak{p}}$, and Drinfeld modules have rank two. Thus

$$[L : \mathbb{F}] = [L : \mathbb{F}_{\mathfrak{p}}] \cdot [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}] = m \cdot d =: n.$$

From (1.4) and (1.5) we get:

1.6 Proposition.
(i) *The number of (rank-two) Drinfeld modules over L is* $q^n(q^n - 1)$.
(ii) *The number of isomorphism classes of such modules is* $(q^n - 1)(q - 1) + \#(L^*/L^{*q^2-1})$. $\square$

Since $\#(L^*/L^{*q^2-1}) = q^2 - 1$ (resp. $q - 1$) if n is even (resp. odd), we also find:

1.7 Corollary. $\sum \frac{1}{\#\mathrm{Aut}_L(\phi)} = q^n = \#(L)$, *where the sum is over the isomorphism classes of* ϕ/L. $\square$

As $\phi = (g, \Delta)$ is defined over L, the polynomials ϕ_a commute with the *Frobenius element* $F = F_L = \tau^n$ of L, i.e., $F \in \mathrm{End}_L(\phi)$. In view of (1.3), F must satisfy a polynomial equation over A, so it has a uniquely determined monic minimal polynomial $M_{\phi,L}(X) \in A[X]$.
(Note that we have identified the subring $\phi(A)$ of $L\{\tau\}$ with A.) We have the following result, which is part of the far-reaching analogy between elliptic curves and Drinfeld modules of rank two.

1.8 Theorem [9]. *Let ϕ be a rank-two Drinfeld module over L, where $[L : \mathbb{F}_{\mathfrak{p}}] = m$, with Frobenius endomorphism $F = F_L$. There exists a polynomial $P_{\phi,L}(X) = X^2 - aX + b \in A[X]$, the* characteristic polynomial *of ϕ, with the following properties:*
(i) $P_{\phi,L}(X) = M_{\phi,L}(X)$ *or* $M_{\phi,L}(X)^2$. *In particular,* $P_{\phi,L}(F) = 0$.
(ii) *The ideal* (b) *equals* $\mathfrak{p}^m$, *thus* $b = \epsilon(\phi)\mathfrak{p}^m$ *with* $\epsilon(\phi) = \mathrm{sgn}(b) \in \mathbb{F}^*$.
(iii) $M_{\phi,L}$ *is irreducible over* K_∞. *In particular,* $2 \deg\ a \leq 1 \deg b = n$.

Note that $P_{\phi,L}(F) = 0$ means that we have the equation

$$F^2 - \phi_a F + \phi_b = 0 \tag{1.9}$$

in $L\{\tau\}$. The quantities $a = a(\phi)$ and $b = b(\phi)$ are called the *Frobenius trace* and *norm*, respectively, of ϕ. Two Drinfeld modules ϕ and ψ are *isogeneous* if they are connected through a non-zero morphism. Being isogeneous is in fact symmetric and therefore an equivalence relation.

1.10 Theorem [9]. *Let ϕ and ψ be (rank-two) Drinfeld modules over L. The following are equivalent:*

(i) *ϕ and ψ are isogeneous;*
(ii) *$\mathrm{End}_L(\phi) \otimes_A K$ and $\mathrm{End}_L(\psi) \otimes_A K$ are isomorphic K-algebras;*
(iii) *$M_{\phi,L} = M_{\psi,L}$;*
(iv) *$P_{\phi,L} = P_{\psi,L}$.*

We aim to study

$$h(a,b,L) = \begin{array}{l}\text{number of isomorphism classes of}\\ \text{Drinfeld modules } \phi \text{ over } L \text{ with}\\ P_{\phi,L}(X) = X^2 - aX + b\end{array} \tag{1.11}$$

and its variation with a and $b \in A$ subject to the conditions given by (1.8). Theorem 8.17 yields a satisfactory description at least in the case where $L = \mathbb{F}_\mathfrak{p}$, a "prime A-field".

1.12 Remarks.

(i) (1.8) and (1.10) are mere special cases of much more general results, valid for arbitrary ranks r and Drinfeld rings A not necessarily polynomial: see [9].
(ii) $P_{\phi,L}(X)$ is the characteristic polynomial of F in the representations of $\mathrm{End}_L(\phi)$ in the various v-adic Tate modules $T_v(\phi)$ of ϕ, which explains the name *(loc. cit.)*.
(iii) $P_{\phi,L} = M_{\phi,L}$ is the generic case, $P_{\phi,L} = M_{\phi,L}^2$ occurs only if ϕ is supersingular *(loc. cit)* and $m = [L : \mathbb{F}_\mathfrak{p}]$ is even.

2. Properties of the characteristic polynomial.

As before, $\phi = (g, \Delta)$ is a rank-two Drinfeld module over the finite A-field L, $[L : \mathbb{F}_\mathfrak{p}] = m$, $\#(L) = q^n$, $n = md$. We let $N = N_\mathbb{F}^L$ be the norm map from L to $\mathbb{F} = \mathbb{F}_q$. As results from (1.4), the *L-forms* of ϕ (i.e., Drinfeld modules ϕ'/L which become isomorphic with ϕ over the algebraic closure $\overline{L}$) are the modules

$$\begin{array}{lcll} \phi^{(c)} & = & (cg, c^{q+1}\Delta) & \text{if } j \neq 0, \text{ i.e., } g \neq 0, \\ \phi^{(c)} & = & (0, c\Delta) & \text{if } j = 0 \end{array} \tag{2.1}$$

with $c \in L^*$, where the L-isomorphism type of $\phi^{(c)}$ depends on $c \pmod{L^{*q-1}}$ or $c \pmod{L^{*q^2-1}}$, respectively.

2.2 Proposition. *Let ϕ have characteristic polynomial $P_{\phi,L}(X) = X^2 - aX + b$ and invariant $j(\phi) \neq 0$. Then*

$$P_{\phi^{(c)},L}(X) = X^2 - \nu^{-1}aX + \nu^{-2}b,$$

where $\nu = N(c)$.

Proof. Choose a $(q-1)$-the root ζ of c and put $L' = L(\zeta)$. Then $\phi_T\zeta = \zeta\phi_T^{(c)}$, so ζ is an isomorphism, defined over L', from $\phi^{(c)}$ to ϕ. In particular, $\phi_a\zeta = \zeta\phi_a^{(c)}$ for arbitrary $a \in A$. The ring isomorphism $\phi_a \longmapsto \phi_a^{(c)} = \zeta^{-1}\phi_a\zeta$ from $\phi(A)$ to $\phi^{(c)}(A)$ extends to an isomorphism $(\ )^{(c)} : f \longmapsto f^{(c)} = \zeta^{-1}f\zeta$ from $\mathrm{End}_L(\phi) =$ centralizer of $\phi(A)$ in $L\{\tau\}$ to $\mathrm{End}(\phi^{(c)})$, and maps the Frobenius $F = \tau^n$ to $\zeta^{-1}F\zeta = \zeta^{q^n-1}F = \nu F$. Applying $(\ )^{(c)}$ to (1.9) yields $(\nu F)^2 - \phi_a^{(c)} + \phi_b^{(c)} = 0$, thus $F^2 - \phi_{a/\nu}^{(c)}F + \phi_{b/\nu^2}^{(c)} = 0$. □

The behavior of $P_{\phi,L}$ under twists $\phi \longrightarrow \phi^{(c)}$ is slightly more complicated if $j(\phi) = 0$. Since it is inessential for our purposes, its elementary study will be omitted.

An element σ of $\mathrm{Gal}(L|\mathbb{F}_\mathfrak{p})$ may be applied to the coefficients of ϕ and thereby yields a new Drinfeld module $\phi^{(\sigma)}$ over L. It is obvious that

$$P_{\phi^{(\sigma)},L} = P_{\phi,L} \tag{2.3}$$

holds. Another invariance property of $P_{\phi,L}$ results from the existence of non-trivial $\mathbb{F}$-automorphisms on A. Viz, let $G = \{\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \mid u, v \in \mathbb{F}, u \neq 0\}$ be the affine group over $\mathbb{F}$. It acts on A through substitutions:

$$f^\alpha(T) = f(\alpha(T)), \quad f \in A,\ \alpha = \left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right),$$

$\alpha(T) = uT + v$. Let L be an extension of $\mathbb{F}_\mathfrak{p}$, and for $\alpha \in G$, choose an isomorphism $\alpha_L : L \longrightarrow L'$ of $\mathbb{F}$-algebras which makes the diagram

$$\begin{array}{ccccc} A & \longrightarrow & \mathbb{F}_\mathfrak{p} & \hookrightarrow & L \\ \alpha\downarrow & & \downarrow & & \alpha_L\downarrow \\ A & \longrightarrow & \mathbb{F}_{\mathfrak{p}'} & \hookrightarrow & L' \end{array} \tag{2.4}$$

commutative. Here $\mathfrak{p}'$ is the prime $\mathfrak{p}^\alpha$, and the middle vertical arrow is $a \pmod{p} \longmapsto a^\alpha \pmod{p^\alpha}$. Via α_L we may push forward a Drinfeld module $\phi = (g, \Delta)$ from L to a module $\phi^\alpha = (g^{\alpha_L}, \Delta^{\alpha_L})$ on L'. Now

α_L is not unique (given $m = [L : \mathbb{F}_\mathfrak{p}]$, there are m choices of α_L), but the characteristic polynomial of ϕ^α will be independent of the choice made, due to (2.3). In fact:

2.5 Proposition. *If* $P_{\phi,L}(X) = X^2 - aX + b$ *then* $P_{\phi^\alpha,L}(X) = X^2 - a^\alpha X + b^\alpha$.

Proof. We extend α_L to an isomorphism of $L\{\tau\}$ with $L'\{\tau\}$ by $\alpha_L(\tau) = \tau$ and find the identity $\phi^\alpha \circ \alpha = \alpha_L \circ \phi$ of ring homomorphisms. Applying α_L to (1.9) we get

$$\begin{array}{rccccc} 0 & = & \alpha_L \circ F^2 & - & \alpha_L \circ \phi_a F & + & \alpha_L \circ \phi_b \\ & = & F^2 & - & (\phi^\alpha \circ \alpha)_a F & + & (\phi^\alpha \circ \alpha)_b \\ & = & F^2 & - & \phi^\alpha_{a^\alpha} F & + & \phi^\alpha_{b^\alpha}. \end{array}$$

□

(2.6) We next want to describe the coefficient $\epsilon(\phi) = \mathrm{sgn}(b) \in \mathbb{F}^*$ that determines the absolute term of $P_{L,\phi}(X)$. We need some preparations. For $w_1, \ldots, w_k$ in the algebraic closure $\overline{L}$ of L, the *Moore determinant* (see [12] sect. 1.3) is defined as

$$M(w_1, \ldots, w_k) = \det \begin{pmatrix} w_1 & , \ldots , & w_k \\ w_1^q & , \ldots , & w_k^q \\ \vdots & & \\ w_1^{q^{k-1}} & , \ldots , & w_k^{q^{k-1}} \end{pmatrix}.$$

Its crucial properties are:

$$M(C \begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix}) = \det(C) M(w_1, \ldots, w_k) \tag{2.7}$$

for each $k \times k$-matrix C over $\mathbb{F} = \mathbb{F}_q$.

(2.8) Let W be an $\mathbb{F}$-subspace of dimension k of $\overline{L}$, with basis $\{w_1, \ldots, w_k\}$. Then

$$\delta(W) := \prod_{0 \neq w \in W} w = (-1)^k M(w_1, \ldots, w_k)^{q-1}.$$

Here (2.7) is obvious since $w \longmapsto w^q$ is $\mathbb{F}$-linear, and (2.8) is Corollary 1.3.8 of [12].

2.9 Proposition. *Let L have degree n over $\mathbb{F}$, and let W be a finite-dimensional $\mathbb{F}$-subspace of $\overline{L}$ stable under the map $F : x \longmapsto x^{q^n}$ given by the Frobenius of L. With $\delta(W)$ as in* (2.8), *we have*

$$\det_{\mathbb{F}}(F|_W) = N^L_{\mathbb{F}}((-1)^{\dim\, W} \delta(W)).$$

Proof. Let C be the matrix of $F|_W$ w.r.t. a basis $\{w_1, \ldots, w_k\}$ of W. Then on the one hand,

$$\begin{aligned} M(F \begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix}) &= M(C \begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix}) = \det(C) M(w_1, \ldots, w_k) \\ &= \det_{\mathbb{F}}(F|_W) M(w_1, \ldots, w_k), \end{aligned}$$

on the other hand, that expression equals $M(w_1, \ldots, w_k)^{q^n}$. Therefore, and by (2.8),

$$\det_{\mathbb{F}}(F|_W) = M(w_1, \ldots, w_k)^{q^n - 1} = N((-1)^k \delta(W)).$$

□

(2.10) Recall that the $(q-1)$-th power residue symbol $\{\frac{a}{\mathfrak{p}}\}$ for $a \in A$ is defined as the unique element of $\mathbb{F}$ that satisfies the congruence

$$\{\frac{a}{\mathfrak{p}}\} \equiv a^{(q^d - 1)/(q-1)} (\mathrm{mod} \ \ \mathfrak{p}),$$

where $d = \deg \mathfrak{p}$. It is extended by linearity to arbitrary ideals $\mathfrak{b}$ instead of $\mathfrak{b} = \mathfrak{p}$ prime. If b is a generator of $\mathfrak{b}$, we also write $\{\frac{a}{b}\}$ for $\{\frac{a}{\mathfrak{b}}\}$; note that $\{\frac{a}{b}\}$ ignores $\mathrm{sgn}(b)$. Then for two coprime elements a and b of A, the following reciprocity law holds:

$$\{\frac{a}{b}\}\{\frac{b}{a}\}^{-1} = (-1)^{\deg \ a \cdot \deg \ b} \mathrm{sgn}(a)^{\deg \ b} \mathrm{sgn}(b)^{-\deg \ a}.$$

See [16] Ch. 3 for a proof, or [15] Theorems 9.3 and 5.4 for a generalization to arbitrary function fields K.

2.11 Theorem. *(see also* [13]*). With notation as before, the absolute term b of $P_{\phi,L}(X)$ is $b = \epsilon(\phi)\mathfrak{p}^m$ with*

$$\epsilon(\phi) = (-1)^n N(\Delta)^{-1}.$$

Proof. Without restriction, $\mathfrak{p} \neq (T)$, otherwise we replace T by $T' = T + 1$. Then $W := \{x \in \overline{L} \mid \phi_T(x) = 0\}$ is a two-dimensional $\mathbb{F}$-space stable under $F = \tau^n$, and

$$\det_{\mathbb{F}}(F|_W) = \{\frac{b}{T}\}. \tag{1}$$

To prove the assertion, we calculate the determinant in a different manner. The polynomial

$$\Delta^{-1}\phi_T(X) = X^{q^2} + (g/\Delta)X^q + (\gamma(T))/\Delta)X$$

equals $\prod_{w \in W}(X - w)$, so $\delta(W) = \gamma(T)/\Delta$. Referring to (2.9), we have

$$\det_{\mathbb{F}}(F|_W) = N(\gamma(T)/\Delta). \tag{2}$$

Since $\gamma(T) \in \mathbb{F}_{\mathfrak{p}}$, its norm $N(\gamma(T))$ is

$$(3) \qquad \begin{aligned} N_{\mathbb{F}}^{L}(\gamma(T)) &= N_{\mathbb{F}}^{\mathbb{F}_{\mathfrak{p}}}(\gamma(T))^m = \gamma(T^{(q^d-1)/(q-1)})^m \\ &= \{\tfrac{T}{\mathfrak{p}}\}^m = \{\tfrac{T}{b}\}, \end{aligned}$$

as $\mathfrak{p}^m = (b)$. Combining (1), (2), (3) yields

$$(4) \qquad \{\frac{b}{T}\}\{\frac{T}{b}\}^{-1} = N(\Delta)^{-1}.$$

Together with (2.10), and taking deg $b = n$ into account, we find $N(\Delta)^{-1} = (-1)^n \operatorname{sgn}(b)$. □

We conclude this section with some results about the term of maximal possible degree in the Frobenius trace a of ϕ/L.

Given $\phi = (g, \Delta)$, we write the polynomial ϕ_{T^i} as

$$(2.12) \qquad \phi_{T^i} = \sum_{0 \le j \le 2i} f_{i,j}\tau^j, \quad f_{i,j} \in L.$$

Then $f_{i,0} = \gamma(T^i)$, $f_{1,1} = g$, $f_{1,2} = \Delta$, and from $\phi_{T^{i+1}} = \phi_{T^i}\phi_T = \phi_T\phi_{T^i}$ we derive the recursions

$$\begin{aligned} f_{i+1,j} &= \gamma(T)^{q^j} f_{i,j} + g^{q^{j-1}} f_{i,j-1} + \Delta^{q^{j-2}} f_{i,j-2} \\ &= \gamma(T) f_{i,j} + g f_{i,j-1}^{q} + \Delta f_{i,j-2}^{q^2}, \end{aligned}$$

where $f_{i,j} = 0$ if $j < 0$. It is straightforward to show that $f_{i,j}$ is an isobaric expression of weight $q^j - 1$ in g and Δ (with weights $q-1$ and q^2-1, respectively), and that

$$(2.13) \qquad \begin{aligned} f_{i,2i} &= \Delta^{(q^{2i}-1)/(q^2-1)} \\ f_{i,2i-1} &= \Delta^{(q^{2i}-1)/(q^2-1)} \textstyle\sum_{0 \le j \le i-1} g^{q^{2j}} \Delta^{-(q^{2i-1}+q^{2j})/(q+1)} \end{aligned}$$

hold.

2.14 Proposition *(see* [14]*). Let $a = \sum_{0 \le i \le [n/2]} a_i T^i$ be the Frobenius trace of ϕ/L, $\phi = (g, \Delta)$.*

(i) *For n even, let $\mathbb{F}^{(2)}$ be the unique quadratic extension of $\mathbb{F}$ in L. Then*

$$a_{n/2} = \operatorname{Tr}_{\mathbb{F}}^{\mathbb{F}^{(2)}}(N_{\mathbb{F}^{(2)}}^{L}(\Delta)^{-1}).$$

(ii) *For n odd, we have*

$a_{(n-1)/2} = -N(g)^{-1}\operatorname{Tr}_{\mathbb{F}}^{L}(j(\phi)^{(q^n-q)/(q^2-1)+1})$ *if* $g \neq 0$, *and* $a = 0$ *if* $g = 0$.

Proof. (i) Equating the coefficients of τ^{2n} in (1.9), we find

$$1 - a_{n/2} f_{n/2,n} + \epsilon(\phi) f_{n,2n} = 0.$$

With the values for $f_{i,2i}$ and $\epsilon(\phi)$ provided by (2.13) and (2.11), we solve for $a_{n/2}$, which yields the stated result.

(ii) $a = 0$ for $g = 0$ is obvious, since F^2 and ϕ_b involve only even terms in τ, whereas $\phi_a F$ is an "odd" polynomial in τ if $a \neq 0$. Let $g \neq 0$. By (2.2), it suffices to prove the assertion for $g = 1$ or equivalently, $j = \Delta^{-1}$. We equate the coefficients of τ^{2n-1} in (1.9), which gives

$$-a_{(n-1)/2} f_{(n-1)/2,n-1} + \epsilon(\phi) f_{n,2n-1} = 0.$$

Solving for $a_{(n-1)/2}$ and taking into account that

$$\Delta^{(q^{2n}-1)/(q^2-1)} = \Delta^{(q^n-1)/(q-1)} = N(\Delta)$$

since n is odd, we first find

$$a_{(n-1)/2} = -\Delta^{-(q^{n-1}-1)/(q^2-1)} \sum_{0 \leq i \leq n-1} \Delta^{-(q^{2n-1}+q^{2i})/(q+1)}.$$

Let $e_i := \frac{q^{n-1}-1}{q^2-1} + \frac{q^{2n-1}+q^{2i}}{q+1}$ be the exponent of the i-th term in the above sum of $\Delta^{-1} = j(\phi)$, and let $e_i' = [(q^n - q)(q^2 - 1) + 1]q^i$ be the exponent of

$$\mathrm{Tr}_{\mathbb{F}}^{L}(j(\phi)^{(q^n-q)/(q^2-1)+1}) = - \sum_{0 \leq i < n} j(\phi)^{[(q^n-q)/(q^2-1)+1]q^i},$$

$0 \leq i < n$.
Note that e_i' is defined by the same formula for each $i \geq 0$, and is periodic (mod q^n) with period n. A straightforward calculation reveals the congruence

$$e_i \equiv e'_{2i-1+n} (\mathrm{mod} \ \ q^n - 1),$$

valid for $0 \leq i < n$, which yields the assertion in view of the oddness of n. □

2.15 Remarks. (i) Like (1.8) and (1.10), the formula (2.11) for $\epsilon(\phi)$ holds in much greater generality, see [13] Thm. 3.1. Our proof follows essentially Hsia and Yu's, except for the use of the Moore determinant, which replaces the argument *loc. cit.* p. 266.

(ii) Closed formulas similar to (2.14), but of increasing complexity, may be worked out for other coefficients a_i of the Frobenius trace a. Also, (2.14)(i) is a special case of [13] Thm. 5.1, whereas (2.14)(ii) has first been given in [14].

3. How to find $P_{\phi,L}$.

Keeping the setting and notations of the last section, we sketch how to determine $P_{\phi,L}(X)$ in practice. Recall that finding the characteristic polynomial of the Frobenius of an elliptic curve over a finite field L amounts to finding the number of solutions of a defining equation over L. This is very simple theoretically and also algorithmically, provided L is not too large. In the absence of simplifying assumptions (as e.g. in (3.7)), the calculation of $P_{\phi,L}(X)$ is much more involved. Viz, the equation (1.9), i.e.,

$$\tau^{2n} - \phi_a \tau^n + \epsilon(\phi)\phi_{\mathfrak{p}^n} = 0 \tag{3.1}$$

is equivalent with the system of linear equations for the $[n/2]+1$ unknown coefficients $a_i \in \mathbb{F}$ of $a = \sum a_i T^i$ described below. Write

$$\sum_{0 \le i \le n = dm} p_i T^i \quad (p_i \in \mathbb{F},\ p_n = 1)$$

for the monic generator $\mathfrak{p}^m(T)$ of the ideal $\mathfrak{p}^m$. With $f_{i,j} \in L$ as in (2.12), (3.1) becomes

$$\tau^{2n} - \sum_{i \le n/2} a_i \sum_{j \le 2i} f_{i,j}\tau^{j+n} + \epsilon(\phi) \sum_{i \le n}\sum_{j \le 2i} p_i f_{i,j} \tau^j = 0. \tag{3.2}$$

Note that the left hand side is divisible by τ^n, and so (3.1) is equivalent with the system of $n+1$ equations

$$-\sum_{0 \le i \le n/2} a_i f_{i,j-n} + \epsilon(\phi) \sum_{j/2 \le i \le n} p_i f_{i,j} = \begin{cases} -1, & j = 2n \\ 0, & j < 2n \end{cases} \tag{3.3}$$

for the unknowns $a_0, \ldots, a_{[n/2]}$, for $n \le j \le 2n$. Re-indexing the coefficients of the a_i shows that

- the j-the equation in (3.3) is redundant, where

$$\begin{array}{lllll} j = & 2n-1, & 2n-3, & \ldots, & n+1 & \text{if } n \text{ is even,} \\ j = & 2n, & 2n-2, & \ldots, & n+1 & \text{if } n \text{ is odd;} \end{array}$$

- the remaining system (which consists of $[\frac{n}{2}]+1$ equations) is triangular with diagonal coefficients $f_{i,2i}$, $i = [n/2]$, $[n/2]-1$, $\ldots, 1, 0$.

As all the $f_{i,2i}$ are different from zero, we may recursively solve for the a_i, in decreasing order. Although the solutions a_i belong to $\mathbb{F}$, calculations must be performed in the larger field L. To conclude, calculating the polynomial $P_{\phi,L}(X)$ requires:

- the determination of $\epsilon(\phi) \in \mathbb{F}$, which is achieved by (2.11);

- the determination of the coefficients $p_i \in \mathbb{F}$ of $\mathfrak{p}^m(T)$ (which are independent of ϕ);
- the determination of the $f_{i,j} \in L$ (which do depend on ϕ);
- the solution of a triangular system of $[n/2]+1$ linear equations over L, where $n = d \cdot m = [L : \mathbb{F}]$.

(3.4) In what follows, we describe a much simpler procedure, which however only works if ϕ is defined over the "prime field" $\mathbb{F}_{\mathfrak{p}}$.

Let ϕ be a Drinfeld module over L, of A-characteristic $\mathfrak{p}$, and write

$$\phi_{\mathfrak{p}} = \sum_{0 \le i \le 2d} h_i(\phi)\tau^i.$$

then h_i vanishes for $i < d$ (as can be seen e.g. from (1.9)). The *Hasse invariant* $H(\phi) := h_d(\phi)$ of ϕ satisfies

$$\gamma(a) = \epsilon(\phi) N^L_{\mathbb{F}_{\mathfrak{p}}}(H(\phi)), \tag{3.5}$$

see [6] Lemma 5.2. As a consequence, the Frobenius trace a of ϕ is fully determined through $H(\phi)$ if $L = \mathbb{F}_{\mathfrak{p}}$, since then deg $a \le n/2 = d/2$, and a is determined by its residue class $\gamma(a)$ modulo $\mathfrak{p}$. On the other hand, the Hasse invariant satisfies the "Deligne congruence"

$$H(\phi) \equiv g_d(\phi) \pmod{\mathfrak{p}}, \tag{3.6}$$

where $g_k(\phi)$ is the value of the normalized Eisenstein series of weight $q^k - 1$ on ϕ (see [8] sect. 12 for details). Given the known recursion for the g_k (*loc. cit.* (6.9)), we get the following simple procedure.

3.7 Proposition. *Let $\phi = (g, \Delta)$ be a Drinfeld module over $\mathbb{F}_{\mathfrak{p}}$. For $k \in \mathbb{N}$, put $[k] := T^{q^k} - T$, regarded as an element of $\mathbb{F}_{\mathfrak{p}}$, and define $g_0 = 1$, $g_1 = g$,*

$$g_k = -[k-1] g_{k-2} \Delta^{q^{k-2}} + g_{k-1} g^{q^{k-1}} \quad (k \ge 2).$$

Then the Hasse invariant $H(\phi)$ of ϕ equals g_d, $d = [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}]$. $\square$

Hence the Frobenius trace $a(\phi) \in A$ of $\phi/\mathbb{F}_{\mathfrak{p}}$ is determined through $a \equiv \epsilon_{\mathbb{F}_{\mathfrak{p}}}(\phi) \cdot g_d \pmod{\mathfrak{p}}$ and deg $a \le d/2$.
Note that, apart from the raising to q-th powers (i.e., applying the Frobenius of $\mathbb{F}$), the recursion for the g_k is *linear* and easy to evaluate.

3.8 Example. Let $q = 2$, $\mathfrak{p}(T) = T^3 + T + 1$, and let ϕ be the Drinfeld module over $\mathbb{F}_{\mathfrak{p}}$ given by $(g, \Delta) = (T, 1)$. We regard the quantities T and 1, like those to follow, as elements of $\mathbb{F}_{\mathfrak{p}}$. Then $g_0 = 1$, $g_1 = T$, $g_2 = T^2 + 1$, $g_3 = 0$, thus $P_{\phi, \mathbb{F}_{\mathfrak{p}}}(X) = X^2 + \mathfrak{p}(T)$.

Similarly, we get for $\psi = (g, \Delta) = (T, T)$: $g_0 = 1$, $g_1 = T$, $g_2 = T^2$,

$g_3 = T$, so $P_{\psi,\mathbb{F}_\mathfrak{p}}(X) = X^2 - TX + \mathfrak{p}(T)$.

The fact that $H(\phi)$ vanishes means that ϕ is *supersingular*; this has similar significance as supersingularity of elliptic curves [9].

4. Frobenius traces of maximal size.

We fix a prime $\mathfrak{p}$ of A of degree d and consider Drinfeld modules ϕ over $L = \mathbb{F}_\mathfrak{p}$. For such ϕ, the Frobenius trace $a(\phi) \in A$ has degree $\leq [d/2]$. Put

$$\begin{array}{rcl} D_+(\mathfrak{p}) & = & \{\phi/L \mid \deg\ a(\phi) = [d/2]\} \\ D_-(\mathfrak{p}) & = & \{\phi/L \mid \deg\ a(\phi) < [d/2]\}. \end{array} \tag{4.1}$$

We further let $H_+(\mathfrak{p})$ and $H_-(\mathfrak{p})$ be the set of L-isomorphism classes in $D_+(\mathfrak{p})$, $D_-(\mathfrak{p})$, respectively. That is, $H_+(\mathfrak{p})$ ($H_-(\mathfrak{p})$) is the orbit space of $D_+(\mathfrak{p})$ ($D_-(\mathfrak{p})$) under the action of L^* through $c \cdot (g, \Delta) = (c^{q-1}g, c^{q^2-1}\Delta)$. We finally write $d_\pm(\mathfrak{p})$, $h_\pm(\mathfrak{p})$ for the cardinalities of these sets. The principal result of this section is:

4.2 Theorem.

(i) *Let d be even. Then*

$$\begin{array}{rcl} d_+(\mathfrak{p}) & = & q^{d+1}(\frac{q^d-1}{q+1}) \\ d_-(\mathfrak{p}) & = & q^d(\frac{q^d-1}{q+1}) \\ h_+(\mathfrak{p}) & = & (q^2-q)(\frac{q^d-1}{q+1}+1) \\ h_-(\mathfrak{p}) & = & (q-1)(\frac{q^d-1}{q+1}+1). \end{array}$$

(ii) *For d odd we have*

$$\begin{array}{rcl} d_+(\mathfrak{p}) & = & (q-1)q^{d-1}(q^d-1) \\ d_-(\mathfrak{p}) & = & q^{d-1}(q^d-1) \\ h_+(\mathfrak{p}) & = & (q-1)^2 q^{d-1} \\ h_-(\mathfrak{p}) & = & (q-1)q^{d-1}. \end{array}$$

Before proving the theorem we establish some preparatory results.

4.3 Proposition. *Let $L = \mathbb{F}^{(d)}$ be the field extension of degree d of $\mathbb{F} = \mathbb{F}_q$ and $\chi : L^* \longrightarrow L^*$ a multiplicative character (i.e., some power of the identity map) of order $(q^d-1)/g$, where g is a divisor of $q-1$ coprime with $(q^d-1)/(q-1)$. If V is an $\mathbb{F}$-subspace of L then*

$$\#((V - \{0\}) \cap \mathrm{image}(\chi)) = (q^{\dim(V)} - 1)/g$$

holds.

Proof. (i) Without restriction, we may assume that $\dim(V) = 1$.

(ii) Let $\chi = (x \longmapsto x^k)$. We have $\#\mathrm{image}(\chi) = \mathrm{ord}(\chi) = (q^d - 1)/g$, where $g = \gcd(q^d - 1, k) = \gcd(q - 1, k)$ by our assumption on g.

(iii) Write $q - 1 = a \cdot g$, $k = b \cdot g$ with $(a, b) = 1$. Then $q^d - 1 = \frac{q^d-1}{q-1}ag$ and also $(a\frac{q^d-1}{q-1}, b) = 1$. Hence $(k, \frac{q^d-1}{q-1}) = 1$ as well.

(iv) Consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{F}^* & \longrightarrow & L^* & \longrightarrow & L^*/\mathbb{F}^* & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{F}^* & \longrightarrow & L^* & \longrightarrow & L^*/\mathbb{F}^* & \longrightarrow & 1 \end{array},$$

where vertical arrows are the k-th power maps. From (iii), the right arrow is bijective, so

$$(*) \qquad \mathbb{F}^*/(\mathbb{F}^*)^k \xrightarrow{\cong} L^*/(L^*)^k$$

by the snake lemma. Both groups have order g.

(v) Let now the class of $v \in L^*$ under $(*)$ be represented by $v_0 \in \mathbb{F}^*$. There are precisely $(q - 1)/g$ elements c of $\mathbb{F}^*$ with $cv_0 \in (\mathbb{F}^*)^k$, and these are also the elements c of $\mathbb{F}^*$ with $cv \in (L^*)^k = \mathrm{image}(\chi)$. □

4.4 Corollary: *With notation and assumptions as in* (4.3)*, and putting* $\chi(0) = 0$*,*

$$\#\{x \in L \mid \mathrm{Tr}^L_{\mathbb{F}}(\chi(x)) = 0\} = q^{d-1}.$$

Proof. Let H be the kernel of $\mathrm{Tr}^L_{\mathbb{F}}$. Then

$$H \cap \mathrm{image}(\chi) = \{0\} \cup \{0 \neq x \in H \mid \exists\, y \in L \text{ s.t. } x = \chi(y)\}.$$

By (4.3),

$$\#((H - \{0\}) \cap \mathrm{image}(\chi)) = (q^{d-1} - 1)/g,$$

and for each x in that set there are precisely g solutions y of $x = \chi(y)$, which yields the result. □

4.5 Corollary. *Let d be odd. Then*

$$\#\{x \in L \mid \mathrm{Tr}^L_{\mathbb{F}}(x^{(q^d-q)/(q^2-1)+1}) = 0\} = q^{d-1}.$$

Proof. An elementary calculation yields

$$g := \gcd((q^d - 1), \tfrac{q^d-q}{q^2-1} + 1) = \gcd(\tfrac{d+1}{2}, q - 1),$$

i.e., a divisor of $q-1$. Let ℓ be a divisor of $\gcd(g, \frac{q^d-1}{q-1}) = \gcd(\frac{d+1}{2}, q - 1, \frac{q^d-1}{q-1})$. Modulo ℓ, the following congruences hold:

$q \equiv 1$, thus $0 \equiv \frac{q^d-1}{q-1} = 1 + q + \cdots + q^{d-1} \equiv d$ and $d+1 \equiv 0$. Therefore $\ell = 1$, and the assertion follows from (4.4). $\square$

Proof of Theorem 4.2. Let d be *even* and $\phi = (g, \Delta)$ a Drinfeld module over L. With notation as in sections 2 and 3,

$$\begin{aligned} \phi \in D_-(\mathfrak{p}) &\Leftrightarrow \mathrm{Tr}_{\mathbb{F}}^{\mathbb{F}^{(2)}}(\Delta^{-(q^d-1)/(q^2-1)}) = 0 \quad \text{(see (2.14))} \\ &\Leftrightarrow (\Delta^{-(q^d-1)/(q^2-1)})^{q-1} = -1 \quad \text{(since } \Delta \neq 0) \\ &\Leftrightarrow \Delta^{(q^d-1)/(q+1)} = -1. \end{aligned}$$

That condition is fulfilled for $\frac{q^d-1}{q+1}$ of the $q^d - 1$ elements Δ of L^*. Together with the q^d possible values of g, we get the asserted values of $d_\pm(\mathfrak{p})$.

Let now d be *odd*. For $\phi = (g, \Delta)$ and $g = 0$, we have $a(\phi) = 0$ by (2.14), so $\phi \in D_-(\mathfrak{p})$. If $g \neq 0$ then

$$a_{[d/2]} = a_{(d-1)/2} = -g^{-(q^d-1)/(q-1)}\mathrm{Tr}_{\mathbb{F}}^{L}(j^{(q^d-q)/(q^2-1)+1}),$$

where $j = j(\phi)$. Hence

$$\phi \in D_-(\mathfrak{p}) \Leftrightarrow \mathrm{Tr}_{\mathbb{F}}^{L}(j^{(q^d-q)/(q^2-1)+1}) = 0,$$

which by (4.5) holds for precisely q^{d-1} values of j (including $j = 0$). Since for each j there are $q^d - 1$ pairs (g, Δ) with $j = g^{q+1}/\Delta$, we find the stated values of $d_\pm(\mathfrak{p})$.

It remains to show the formulas for $h_\pm(\mathfrak{p})$. The isomorphism class of $\phi = (g, \Delta)$ contains $(q^d - 1)/\#\mathrm{Aut}_L(\phi)$ elements, where $\#\mathrm{Aut}_L(\phi) = q - 1$ except for (d even and $j = 0$), in which case $\#\mathrm{Aut}_L(\phi) = q^2 - 1$ (see (1.5)). The result now follows by counting. $\square$

4.6 Remark. By the theorem, the ratios $d_+(\mathfrak{p})/d_-(\mathfrak{p}) = h_+(\mathfrak{p})/h_-(\mathfrak{p})$ equal q in the even and $q - 1$ in the odd degree case, respectively. For d odd, this is the ratio expected from an equidistribution hypothesis, whereas for even d, large Frobenius traces $a(\phi)$ occur with higher frequency than expected from equidistribution. There are other deviations from a naive equidistribution expectance for the pairs $(a, b) = (a(\phi), \epsilon(\phi)\mathfrak{p}(T))$ appearing as coefficients of $P_{\phi,\mathbb{F}_\mathfrak{p}}(X)$. Since $\mathrm{End}_L(\phi) \otimes K_\infty$ is a division algebra, $P_{\phi,\mathbb{F}_\mathfrak{p}}(X)$ must be irreducible over K_∞. E.g., for $d = \deg\ \mathfrak{p}$ even, we find the restriction that the polynomial $X^2 - a_{d/2}X + \epsilon(\phi)$ cannot have two different roots in $\mathbb{F}$.

5. Primes of small degree.

We show that the number of Drinfeld modules (resp. of isomorphism classes of Drinfeld modules) over $L = \mathbb{F}_{\mathfrak{p}}$ with a fixed Froebenius trace a depends only on deg a and $d =$ deg $\mathfrak{p}$ if d is less or equal to 3.

Let for the moment $d(a, \mathfrak{p})$ (resp. $h(a, \mathfrak{p})$) be the number of $\phi = (g, \Delta)$ (resp. of isomorphism classes of ϕ) over $\mathbb{F}_{\mathfrak{p}}$ with trace a. We see from (2.2) that

$$d(ca, \mathfrak{p}) = d(a, \mathfrak{p}) \text{ and } h(ca, \mathfrak{p}) = h(a, \mathfrak{p}) \tag{5.1}$$

for $c \in \mathbb{F}^*$.

5.2 Theorem. *For $d \le 3$, the numbers $d(a, \mathfrak{p})$ and $h(a, \mathfrak{p})$ depend only on* deg a *and $d =$* deg $\mathfrak{p}$. *They are given by the table:*

a	$d=1$		$d=2$		$d=3$	
0	$q-1$	$q-1$	q^2-1	$q-1$	$(q^3-1)(q+1)$	q^2-1
$a \in \mathbb{F}^*$	$q-1$	$q-1$	q^2-q-1	$q-1$	$q^4-(q+1)^2$	q^2-q-1
deg $a = 1$	0	0	q^2	q	q^4-q	$q(q-1)$

(The first entry is $d(a, \mathfrak{p})$, the second $h(a, \mathfrak{p})$.)

Proof. We first determine $d(a, \mathfrak{p})$. We have $a(\phi) = 0$ if and only if ϕ is supersingular. It is known ([6] Satz 5.9) that for $d = 1, 2, 3$ there are precisely $1, 1, q+1$ supersingular j-invariants in A-characteristic $\mathfrak{p}$, and all of them lie in the prime field $\mathbb{F}_{\mathfrak{p}}$ ([7] Korollar 5.5). Since each of them gives rise to $q^d - 1$ different modules $\phi = (g, \Delta)$, the line "$a = 0$" results. (Here we used that $\mathrm{Aut}_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ always equals $\mathbb{F}^*$ since $j = 0$ is not supersingular if $d = 2$.) The line "$a \in \mathbb{F}^*$" follows from (5.1) and (4.2). Thus it remains to verify the entries $d(a, \mathfrak{p})$ for deg $a = 1$, which is trivial for $d = 1$.

In what follows, we use Proposition 3.7 and the notation introduced there. Further, since the Frobenius trace $a(\phi) \in A$ is determined through its class (mod $\mathfrak{p}$), we regard it as an element of $\mathbb{F}_{\mathfrak{p}}$. Then (3.7) combined with (2.11) gives the following values for $a(\phi) = a(g, \Delta)$:

$$\begin{aligned} d = 2: \quad a(g, \Delta) &= \tfrac{-[1]\Delta + g^{q+1}}{\Delta^{q+1}}; \\ d = 3: \quad a(g, \Delta) &= \tfrac{-[2]g\Delta^q - [1]g^{q^2}\Delta + g^{q^2+q+1}}{\Delta^{q^2+q+1}}. \end{aligned}$$

Let $\boxed{d = 2}$. We have to show that for each $u \in \mathbb{F}_{\mathfrak{p}} - \mathbb{F}$ there are precisely q^2 solutions $(g, \Delta) \in \mathbb{F}_{\mathfrak{p}} \times \mathbb{F}_{\mathfrak{p}}^*$ of

$$a(g, \Delta) = u. \tag{1}$$

Let $u \in \mathbb{F}_{\mathfrak{p}} - \mathbb{F}$ be given. Since $[1] \neq 0$ in $\mathbb{F}_{\mathfrak{p}}$, there exists a unique $\Delta \in \mathbb{F}_{\mathfrak{p}}$ such that $u = a(0, \Delta) = -[1]\Delta^{-q}$, viz., $\Delta = (-[1]u^{-1})^q = [1]u^{-q}$.

Similarly, for each fixed value $r \in \mathbb{F}_{\mathfrak{p}}^*$ of g/Δ, $r^{q+1} = (g/\Delta)^{q+1} \in \mathbb{F}^*$, and the equation $a(g,\Delta) = u$ is equivalent with

$$[1]/(r^{q+1} - u) = \Delta^q,$$

which has a unique solution Δ. This gives another $q^2 - 1$ solutions of equation (1), one for each $r = g/\Delta \in \mathbb{F}_{\mathfrak{p}}^*$.

(2) Note that among our q^2 solutions $\phi = (g,\Delta)$ of (1), there is precisely one that satisfies $j(\phi) = 0$.

Now consider the case $\boxed{d = 3}$. Let $N : \mathbb{F}_{\mathfrak{p}} \longrightarrow \mathbb{F}$ denote the norm map. The following facts are immediate:

(3) $a(cg, c^{q+1}\Delta) = N(c)^{-1}a(g,\Delta)$ if $c \in \mathbb{F}_{\mathfrak{p}}^*$, thus

$$a(g,\Delta) = N(g)^{-1}a(1, \tfrac{\Delta}{g^{q+1}}) \text{ if } g \neq 0;$$

(4) the polynomial $[2]X^q + [1]X \in \mathbb{F}[X]$ is q-additive with kernel $U := \mathbb{F}[2]$ and range $V := \mathbb{F} + \mathbb{F}T \hookrightarrow \mathbb{F}_{\mathfrak{p}}$ on $\mathbb{F}_{\mathfrak{p}}$.
(The fastest way to see the last assertion is to compare with the formula for $a(g,\Delta)$, which *a priori* belongs to V.)

Hence, putting $f(X) = 1 - [1]X - [2]X^q$, the equation $f(x) = u$ has precisely q solutions x if $u \in V$, which are all non-zero if $u \notin \mathbb{F}$. Given $u \in V - \mathbb{F}$, the equation

$$a(g,\Delta) = u \tag{1}$$

can hold only for $g \neq 0$, and is in view of (3) and (4) equivalent with $u = N(g)^{-1}a(1, \frac{\Delta}{g^{q+1}}) = N(g^{-1})f(\frac{\Delta}{g^{q+1}})N(\frac{g^{q+1}}{\Delta})$, i.e., with

$$f(\tfrac{\Delta}{g^{q+1}}) = N(\tfrac{\Delta}{g})u.$$

Therefore, we find precisely $q^4 - q = (q^3 - 1)q$ solutions (g,Δ) of (1), which may be enumerated as follows: Choose $y := \frac{\Delta}{g}$ arbitrary in $\mathbb{F}_{\mathfrak{p}}^*$ ($q^3 - 1$ choices), and let x run through the q solutions of $f(x) = N(y)u$. From $y = \frac{\Delta}{g}$ and $x = \frac{\Delta}{g^{q+1}}$ we find the corresponding solutions $g(y/x)^{q^2}$, $\Delta = (y/x)^{q^2} \cdot y$. This completes the calculation of $d(a,\mathfrak{p})$ as stated in the table.

The $h(a,\mathfrak{p})$ are immediate for $d = 1$ and $d = 3$, since then all the isomorphism classes have length $(q^d - 1)/(q - 1)$, and so $h(a,\mathfrak{p}) = d(a,\mathfrak{p})/\frac{q^d-1}{q-1}$. For $d = 2$ all the isomorphism classes have length $(q^d - 1)/(q - 1) = q + 1$ except for $q^2 - 1$ classes of length one, and the result follows from counting and the remark (2). $\square$

5.3 Remark. The assertion of Theorem 5.2 becomes definitely wrong if applied to prime A-fields $\mathbb{F}_{\mathfrak{p}}$ of degree > 3. For example, let $q = 2$ and $\mathfrak{p} = (T^4 + T^3 + 1)$. The numbers $d(a, \mathfrak{p})$ and $h(a, \mathfrak{p})$ are given by the table below. It shows that $d(a, \mathfrak{p})$ and $h(a, \mathfrak{p})$ differ even on the two elements $a = T, T + 1$ of degree one.

5.4 Example. $q = 2$, $\mathfrak{p} = (T^4 + T^3 + 1)$

a	$d(a, \mathfrak{p})$	$h(a, \mathfrak{p})$
0	45	3
1	15	1
T	0	0
$T+1$	20	2
T^2	50	4
T^2+1	30	2
T^2+T	60	4
T^2+T+1	20	2

6. Class number formulas.

(6.1) Let $H(a, b, \mathfrak{p}) = H(a, b, \mathbb{F}_{\mathfrak{p}})$ be the set of isomorphism classes of rank-two Drinfeld modules over $\mathbb{F}_{\mathfrak{p}}$ with characteristic polynomial $P(X) = X^2 - aX + b$. We relate its cardinality $h(a, b, \mathfrak{p})$ and the weighted number

$$h^*(a, b, \mathfrak{p}) = \sum_{\phi \in H(a,b,\mathfrak{p})} w^{-1}(\phi),$$

where $w(\phi) = (q-1)^{-1} \# \mathrm{Aut}_{\mathbb{F}_{\mathfrak{p}}}(\phi)$, with class numbers of "imaginary quadratic orders" over A and express them through the analytic class number formula.

(6.2) A quadratic field extension E of K is *imaginary quadratic* if the place ∞ of K doesn't split in E, in which case it has a unique extension, also labelled by ∞, to E. Put B for the integral closure of A in E. An *order* in B or E is a subring C of B containing A and free of rank two over A. It necessarily has the form

$$C = B_f = A + fB$$

with some monic $f \in A$, the *index* of C in B. We have $B_f \subset B_{f'} \Leftrightarrow f'|f$. A finitely generated C-submodule $\mathfrak{c} \neq 0$ of $E = \mathrm{quot}(B) = \mathrm{quot}(C)$ is a *fractional ideal* ("ideal" for short) of C, and is *proper* if its multiplier ring $M(\mathfrak{c}) = \{x \in B \mid x\mathfrak{c} \subset \mathfrak{c}\}$ agrees with C. Two ideals $\mathfrak{c}$, $\mathfrak{c}'$

are *equivalent* iff they are related by $\mathfrak{c}' = g \cdot \mathfrak{c}$ with some $g \in E^*$. We let $H(C)$ be the set of equivalence classes of (not necessarily proper) ideals of C, and $h(C)$ its (finite) cardinality. As with Dedekind rings, the set of proper fractional ideals of C forms a group under multiplication. The order $h_{\mathrm{prop}}(C)$ of the associated ideal class group is related to $h(B) = h_{\mathrm{prop}}(B)$ by

$$h_{\mathrm{prop}}(C) = \frac{|f|}{[B^* : C^*]} \prod_{\mathfrak{p}|f} (1 - \chi_E(\mathfrak{p})|\mathfrak{p}|^{-1}) h(B), \tag{6.3}$$

where $C = B_f$, $\mathfrak{p}$ runs through the prime divisors of f, "$|\ .\ |$" is the absolute value $q^{\deg(\cdot)}$, and χ_E is the Dirichlet character associated with E. That is, for primes $\mathfrak{p}$ of K (i.e., $\mathfrak{p}$ is a prime of A, or $\mathfrak{p} = \infty$ is the prime at infinity),

$$\chi_E(\mathfrak{p}) = \left\{ \begin{array}{c} 1 \\ 0 \\ -1 \end{array} \right\} \text{ if } \mathfrak{p} \text{ is } \left\{ \begin{array}{l} \text{split} \\ \text{ramified} \\ \text{inert} \end{array} \right\} \text{ in } E. \tag{6.4}$$

We point out the following special cases:

(E_1) if $E = \mathbb{F}_{q^2}(T)$, then $B = \mathbb{F}_{q^2}[T]$ and

$$\chi_E(\mathfrak{p}) = (-1)^{\deg\ \mathfrak{p}};$$

(E_2) if $\mathrm{char}(\mathbb{F}) = 2$ and $E = \mathbb{F}(\sqrt{T})$, then

$$B = \mathbb{F}[\sqrt{T}] \text{ and } \chi_E(\mathfrak{p}) = 0 \text{ for each } \mathfrak{p}.$$

The proofs of the above statements are essentially identical to those in the number field case ([18] sect. 4.4); in the two exceptional cases (E_1) and (E_2), (6.3) is easily proved directly. The unit group C^* has order $q - 1$ except for $C = \mathbb{F}_{q^2}[T]$, which has a unit group of order $q^2 - 1$. Putting

$$w(C) = (q-1)^{-1} \# C^* \text{ and } h^*_{\mathrm{prop}}(C) = w(C)^{-1} h_{\mathrm{prop}}(C),$$

we have

$$h^*_{\mathrm{prop}}(C) = |f| \prod_{\mathfrak{p}|f} (1 - \chi_E(\mathfrak{p})|\mathfrak{p}|^{-1}) h^*_{\mathrm{prop}}(B). \tag{6.5}$$

Since ideals for orders C' containing C are also ideals for C and each ideal $\mathfrak{c}$ of C has some $C' \supset C$ as its multiplier ring, we get for $C = B_f$:

$$h(C) = h(B_f) = \sum_{f'|f} h_{\mathrm{prop}}(B_{f'}), \tag{6.6}$$

which we call the *unweighted Gauß class number* of C. Counting each ideal $\mathfrak{c}$ of C with w^{-1}, where $w = w(M(\mathfrak{c}))$, we get the *weighted Gauß class number*

$$h^*(C) = \sum_{f'|f} h^*_{\mathrm{prop}}(B_{f'}). \tag{6.7}$$

Let now ϕ be a rank-two Drinfeld module over $\mathbb{F}_\mathfrak{p}$, with characteristic polynomial $P(X) = X^2 - aX + b$. Consider the A-algebra C generated by the Frobenius endomorphism F of ϕ over $\mathbb{F}_\mathfrak{p}$. Since F is a zero of P, (1.8) shows that C is an order in the imaginary quadratic extension $E = \mathrm{quot}(C)$ of K. Let B be the maximal order of E and $C = B_f$ as above.

6.8 Proposition *(see* [19], *Corollary to Prop. 7). The number $h(a, b, \mathfrak{p})$ of isomorphism classes of rank-two Drinfeld modules over $\mathbb{F}_\mathfrak{p}$ with characteristic polynomial $P(X) = X^2 - aX + b$ equals the Gauß class number $h(C)$ of $C = A[F]$, where F is a zero of $P(X)$. Similarly, the weighted number $h^*(a, b, \mathfrak{p})$ equals $h^*(C)$.* □

This is analogous with a similar statement, due to Deuring [3], for elliptic curves over $\mathbb{F}_\mathfrak{p}$. Its proof uses the fact that Drinfeld modules ϕ and ϕ' are isogeneous if and only if their characteristic polynomials agree, i.e., Theorem 1.10, and then constructs an explicit bijection of the class set $H(C)$ with $H(a, b, \mathfrak{p})$ compatible with respective weights. The assumption of characteristic different from 2 made in [19] p. 168 is irrelevant for the proposition as given above, and may be suppressed.

Fix $\mathfrak{p}$, a and b as before, let C be the A-algebra generated by a root of $P(X) = X^2 - aX + b$, with $C = B_f$, where B is the maximal order in $E = \mathrm{quot}(C)$, and let $\chi = \chi_E$ be the Dirichlet character corresponding to E (see (6.4)). From (6.5), (6.7) and (6.8) we get

$$h^*(a, b, \mathfrak{p}) = S(f, B)h^*(B) \tag{6.9}$$

with

$$S(f, B) := \sum_{f'|f} |f'| \prod_{\substack{\mathfrak{l} \text{ prime of } A \\ \mathfrak{l}|f'}} (1 - \chi(\mathfrak{l})|\mathfrak{l}|^{-1}). \tag{6.10}$$

The quantity $S(f, B)$ also satisfies (see [11], Lemmata 5.1 + 5.2):

6.11 Proposition.

(i) *If f, f' are coprime then $S(ff', B) = S(f, B)S(f', B)$.*
(ii) *If $f = \mathfrak{l}^m$ is a power of a prime $\mathfrak{l}$ then*

$$S(f, B) = 1 + (|\mathfrak{l}| - \chi(\mathfrak{l}))(|\mathfrak{l}|^m - 1)(|\mathfrak{l}| - 1)^{-1}. \quad \square$$

(Recall that we use "$\mathfrak{l}$" both for a prime ideal and for its monic generator.)

Exclude for the moment the two exceptional cases (E_1) and (E_2). Then the genus of E (i.e., of the associated algebraic curve) is given by

$$g = g(E) = \frac{1}{2}\deg\ \mathrm{cond}(\chi) - 1, \tag{6.12}$$

where $\mathrm{cond}(\chi)$ is the conductor of χ. Further, putting $\eta = \eta(E/K) = 2$ (resp. 1) if ∞ is inert (resp. ramified) in E/K, the analytic class number formula reads

$$h^*(B) = h(B) = \eta q^g L(1, \chi). \tag{6.13}$$

Here $L(s, \chi)$ is the L-function defined for $\mathrm{Re}(s) > 1$ by the absolutely convergent product

$$L(s, \chi) = \prod_{\mathfrak{l} \text{ prime of } K} (1 - \chi(\mathfrak{l})|\mathfrak{l}|^{-s})^{-1}. \tag{6.14}$$

Formulas (6.12) and (6.13) are well-known consequences of properties of the respective zeta functions of K and E (see e.g. [16]). Note that the product (6.14) for $s = 1$ still converges conditionally (in an order compatible with the degree of primes) towards $L(1, \chi)$.

Now consider the exceptional case (E_1), $B = \mathbb{F}_{q^2}[T]$. We formally put $g = g(E/\mathbb{F}_q) := -1$. Then

$$L(s, \chi) = ((1 + q^{-s})(1 + q^{1-s}))^{-1}$$

and

$$h^*(B) = (q + 1)^{-1} = \eta q^g L(1, \chi). \tag{6.15}$$

Finally, in case (E_2) we have $g = 0$, $h(B) = 1$, and

$$h^*(B) = h(B) = \eta q^g L(1, \chi). \tag{6.16}$$

holds trivially. Combining (6.13)–(6.16) with (6.9), we find the expression

$$h^*(a, b, \mathfrak{p}) = \eta q^g S(f, B) L(1, \chi), \tag{6.17}$$

which is valid in all cases. We point out that all the ingredients of the right hand side are determined by a and b.

For later use, we write this formula as a product of $\mathfrak{l}$-local terms, where $\mathfrak{l}$ runs through the places of K. Namely, let $L_{\mathfrak{l}}(s, \chi) = (1 - \chi(\mathfrak{l})|\mathfrak{l}|^{-s})^{-1}$ be the $\mathfrak{l}$-th factor in (6.14), and for $\mathfrak{l}$ finite,

$$V_{\mathfrak{l}}(a, b) := S(\mathfrak{l}^{m_{\mathfrak{l}}(f)}, B) L_{\mathfrak{l}}(1, \chi), \tag{6.18}$$

where $f = \prod_{\mathfrak{l}} \mathfrak{l}^{m_{\mathfrak{l}}(f)}$. Due to (6.11), (6.17) reads

$$h^*(a,b,\mathfrak{p}) = \eta q^g L_\infty(1,\chi) \prod_{\mathfrak{l} \text{ prime of } A} V_{\mathfrak{l}}(a,b). \tag{6.19}$$

Note that the infinite product up to a finite number of factors agrees with $L(1,\chi)$ and is therefore conditionally convergent too.

7. The local density.

We now want to give a local analytic interpretation of the factors $V_{\mathfrak{l}}(a,b)$ in (6.18). In the whole section, $\mathfrak{l}$ is a fixed prime of A, of absolute value $|\mathfrak{l}| = q^{\deg \mathfrak{l}}$, a and b are elements of the $\mathfrak{l}$-adic completion $A_{\mathfrak{l}}$ of A, and $P(X) = X^2 - aX + b \in A_{\mathfrak{l}}[X]$.

We define
(7.1)

$$v_{\mathfrak{l}}(a,b) := \lim_{k\to\infty} \frac{\#\{M \in \mathrm{Mat}(2, A/\mathfrak{l}^k) \mid \mathrm{tr}(M) = a,\ \det(M) = b\}}{|\mathfrak{l}|^{2k-2}(|\mathfrak{l}|^2 - 1)},$$

provided the limit exists. Here and in what follows, we use simplifying notation and write e.g. $\mathrm{tr}(M) = a$ for $\mathrm{tr}(M) \equiv a(\bmod\ \mathfrak{l}^k)$. It will turn out that the following properties hold:

(7.2) The limit in (7.1) exists; in fact, it is attained for all $k \geq k_0(a,b)$ provided that $P(X)$ is not a square in $A_{\mathfrak{l}}[X]$;

(7.3) $v_{\mathfrak{l}}(a,b)$ defines a continuous function on the compact group $A_{\mathfrak{l}} \times A_{\mathfrak{l}}$, which averages to 1 on $A_{\mathfrak{l}} \times A_{\mathfrak{l}}^*$;

(7.4) if $P(X)$ is a possible characteristic polynomial for $\phi \in H(a,b,\mathfrak{p})$ as in section 6, then $v_{\mathfrak{l}}(a,b)$ essentially agrees with $V_{\mathfrak{l}}(a,b)$ (see Proposition 8.3 for the precise statement).

Intuitively, $v_{\mathfrak{l}}(a,b)$ quantifies the frequency of characteristic polynomials of 2×2-matrices over $A_{\mathfrak{l}}$. In other words, letting μ and ν be the normalized Haar measures on $\mathrm{Mat}(2, A_{\mathfrak{l}})$ and $A_{\mathfrak{l}} \times A_{\mathfrak{l}}$, respectively, and

$$\begin{array}{rrcl} TD: & \mathrm{Mat}(2, A_{\mathfrak{l}}) & \longrightarrow & A_{\mathfrak{l}} \times A_{\mathfrak{l}} \\ & M & \longmapsto & (\mathrm{tr}(M), \det(M)) \end{array}$$

the trace-determined map, then

$$(TD_*\mu)(a,b) = c_{\mathfrak{l}} v_{\mathfrak{l}}(a,b) \nu(a,b) \tag{7.5}$$

with some constant $c_{\mathfrak{l}} > 0$.

Before studying $v_{\mathfrak{l}}(a,b)$, we make some definitions.

(7.6) The *Kronecker symbol* is

$$(\frac{a,b}{\mathfrak{l}}) := 1, 0, -1$$

if the reduced polynomial $\overline{P}(X) = X^2 - \overline{a}X + \overline{b} \in \mathbb{F}_{\mathfrak{l}}[X]$ has 2, 1, 0 different roots in $\mathbb{F}_{\mathfrak{l}}$, respectively. Thus if char($\mathbb{F}$) is different from 2 and $D = D(a,b) = a^2 - 4b$ is the discriminant of P, then

$$(\frac{a,b}{\mathfrak{l}}) = (\frac{D}{\mathfrak{l}}) = (\frac{D}{\mathbb{F}_{\mathfrak{l}}}) = \text{quadratic symbol.}$$

(7.7) We define a number $\delta = \delta(a,b) \in \mathbb{N}_0 \cup \{\infty\}$ and a symbol $\chi_{a,b}(\mathfrak{l}) \in \{0, \pm 1\}$, distinguishing the cases:

<u>char($\mathbb{F}$) $\neq 2$:</u> Here we put

$$\begin{aligned} \delta(a,b) &:= \sup\{i \in \mathbb{N}_0 \mid \mathfrak{l}^{2i} \text{ divides } D(a,b)\}, \\ \chi_{a,b}(\mathfrak{l}) &= (\tfrac{D(a,b)/\mathfrak{l}^{2\delta}}{\mathbb{F}_{\mathfrak{l}}}) \text{ if } \delta < \infty \text{ and } \chi_{a,b}(\mathfrak{l}) = 0 \text{ otherwise.} \end{aligned}$$

<u>char($\mathbb{F}$) $= 2$:</u> Given $(a,b) \in A_{\mathfrak{l}} \times A_{\mathfrak{l}}$, let $s \in \mathbb{F}_{\mathfrak{l}}$ be the unique solution of $s^2 \equiv b(\bmod\ \mathfrak{l})$ and $b' := s^2 + as + b$. (Here we regard s as an element of $A_{\mathfrak{l}}$. Instead of $\mathbb{F}_{\mathfrak{l}} \hookrightarrow A_{\mathfrak{l}}$, we could use another system of representatives for $A_{\mathfrak{l}}/\mathfrak{l}A_{\mathfrak{l}}$: see Remark 7.11.) If

$$(*) \qquad a \equiv 0(\bmod\ \mathfrak{l}) \text{ and } b' \equiv 0(\bmod\ \mathfrak{l}^2)$$

holds, put $(a_1, b_1) = (a/\mathfrak{l}, b'/\mathfrak{l}^2)$. Define a series of pairs $(a_i, b_i) \in A_{\mathfrak{l}} \times A_{\mathfrak{l}}$ by

$$(a_0, b_0) := (a,b),\ (a_{i+1}, b_{i+1}) := ((a_i)_1, (b_i)_1)$$

as long as $(*)$ holds for (a_i, b_i). Finally, we put

$$\begin{aligned} \delta(a,b) &:= \sup\{i \in \mathbb{N}_0 \mid (a_i, b_i) \text{ is defined}\}, \\ \chi_{a,b}(\mathfrak{l}) &= (\tfrac{a_\delta, b_\delta}{\mathfrak{l}}) \text{ if } \delta < \infty \text{ and } \chi_{a,b}(\mathfrak{l}) = 0 \text{ otherwise.} \end{aligned}$$

In all characteristics, $\delta = \infty$ if and only if $P(X)$ is a square in $A_{\mathfrak{l}}[X]$, and the function δ is locally constant on $A_{\mathfrak{l}} \times A_{\mathfrak{l}}$ off the locus of $\delta = \infty$.

Now (7.2)–(7.5) will be consequences of the main result of this section:

7.8 Theorem. *Put $\alpha^{(k)}(a,b)$ for the numerator*

$$\#\{M \in \mathrm{Mat}(2, A/\mathfrak{l}^k) \mid \mathrm{tr}(M) = a, \det(M) = b\} \text{ in (7.1).}$$

(a) *Suppose that* $\delta = \delta(a,b) < \infty$ *and* $k \geq 2\delta + 2$. *Then*

$$\alpha^{(k)}(a,b) = |\mathfrak{l}|^{2k} + |\mathfrak{l}|^{2k-1} + \gamma^{(k)}(a,b)$$

with $\gamma^{(k)}(a,b) = 0, -(|\mathfrak{l}|+1)|\mathfrak{l}|^{2k-\delta-2}, -2|\mathfrak{l}|^{2k-\delta-1}$ *according to the values* $1, 0, -1$ *of* $\chi_{a,b}(\mathfrak{l})$.

(b) *Suppose that* $\delta(a,b) = \infty$. *Then*

$$\alpha^{(k)}(a,b) = |\mathfrak{l}|^{2k} - |\mathfrak{l}|^{2k-2} + (|\mathfrak{l}|-1)^2|\mathfrak{l}|^{2k-2}\textstyle\sum_{1\leq i<k/2}(2i-1)|\mathfrak{l}|^{-i}$$
$$+|\mathfrak{l}|^{k-1+[k/2]}((k-1)(|\mathfrak{l}|-1)+1).$$

Before proving the theorem, we draw some easy conclusions.

7.9 Corollary. *The limit in* (7.1) *exists and is given by*

$$v_{\mathfrak{l}}(a,b) = (1-|\mathfrak{l}|^{-2})^{-1}(1+|\mathfrak{l}|^{-1} + \left\{\begin{array}{c} 0 \\ -(|\mathfrak{l}|+1)|\mathfrak{l}|^{-\delta-2} \\ -2|\mathfrak{l}|^{-\delta-1} \end{array}\right\}),$$

with $\delta = \delta(a,b)$ *and according to the values* $1, 0, -1$ *of* $\chi_{a,b}(\mathfrak{l})$. *It defines a continuous function* $v_{\mathfrak{l}}$ *on* $A_{\mathfrak{l}} \times A_{\mathfrak{l}}$, *which is locally constant off the locus of* $\delta = \infty$.

Proof. The assertion is immediate from 7.8(a) and the properties of δ, as long as $\delta < \infty$. For $\delta \longrightarrow \infty$, $v_{\mathfrak{l}}(a,b)$ converges to $(1+|\mathfrak{l}|^{-1})/(1-|\mathfrak{l}|^{-2}) = |\mathfrak{l}|/(|\mathfrak{l}|-1)$. On the other hand, if $\delta = \infty$ then

$$v_{\mathfrak{l}}(a,b) = \lim_{k\to\infty} \frac{\alpha^{(k)}(a,b)}{|\mathfrak{l}|^{2k-2}(|\mathfrak{l}|^2-1)} = \frac{|\mathfrak{l}|}{|\mathfrak{l}|-1},$$

as results from 7.8(b), taking into account that

$$\lim_{k\to\infty} \sum_{1\leq i<k/2} (2i-1)|\mathfrak{l}|^{-i} = \frac{|\mathfrak{l}|+1}{(|\mathfrak{l}|-1)^2}.$$

□

7.10 Corollary. *The function* $v_{\mathfrak{l}}$ *averages to* 1 *on* $A_{\mathfrak{l}} \times A_{\mathfrak{l}}^*$ *and satisfies equation* (7.5) *with* $c_{\mathfrak{l}} = 1 - |\mathfrak{l}|^{-2}$.

Proof. The first assertion follows from the continuity of $v_{\mathfrak{l}}$ and the fact that

$$\begin{aligned} |\mathfrak{l}|^{2k-2}(|\mathfrak{l}|^2-1) &= \#\mathrm{SL}(2, A/\mathfrak{l}^k)/|\mathfrak{l}|^k \\ &= \text{average over all } a \in A/\mathfrak{l}^k, \text{ with} \\ & \ b \in (A/\mathfrak{l}^k)^* \text{ fixed, of } \alpha^{(k)}(a,b). \end{aligned}$$

The second assertion results from $\mathrm{vol}(c_{\mathfrak{l}} \cdot v_{\mathfrak{l}} \cdot \nu) = 1$ and an elementary calculation, which we omit. □

Proof of Theorem 7.8. (a) In [11], sect. 4, the proof of an analoguous statement for the ℓ-adic integers $\mathbb{Z}_\ell$ with a natural prime ℓ instead of $A_\mathfrak{l}$ is given. It applies without essential changes to the case of $A_\mathfrak{l}$ of characteristic different from 2. We therefore assume from now on that $\mathrm{char}(\mathbb{F}) = 2$. To simplify notation, let:
$R_k := A/\mathfrak{l}^k$, $M_k := \mathrm{Mat}(2, R_k)$, $I = I_2 =$ unit 2×2-matrix; for any 2×2-matrix M, $TD(M) = (\mathrm{tr}(M), \det(M))$, and "reduction mod $\mathfrak{l}$" of scalars or matrices will be denoted by a "$\overline{(\ )}$". We consider $\mathbb{F}_\mathfrak{l}$ both as a quotient and a subfield of R_k.

(i) For given $(a, b) \in A_\mathfrak{l} \times A_\mathfrak{l}$ (or $R_k \times R_k$), put

$$\begin{aligned}\beta^{(k)}(a,b) \ &= \ |\mathfrak{l}|^{2k} + |\mathfrak{l}|^{2k-1}, |\mathfrak{l}|^{2k} - |\mathfrak{l}|^{2k-2}, |\mathfrak{l}|^{2k} - |\mathfrak{l}|^{2k-1} \\ &\qquad \text{if } (\tfrac{a,b}{\mathfrak{l}}) = 1, 0, -1, \text{ respectively.}\end{aligned}$$

There are precisely $\beta^{(k)}(a, b)$ matrices $M \in M_k$ such that $TD(M) = (a, b) \in R_k \times R_k$ and $\overline{M} \in M_1$ is non-scalar, and all these M are conjugate in M_k. This is immediate for $k = 1$ (since we then work over a field), and follows by a straightforward induction for general k: *loc. cit.*, Lemma 4.1. In particular we have

$$\alpha^{(1)}(a,b) = |\mathfrak{l}|^2 + (\frac{a,b}{\mathfrak{l}})|\mathfrak{l}|.$$

(ii) From now on, assume $k \geq 2$. We must determine the number of $M \in M_k$ with $\overline{M}$ scalar and $TD(M) = (a, b)$, which can only exist if $\overline{a} = 0$. Then, writing

$$M = sI + M'$$

with $s \in \mathbb{F}_\mathfrak{l} \hookrightarrow R_k$, $\overline{M'} = 0$ and $\mathrm{tr}(M') = a$, we have

$$\det(M') + \mathrm{tr}(M')s + s^2 = b$$

in R_k. Such an s is uniquely determined through $s^2 = \overline{b}$. Given M and s as above, let $b' = \det(M') = s^2 + as + b$, which necessarily satisfies $b' \equiv 0(\mathrm{mod}\ \ \mathfrak{l}^2)$.

(iii) Conversely, suppose that

$$(*) \qquad \begin{gathered}\overline{a} = 0 \text{ (i.e., } a \equiv 0(\mathrm{mod}\ \ \mathfrak{l})\text{) and } b' = s^2 + as + b \equiv 0(\mathrm{mod}\ \ \mathfrak{l}^2), \\ \text{where } s \in \mathbb{F}_\mathfrak{l},\ s^2 = \overline{b}.\end{gathered}$$

The solutions M' as in (ii) correspond bijectively to solutions $N \in M_{k-1}$ of $\mathrm{tr}(N) = \mathfrak{l}^{-1}a$, $\det(N) \equiv \mathfrak{l}^{-2}b'(\ \mathrm{mod}\ \ \mathfrak{l}^{k-2})$. This holds since $N \longmapsto \mathfrak{l}N$ is a bijection from M_{k-1} to $\mathfrak{l}M_k$ and $\det(\mathfrak{l}N) = \mathfrak{l}^2 \det(N)$.

(iv) If thus $(*)$ holds and $(a_1, b_1) = (a/\mathfrak{l}, b'/\mathfrak{l}^2)$ as defined in (7.7),

$$\alpha^{(k)}(a,b) = \beta^{(k)}(a,b) + \sum_{c \in \mathfrak{l}^{k-2}R_{k-1}} \alpha^{(k-1)}(a_1, b_1 + c).$$

(The summation is over a system of representatives c of $\mathfrak{l}^{k-2}A_{\mathfrak{l}}$ modulo $\mathfrak{l}^{k-1}A_{\mathfrak{l}}$.) Otherwise (if $(*)$ fails), $\alpha^{(k)}(a,b) = \beta^{(k)}(a,b)$.

(v) Now we prove the assertion by induction on $\delta = \delta(a,b)$. Note that $\delta(a,b) = \delta(a, b+c)$ for $c \equiv 0 (\mathrm{mod}\ \mathfrak{l}^{2\delta+2})$. If $\delta = 0$ then $\alpha^{(k)}(a,b) = \beta^{(k)}(a,b)$, and the formula results from (i). Thus let $\delta = \delta(a,b) > 0$. Then $\delta(a_1,b_1) = \delta - 1$. In view of $k \geq 2\delta+2$, we have $k-2 \geq 2(\delta-1)+2$ and hence $\delta(a_1, b_1+c) = \delta(a_1,b_1) = \delta - 1$ for each $c \in \mathfrak{l}^{k-2}R_{k-1}$. The induction hypothesis applies to the $\alpha^{(k-1)}(a_1, b_1+c)$ in (iv), which all have the same value $\alpha^{(k-1)}(a_1,b_1)$. Plugging in, the result follows.

(b) Here we allow all characteristics, but use the same notation as introduced in the proof of (a).

(i) We have $\delta(a,b) = \infty \Leftrightarrow (a,b) = (2c, c^2)$, some $c \in A_{\mathfrak{l}}$ and $\alpha^{(k)}(2c,c^2) = \alpha^{(k)}(0,0)$, hence we may assume $(a,b) = (0,0)$. We thus have to determine the matrices $M = \left(\begin{smallmatrix} u & v \\ w & -u \end{smallmatrix}\right) \in M_k$ such that $u^2 + vw = 0$.

(ii) There are precisely $|\mathfrak{l}|^{2k-2}(|\mathfrak{l}|^2 - 1)$ such M with $\overline{M} \neq 0$. This is obvious for $k = 1$ and follows for arbitrary k by induction.

(iii) We are now reduced to counting the number of M with $\overline{M} = 0$, i.e., of solutions $u, v, w \in \mathfrak{l}R_k$ of $u^2 + vw = 0$. This is somewhat laborious but elementary, and will be omitted. Suffice it to say that the term $(|\mathfrak{l}|^2 - 1)|\mathfrak{l}|^{2k-2}(2i-1)|\mathfrak{l}|^{-i}$ in the stated formula gives the number of (u,v,w) where u has $\mathfrak{l}$-adic valuation i, and the last term $|\mathfrak{l}|^{k-1+[k/2]}((k-1)(|\mathfrak{l}|-1)+1)$ counts the (u,v,w) where u has valuation larger or equal to $k/2$. □

7.11 Remark. In (7.7), case char$(\mathbb{F}) = 2$, definition of the series (a_i, b_i) and of $\delta(a,b)$, we use $\mathbb{F}_{\mathfrak{l}} \hookrightarrow A_{\mathfrak{l}}$ as a system of representatives S for $A_{\mathfrak{l}}/\mathfrak{l}A_{\mathfrak{l}}$. (We did so in selecting the unique solution $s \in \mathbb{F}_{\mathfrak{l}}$ of $s^2 \equiv b (\mathrm{mod}\ \mathfrak{l})$.)

It is an easy consequence of the properties of the Kronecker symbol (and also results from the proof of (7.8)(a)) that neither $\delta = \delta(a,b)$ nor the value $\chi_{a,b}(\mathfrak{l}) = (\frac{a_\delta, b_\delta}{\mathfrak{l}})$ depends on that choice, although the arising (a_i, b_i) change if another system of representatives S is used.

8. The class number formula: final version.

We come back to the situation of section 6 and describe the ingredients of formula (6.19), notably, the factors $V_{\mathfrak{l}}(a,b)$, the character χ, and the genus g, which are all determined by a and b. Thus let $\mathfrak{p}$ and $\mathfrak{l}$ be primes of A ($\mathfrak{p}=\mathfrak{l}$ allowed), $d = \deg\ \mathfrak{p}$, and let $P(X) = X^2 - aX + b$ be a possible characteristic polynomial for some Drinfeld module ϕ over $\mathbb{F}_{\mathfrak{p}}$. That is: $a, b \in A$, $(b) = \mathfrak{p}$, and P generates an imaginary quadratic extension E of K (which in particular implies $2\ \deg\ a \leq d$). Further, we let B be the maximal A-order in E and $C = B_f$ the ring extension of A generated by (the zeroes of) P. Recall this means that $C = A + fB$ with $f \in A$ monic.

8.1 Proposition.

(i) *The exponent* $m = m_{\mathfrak{l}}(f)$ *agrees with* $\delta = \delta_{\mathfrak{l}}(a,b)$ *as defined in* (7.7).

(ii) *Let* χ *be the Dirichlet character* χ_E *associated to* E *(see* (6.4)*). Then* $\chi(\mathfrak{l}) = \chi_{a,b}(\mathfrak{l})$ *as in* (7.7).

Proof. Suppose that char($\mathbb{F}$) is odd. Then both m and δ are described as $\max\{i \in \mathbb{N}_0 \mid \mathfrak{l}^{2i}$ divides $a^2 - 4b\}$, so the order $A[\sqrt{D/\mathfrak{l}^{2\delta}}] \supset C$ is $\mathfrak{l}$-maximal, and the result follows.

Thus let char($\mathbb{F}$) $= 2$. According to Remark 7.11, we use $\{a \in A \mid \deg\ a < \deg\ \mathfrak{l}\}$ as a system of representatives for $A_{\mathfrak{l}}/\mathfrak{l}A_{\mathfrak{l}}$ and perform the construction (7.7). This has the advantage that all the (a_i, b_i) that arise belong to A. Then (i) follows by induction on m (or on δ), applying Lemma 8.2 below. Increasing i by one, the index f_i of the order $C_i = B_{f_i}$ generated by the zeroes of $P_i(X) = X^2 + a_iX + b_i$ is divided by $\mathfrak{l}$. Thus C_δ is $\mathfrak{l}$-maximal and contains C, which shows (ii) also in this case. □

8.2 Lemma. *Suppose that* char($\mathbb{F}$) $= 2$, *let* a, b *be any elements of* A *such that* $P(X) = X^2 + aX + b$ *generates an imaginary quadratic order* $C = B_f$, *and let* $m = m_{\mathfrak{l}}(f)$. *Then the following three conditions are equivalent:*

(a) $m > 0$;

(b) $a \equiv 0 (\mathrm{mod}\ \ \mathfrak{l})$, *and there exists* $s \in A$ *such that*

$$(*) \qquad s^2 + as + b \equiv 0 (\mathrm{mod}\ \ \mathfrak{l}^2);$$

(c) $a \equiv 0 (\mathrm{mod}\ \ \mathfrak{l})$, *and for each* $s \in A$ *such that* $s^2 \equiv b (\mathrm{mod}\ \ \mathfrak{l})$, *condition* $(*)$ *holds.*

Proof. (a) $\Rightarrow$ (b): Let z be a root of $P(X)$, $z = s + \mathfrak{l}t$ with $s \in A$, $t \in B$. Then $z - s = z + s$ is divisible by $\mathfrak{l}$ and has minimal polynomial $X^2 + aX + s^2 + as + b$. (b) $\Rightarrow$ (c) is trivial. (c) $\Rightarrow$ (a): Choose any s with $s^2 \equiv b(\mathrm{mod}\ \mathfrak{l})$. Then $P_1(X) = X^2 + a_1X + b_1$ with $(a_1, b_1) = (a/\mathfrak{l}, (s^2+as+b)/\mathfrak{l})$ generates an order which at $\mathfrak{l}$ is strictly larger than C. □

8.3 Proposition. *The quantities $V_\mathfrak{l}(a,b)$ and $v_\mathfrak{l}(a,b)$ are related by*

$$V_\mathfrak{l}(a,b) = |\mathfrak{l}|^{m_\mathfrak{l}(f)} v_\mathfrak{l}(a,b).$$

Both sides equal $L_\mathfrak{l}(1,\chi) = (1 - \chi(\mathfrak{l})|\mathfrak{l}|^{-1})^{-1}$ if $m_\mathfrak{l}(f) = 0$.

Proof. This follows from comparing the left hand side, given by (6.18) and (6.11)(ii), with the formula (7.9) for $v_\mathfrak{l}(a,b)$, taking both parts of (8.1) into account. □

Therefore, the product in (6.19) equals

$$\prod_{\mathfrak{l} \text{ prime of } A} V_\mathfrak{l}(a,b) = |f| v(a,b) \tag{8.4}$$

with $v(a,b) = \prod_\mathfrak{l} v_\mathfrak{l}(a,b)$.

We still need to express the genus of E or, equivalently, the degree of the conductor $\mathrm{cond}(\chi)$ of χ, in terms of a and b. This is easy in case

$\boxed{\mathrm{char}(\mathbb{F}) \neq 2}$, which we suppose for the moment.

Let $D = D(a,b) = a^2 - 4b = f^2 D_0$ be the discriminant with its maximal monic quadratic divisor f^2. Then $C = B_f$, and for any finite prime $\mathfrak{l}$ of A, $\chi(\mathfrak{l}) = (\frac{D_0}{\mathfrak{l}})$. We have $\chi(\infty) \in \{0, -1\}$, with

$$\chi(\infty) = 0 \Leftrightarrow \infty \text{ ramified in } E \Leftrightarrow \deg\ D_0 \text{ odd},$$

in which case $\mathrm{cond}(\chi)$ is the divisor $(D_0) \cdot \infty$, since the ramification at ∞ is tame. Further, $\mathrm{cond}(\chi) = (D_0)$ if $\chi(\infty) = -1$. Here we use multiplicative notation for divisors, and (D_0) is the finite part (i.e., the part coprime with ∞) of the divisor of D_0. With (6.12) we find

$$q^g = q^{-1}|D_0|^{1/2} \quad (\text{resp. } q^{-1/2}|D_0|^{1/2})$$

and

$$|f|q^g = q^{-1}|D|^{1/2} \quad (\text{resp. } q^{-1/2}|D|^{1/2})$$

in case $\deg\ D$ is even (resp. odd). Combining this with (8.4), formula (6.19) may be written

$$h^*(a,b,\mathfrak{p}) = |\mathfrak{p}|^{1/2} v(a,b) v_\infty(a,b), \tag{8.5}$$

where

$$v_\infty(a,b) = |\frac{D}{b}|^{1/2} \left\{ \begin{array}{c} \frac{2}{q+1} \\ q^{-1/2} \end{array} \right\} \text{ if } \deg\ D \text{ is } \left\{ \begin{array}{c} \text{even} \\ \text{odd} \end{array} \right\}.$$

Note that $|D| = |\mathfrak{p}| = |b|$ if $d = \deg\ \mathfrak{p}$ is odd, so $v_\infty(a,b) = q^{-1/2}$ in this case.

Now we deal with the more complicated case

$\boxed{\mathrm{char}(\mathbb{F}) = 2}$, that hypothesis being in force until (8.17).

(8.6) Let for the moment L be a local (i.e., complete with finite residue class field) nonarchimedean field of characteristic 2 with normalized valuation w. We put H_L for the additive subgroup $\{s^2 + s \mid s \in L\}$ of L and call $c \in L$ *reduced* if $w(c) = w_{\mathrm{red}}(c) := \sup\{w(c') \mid c' \in c + H_L\}$. We need the following result, a proof of which may be found in [10] Prop. 1.3.

8.7 Proposition. *Let $c \in L$ have valuation $w(c) = -k \in \mathbb{Z}$, L' be the splitting field of $X^2 + X + c$ over L, and e the conductor exponent of L'/L.*

(i) *If $k > 0$ then x is reduced if and only if k is odd; in this case, $e = k + 1$;*
(ii) *if $k = 0$ then either x is reduced or $x \in H_L$;*
(iii) *if $k < 0$ then $x \in H_L$.*

Further, $e = 0$ in cases (ii) and (iii).

We now return to the general situation of this section, restricted to characteristic 2, and apply the above to determine the conductor $\mathrm{cond}(\chi)$.

8.8 Proposition. *Let a, b subject to our general assumptions be given, with $a \neq 0$. Then the finite part of* $\mathrm{cond}(\chi)$ *is $(a/f)^2$.*

Proof. The assertion may be verified locally for each prime $\mathfrak{l}$ of A. Thus let $m_\mathfrak{l}$ be the $\mathfrak{l}$-adic valuation, and consider the series $(a,b) = (a_0, b_0), \ldots, (a_\delta, b_\delta)$ as in the proof of (8.1), where $\delta = \delta_\mathfrak{l}(a,b) = m_\mathfrak{l}(f)$. We have

$$\mathfrak{l} | \mathrm{cond}(\chi) \Leftrightarrow \chi(\mathfrak{l}) = 0 \Leftrightarrow a_\delta \equiv 0 \pmod{\mathfrak{l}},$$

and in this case $b'_\delta = s^2 + a_\delta s + b_\delta$ (where $s \in A$ satisfies $s^2 = b_\delta (\bmod\ \mathfrak{l})$) has valuation $m_\mathfrak{l}(b'_\delta) = 1$. The two polynomials $X^2 + aX + b$ and $X^2 + X + c$ with $c = a_\delta^{-2} b'_\delta = a^{-2} \mathfrak{l}^{2\delta} b'_\delta$ have the same splitting field. Since $m_\mathfrak{l}(c) = -2m_\mathfrak{l}(a) + 2\delta + 1$, Proposition 8.7 yields $2m_\mathfrak{l}(a) - 2\delta = 2m_\mathfrak{l}(a/f)$ for the conductor exponent at $\mathfrak{l}$. $\square$

It remains to determine the conductor exponent of χ at ∞. We use the notation introduced in (8.6), with $(L, w) = (K_\infty, -\deg)$. Further, $|x|_{\text{red}} := q^{\deg_{\text{red}}(x)}$ for $x \in K_\infty$.

8.9 Proposition. *Suppose that $a \neq 0$, put $c := b/a^2$ and $|c|_{\text{red}} = q^k$. The conductor exponent of χ at ∞ is 0 if $k = 0$ and $k+1$ if $k > 0$.*

Proof. The splitting fields of $X^2 + aX + b$ and of $X^2 + X + c$ agree. Therefore the result follows from (8.7). $\square$

In the subcase of $\boxed{a \neq 0}$, the data relevant for the evaluation of (6.19) are thus given by the following table, where $|b/a^2|_{\text{red}} = q^k$:

(8.10)

k	η	$\chi(\infty)$	$\deg\ \operatorname{cond}(\chi)$	$\eta L_\infty(1,\chi)q^g\|f\|$
0	2	-1	$2\deg\ a - 2\deg\ f$	$\frac{2}{q+1}\|a\|$
$> 0, \text{odd}$	1	0	$2\deg\ a - 2\deg\ f + k + 1$	$q^{(k-1)/2}\|a\|$

We encode this information in the function $\psi : K_\infty \longrightarrow \mathbb{R}$, defined by

$$\psi(x) = \left\{ \begin{array}{c} 0 \\ \frac{2}{q+1} \\ q^{(k-1)/2} \end{array} \right\} \quad \text{if } |x|_{\text{red}} = \left\{ \begin{array}{c} 0 \\ 1 \\ q^k \end{array} \right\}. \tag{8.11}$$

It is locally constant, thus continuous, since H_{K_∞} is open in K_∞.

Let us finally consider the subcase $\boxed{a = 0}$, which implies that we are in the exceptional case (E_2) of section 6, i.e., E/K is inseparable and $B = \mathbb{F}[\sqrt{T}]$. Here $\eta L_\infty(1,\chi)q^g = 1$ trivially, so

$$h^*(0, b, \mathfrak{p}) = |f| v(0, b), \tag{8.12}$$

which, by virtue of (6.10), equals $S(f, B) = \sum_{f'|f} |f'|$. The quantity f may be determined by the following lemma.

8.13 Lemma. *Any element x of K_∞ may uniquely be written in the form $x = s^2 + Tt^2$ with $s = s_x$, $t = t_x \in K_\infty$. Then $C := \mathbb{F}(\sqrt{\mathfrak{p}}) = \mathbb{F}(\sqrt{b})$ is the order $A + t_b B$ in $B = \mathbb{F}[\sqrt{T}]$, i.e., f is the monic associated with t_b.*

Proof. Obvious. $\square$

We may now give the formula that substitutes (8.5) in characteristic 2. Viz, combining (8.10)–(8.13), we find

$$h^*(a, b, \mathfrak{p}) = |\mathfrak{p}|^{1/2} v(a, b) v_\infty(a, b), \tag{8.14}$$

where

$$v_\infty(a,b) = \begin{cases} |a^2/b|^{1/2}\psi(b/a^2), & \text{if } a \neq 0 \\ |t_b^2/b|^{1/2}, & \text{if } a = 0. \end{cases}$$

The following observations are in order:

(8.15) As in the case of odd characteristic, we have

$$v_\infty(a,b) \leq q^{-1/2},$$

with equality if and only if $d = \deg\ \mathfrak{p}$ is odd. This results from (8.10) and (8.13);

(8.16) Our formulas define $v_\infty(a,b)$ on $\{(a,b) \in K_\infty \times K_\infty \mid |a|^2 \leq |b|,\ b \neq 0\}$, and it is an amusing exercise to show that the resulting function is continuous on this set. We leave the details to the reader.

The results of this section are summarized as follows, allowing now arbitrary characteristics for $\mathbb{F}$.

8.17 Theorem. *The weighted class number $h^*(a,b,\mathfrak{p})$ of Drinfeld modules of rank two over $\mathbb{F}_\mathfrak{p}$ with characteristic polynomial $X^2 - aX + b$ may be written as*

$$h^*(a,b,\mathfrak{p}) = |\mathfrak{p}|^{1/2} v(a,b) v_\infty(a,b),$$

where

$$v(a,b) = \prod_{\mathfrak{l} \text{ prime of } A} v_\mathfrak{l}(a,b)$$

is a conditionally convergent product, the $v_\mathfrak{l}(a,b)$ are the continuous local density functions defined in (7.1) *and calculated in* (7.9)*, and the factors $v_\infty(a,b)$ are given by* (8.5) *and* (8.14) *for the case of odd or even characteristics, respectively.* □

This should be compared with Theorem 5.5 of [11], where elliptic curves over the prime field $\mathbb{F}_p$ are counted in a similar way. The "classical" counterpart of the present $v_\infty(a,b)$ is the Sato-Tate function $(a,b) \longmapsto \frac{2}{\pi}\sqrt{1 - a^2/4b}$, where now a and $b > 0$ are elements of the infinite completion $\mathbb{R}$ of $\mathbb{Q}$.

In view of Theorem 4.2(ii) (see also Remark 4.6), the fact (8.15), the results of [13] sect. 6 and some numerical evidence in [14], we dare to propose the following conjecture, which is a partial analogue for Drinfeld modules of the Sato-Tate conjecture.

8.18 Conjecture. *Let $\phi = (g, \Delta)$ be a Drinfeld A-module of rank two defined over K without complex multiplication, i.e., such that* $\mathrm{End}_{\overline{K}}(\phi) = A$*. Suppose that $q^2 - 1$ is the least number s such that Δ^s is a (q^2-1)-th power in K. For each $\mathfrak{p}$ of K where ϕ has good reduction,* *let $F^{(\mathfrak{p})}$ be the Frobenius endomorphism of the reduced module $\phi^{(\mathfrak{p})}$ over $\mathbb{F}_{\mathfrak{p}}$, with trace $a(\phi^{(\mathfrak{p})})$. For $\mathfrak{p}$ of degree d put*

$$a^{(\mathfrak{p})} := \left\{ \begin{array}{c} a(\phi^{(\mathfrak{p})})T^{-(d-1)/2} \\ a(\phi^{(\mathfrak{p})})T^{-d/2} \end{array} \right\} \textit{ if } d \textit{ is } \left\{ \begin{array}{c} \textit{odd} \\ \textit{even} \end{array} \right\}.$$

Then the collection $\{a^{(\mathfrak{p})} \mid \deg\ \mathfrak{p}$ odd and ϕ has good reduction at $\mathfrak{p}\}$ is equidistributed in the ring O_∞ of integers of K_∞.

The idea behind is that the distribution of the normalized traces $a^{(\mathfrak{p})}$ in O_∞ should be determined by the factor $v_\infty(a, b)$ alone, which is constant for $\mathfrak{p}$ of odd degree.

A similar conjecture, taking the shape of $v_\infty(a, b)$ into account, could be made for $\mathfrak{p}$ of even degree; details still to be worked out. The question is certainly related to Jiu-Kang Yu's "Sato-Tate law", formulated and proved in [20], although it is difficult to find a direct implication as long as the range H of Yu's Galois representation (*loc. cit.* 3.5) is unknown.

Another possible direction of future research is the average behavior of $h^*(a, b, \mathfrak{p})$ with a fixed, $\deg\ \mathfrak{p} \longrightarrow \infty$, similar to [11] Theorem 6.4. For a first approach, see [1].

References

[1] David, C.: Frobenius distributions of Drinfeld modules of any rank, J. Numb. Th. **90** (2001),329–340.

[2] Deligne, P., Husemöller, D.: Survey of Drinfeld modules, Contemp. Math. **67** (1987), 25–91.

[3] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg **14** (1941), 197–272.

[4] Drinfeld, V.G.: Elliptic modules (Russian), Math. Sbornik **94** (1974), 594–627, English translation: Math. USSR-Sbornik **23** (1976), 561–592.

[5] Drinfeld, V.G.: Elliptic modules II, Math. USSR-Sbornik **31** (1977), 159–170.

[6] Gekeler, E.-U.: Zur Arithmetik von Drinfeld-Moduln, Math. Ann. **262** (1983), 167–182.

[7] Gekeler, E.-U.: Über Drinfeld'sche Modulkurven vom Hecke-Typ, Comp. Math. **57** (1986), 219–236.

[8] Gekeler, E.-U.: On the coefficients of Drinfeld modular forms, Invent. Math. **93** (1988), 667–700.

[9] Gekeler, E.-U.: On finite Drinfeld modules, J. Algebra **141** (1991), 187–203.

[10] Gekeler, E.-U.: Highly ramified pencils of elliptic curves in characteristic two, Duke Math. J. **89** (1997), 95–107.

[11] Gekeler, E.-U.: Frobenius distributions of elliptic curves over finite prime fields, Int. Math. Res. Notes **37** (2003), 1999–2018.

[12] Goss, D.: Basic structures of function field arithmetic, Springer-Verlag 1996.

[13] Hsia, L.-Ch., Yu, J.: On characteristic polynomials of geometric Frobenius associated to Drinfeld modules, Comp. Math. **122** (2000), 261–280.

[14] Jung, F.: Charakteristische Polynome von Drinfeld-Moduln, Diplomarbeit Saarbrücken 2000.
[15] Neukirch, J.: Class field theory, Springer-Verlag 1986.
[16] Rosen, M.: Number theory in function fields, Springer-Verlag 2002.
[17] Schweizer, A.: On Drinfeld modular curves with many rational points over finite fields, Finite Fields Appl. **8** (2002), 434–443.
[18] Shimura, G.: Arithmetic theory of automorphic functions, Princeton University Press 1971.
[19] Yu, J.-K.: Isogenies of Drinfeld modules over finite fields, J. Number Th. **54** (1995), 161–171.
[20] Yu, J.-K.: A Sato-Tate law for Drinfeld modules, Comp. Math. **138** (2003), 189–197.
[21] Drinfeld modules, modular schemes and applications, Proc. Alden-Biesen 1996, E.-U. Gekeler et al. (eds.), World Scientific 1997.

Ernst-Ulrich Gekeler
FR 6.1 Mathematik
Universität des Saarlandes
Postfach 15 11 50
D-66041 Saarbrücken
Germany
gekeler@math.uni-sb.de