ON FINITE DRINFELD MODULES

by

Ernst–Ulrich Gekeler

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Str. 26
5300 Bonn 3
Federal Republic of Germany

MPI/89 –9

ON FINITE DRINFELD MODULES

Introduction

In [5], Deuring determined the possible isomorphism types of endomorphism rings of elliptic curves, notably for those curves that are defined over a finite field. His results were later generalized to abelian varieties of higher rank by Tate [17] and Honda [13].

Now in the fundamental paper [6], Drinfeld transports the modular theory of elliptic curves to the function field case. He found the kind of dioplantine objects (called by him "elliptic modules") that over global function fields play the role of elliptic curves in number theory. By his theory, he was able to prove analogues of the theorem of Kronecker–Weber, the main theorem of complex multiplication, and parts of the Langlands conjectures for $GL(2)$ over function fields. Actually, in the course of the last few years, the theory of Drinfeld modules has shown to be the key tool in the arithmetic of function fields over finite fields. This comes from the fact that Drinfeld modules lead to moduli problems that are related to $GL(r)$ (r arbitrary), and to Galois representations in local fields of positive characteristic, which one needs in order to describe the absolute Galois group of a global function field.

In this paper, we treat Deuring's problem of endomorphism rings in the Drinfeld module setting, i.e., we study Drinfeld modules that are defined over a finite field, and their endomorphism rings. Let (K,∞) be a pair consisting of a function field K in one variable over a finite field, and a place ∞ of K. Let further A be the ring of elements of K with poles at most at ∞, and $\mathfrak{p}$ a prime of A with finite residue field $\mathbf{F}_{\mathfrak{p}} = A/\mathfrak{p}$. As for elliptic curves, the classification up to isogeny of Drinfeld modules ϕ

over extensions of $\mathbb{F}_p$ is given by the isomorphism type of $\mathrm{End}(\phi) \otimes_A K$ (Thm. 3.5). This ring turns out to be a certain division algebra central over the subfield E generated over K by the Frobenius endomorphism F of ϕ (Thm. 2.9). (These two results are stated in [7], Prop. 2.1 in a somewhat disguised form, and with a few cryptical hints as proofs.). We call ϕ supersingular if E equals K. One of our results is that for supersingular ϕ, $\mathrm{End}(\phi)$ is a maximal order in $\mathrm{End}(\phi) \otimes K$ (Thm. 4.3). This opens the way to use Drinfeld modules in the arithmetic of division algebras over function fields, exploiting properties of modular schemes. In a subsequent paper, we will use this approach to effectively determine the class and type numbers of such algebras. Simple examples on this are given in (4.4) and (4.7).

We introduce the norm $n(u)$ of an isogeny u, an ideal of A which for separable u is the Euler–Poincaré characteristic of $\mathrm{Ker}(u)$, and for u an endomorphism agrees with the reduced norm. By means of $n(u)$, we may interpret the value $P_\phi(1)$ of the characteristic polynomial of F as the E.–P. characteristic of our finite Drinfeld A–module (Thm. 5.1). This leads to the definition of the local zeta function (or rather Z–function) $Z_\phi(t)$ attached to ϕ, which has properties similar to those of the Z–function of an abelian variety over a finite field. Also, our results suggest that the global zeta functions ζ_ϕ (for Drinfeld modules ϕ over finite extensions of K) which may be constructed through local factors as above, have reasonable properties. This is at least the case if ϕ has "complex multiplication", as results e.g. from Takahashi's paper [16].

I. Background on Drinfeld modules

Let K be a function field in one variable over the finite field $\mathbb{F}_q$ with q elements, which we suppose to be algebraically closed in K. Fix a place "∞" of K, let K_∞ be the completion, and A the ring of elements of K regular outside of ∞. On A, we have the degree function $\deg: A \longrightarrow \mathbb{Z}$ (extended to K in the obvious way) that maps a to $\log_q \#(A/a)$. The typical example is given by the polynomial ring $A = \mathbb{F}_q[T]$, where "deg" is the usual degree function. By an "ideal" of A, we understand a non–zero ideal. We use "prime", "prime ideal", and "place" of A as synonyms.

Let L be a field that is an extension of either K or of $\mathbb{F}_p = A/\mathfrak{p}$, $\bar{L}$ its algebraic closure, and $\gamma: A \longrightarrow L$ the canonical structure as an A–algebra. L has characteristic (written $\mathrm{char}(L)$) ∞ or $\mathfrak{p}$, respectively. Let τ be the Frobenius endomorphism relative to $\mathbb{F}_q$, i.e., the map $x \longmapsto x^q$. In the ring $\mathrm{End}_L(G_a)$ of all L–endomorphisms of the additive group scheme $G_a|L$, τ generates a subalgebra $L\{\tau\}$ that is simply the non–commutative polynomial algebra in τ subject to the commutation rule $\tau \circ x = x^q \circ \tau$, $x \in L$. Let $\deg_\tau f$ be the well–defined "degree" of $f \in L\{\tau\}$ in τ.

Monic elements $f \in L\{\tau\}$ (i.e., those with leading coefficient 1) correspond bijectively to finite subschemes of $\mathbb{F}_q$–vector spaces of $G_a|L$ by $f \longmapsto H = \ker(f)$. Any monic f may uniquely be written $f = f_s \circ f_i$, where f_s is separable (i.e., its constant coefficient is non–zero) and $f_i = \tau^h$ is purely inseparable. We write $h = \mathrm{ht}(f) = \mathrm{ht}(H)$ and call it the height of f or H, respectively.

1.1. Definition: A Drinfeld module over L of rank $r \geq 1$ is a structure of A–module on $G_a|L$, given by a ring homomorphism

$$\phi : \quad A \longrightarrow L\{\tau\} \subset \mathrm{End}_L(G_a) ,$$

$$a \longmapsto \phi_a$$

where we require that for any $a \in A$, the following two conditions hold:

(i) $\deg_\tau \phi_a = r \cdot \deg a$;

(ii) $\phi_a = \gamma(a) +$ terms divisible by τ .

Thus if $A = \mathbb{F}_q[T]$, a rank r Drinfeld module ϕ is given by

$$\phi_T = \gamma(T) + g_1\tau + \ldots + g_r\tau^r ,$$

where $g_1, \ldots, g_{r-1}$, $g_r \neq 0$ may be chosen arbitrarily in L . A <u>morphism</u> $u : \phi \longrightarrow \psi$ of D. modules (more precisely, a morphism defined over L , or L–morphism) is a morphism of group schemes over L commuting with the A–action , i.e., an element $u \in L\{\tau\}$ such that for all $a \in A$

(*) $$u \circ \phi_a = \psi_a \circ u$$

holds. Therefore, we have endomorphisms, isomorphisms, and automorphisms of D. modules, where e.g. an isomorphism is a non–zero constant $u \in L$ for which (*) is satisfied. Non–zero morphisms are possible only between D. modules of the same rank; they are called <u>isogenies</u>.

<u>1.2. Proposition</u> (see e.g. [2], Thm. 4.9): The endomorphism ring End (ϕ) of the rank r Drinfeld module ϕ is a finitely generated projective A–module of rank less or

equal to r^2. Moreover, $\mathrm{End}(\phi) \underset{A}{\otimes} K_\infty$ is a division ring.

Clearly, there exists a finite extension L' of L such that all $\bar{L}$ – endomorphisms of ϕ are defined over L'.

We let ${}_a\phi = \ker(\phi_a)$ be the scheme of a–division points, which is a finite subscheme of A–modules of $G_a \mid L$. For an ideal n of A, we let

$$ {}_n\phi = \bigcap_{a \in n} \ker(\phi_a) . $$

It is easy to see that ${}_n\phi$ is reduced, and its module ${}_n\phi(\bar{L})$ of $\bar{L}$–points is isomorphic with $(A/n)^r$ if and only if n is relatively prime to $\mathrm{char}(L)$. Thus let q be a prime ideal of A different from $\mathrm{char}(L)$, K_q and A_q the q–adic completions, and put

$$ {}_{q^\infty}\phi = \varinjlim {}_{q^n}\phi . $$

We define the q–adic Tate module of ϕ by

$$ T_q(\phi) = \mathrm{Hom}_{A_q}(K_q/A_q, {}_{q^\infty}\phi(\bar{L})) , \tag{1.3} $$

which is a free A_q–module of dimension r. On $T_q(\phi)$ we have representations of

a) the Galois group $\mathrm{Gal}(\bar{L}:L)$ of L and

b) the ring $\mathrm{End}(\phi)$.

Since any endomorphism $u \neq 0$ of ϕ has finite kernel, the associated homomorphism

$i_q : \mathrm{End}(\phi) \otimes A_q \longrightarrow \mathrm{End}_{A_q}(T_q)$ is injective.

Later on, we will need the following characterization of kernels of isogenies:

(1.4) Let ϕ be a Drinfeld module over L and $H \subset Ga|L$ a finite subscheme of $\mathbb{F}_q$–vector spaces. Then H is the kernel of some isogeny $u : \phi \longrightarrow \psi$ if and only if

(i) $H(\bar{L})$ is an A–submodule of $\bar{L}$ (A–action by ϕ) ;

(ii) $\mathrm{ht}(H) = 0$ $\quad (\mathrm{char}(L) = \infty)$

$\mathrm{ht}(H) \equiv 0(\deg \mathfrak{p})$ $\quad (\mathrm{char}(L) = \mathfrak{p})$.

This implies e.g. that for any isogeny $u : \phi \longrightarrow \psi$, there exists $v : \psi \longrightarrow \phi$ such that $v \circ u = \phi_a$ for some $a \in A$.

Proofs of all the assertions collected here may be found in [6], [8], or [2].

2. Endomorphism rings

Let now $\mathfrak{p}$ be a prime of A of degree d, and suppose L is a finite extension of degree m of $\mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}$. Then L has cardinality q^n, where $n = d \cdot m$, and contains $\mathbb{F}_q$ via $\gamma : A \longrightarrow L$. Let $F = \tau^n : x \longmapsto x^{q^n}$ be the associated Frobenius morphism. If the Drinfeld module ϕ (always assumed of rank r) is defined over L, F commutes with $\phi(A) \subset L\{\tau\}$, i.e., $F \in \mathrm{End}(\phi)$. As long as ϕ is fixed, we write "A" for the subring $\phi(A)$ of $L\{\tau\}$.

(2.1) Let $L(\tau)$ be the division ring of fractions of $L\{\tau\}$. It is central of degree n^2 over $\mathbb{F}_q(F)$ = quotient field of $\mathbb{F}_q\{F\}$, and splits at the places of $\mathbb{F}_q(F)$ different from $F = 0$ and $F = \infty$. At $F = 0$ ($F = \infty$), its invariants are $1/n$ ($-1/n$), respectively. (See e.g. [14]. In the identification of local Brauer groups with $\mathbb{Q}/\mathbb{Z}$, there are two possible sign choices. Ours, which agrees with that of [14], is defined by the assertion above.)

(2.2) Recall that for any field extension E of $\mathbb{F}_q(F)$ that embeds into $L(\tau)$, there is only one place extending the ramified place $F = 0$ or $F = \infty$, respectively. This follows for example from Thm. 32.15, loc. cit ..

(2.3) Regarding $\phi : A \longrightarrow L\{\tau\}$ as an embedding, $K = \mathrm{Quot}(A)$ is contained in $L(\tau)$. Let E be the extension of K generated by F. Then $E_\infty = E \underset{K}{\otimes} K_\infty$ is a field.

(2.4) Let $\deg : E^* \longrightarrow \mathbb{Q}$ be the extension to E of the valuation $\deg : K^* \longrightarrow \mathbb{Z}$, which is uniquely determined by the preceding. From $\deg_\tau(\phi_a) = r \cdot \deg a$ ($a \in A$), we derive $\deg F = n/r$. If d_∞ denotes the degree of ∞ over $\mathbb{F}_q$, this means that F

has fractional pole order $n/r \cdot d_\varpi$ at ϖ with respect to the field K_ϖ.

(2.5) By (2.3), $[E : K] = [E_\varpi : K_\varpi] = e \cdot f$, where e = ramification index and f = residual degree of $E_\varpi : K_\varpi$. But $E_\varpi = K_\varpi(F)$, hence

$$e = \text{denominator of pole order of } F \text{ w.r.t. } K_\varpi .$$

(2.6) Correspondingly, $[E : \mathbb{F}_q(F)] = [E_\varpi : \mathbb{F}_q(F)_\varpi] = e' \cdot f'$ by (2.2). Clearly, the residual degree f' equals $d_\varpi \cdot f$, whereas the ramification index e' is given by

$$e' = \text{pole order of } F \text{ w.r.t. } E_\varpi = \text{numerator of } n/r \cdot d_\varpi .$$

Combining (2.5) and (2.6) yields the equality

$$[E : \mathbb{F}_q(F)] / [E : K] = n/r \tag{2.7}$$

(compare "proof" of Prop. 2.1 in [7]).

Therefore, letting $r_1 = [E : K]$,

$$r_2 = r/r_1 = n/[E : \mathbb{F}_q(F)]$$

is an integer.

(2.8) For a subset S of $L(\tau)$, let $\mathscr{C}(S)$ be its commutant. Then

$$\mathrm{End}(\phi) \underset{A}{\otimes} K = \mathscr{E}(K) = \mathscr{E}(E)$$

since $E = K(F)$ and F is central. From the commutant equality ([1], § 10, Thm. 2), we see that $\mathrm{End}(\phi) \otimes K$ is central over E of degree r_2^2. Its class in the Brauer group of E is the class of $L(\tau)$ over $\mathbb{F}_q(F)$ restricted to E, as follows from loc. cit., § 10, Prop. 2. Denoting by $\mathfrak{P}$ the unique prime of E that divides F (note that $\mathfrak{P}$ lies above the prime $p = \mathrm{char}(L)$ of K), the invariants of $\mathrm{End}(\phi) \otimes K$ are therefore $[E : \mathbb{F}_q(F)] \cdot 1/n = 1/r_2$ at $\mathfrak{P}$, $-1/r_2$ at the place ∞ of E, and zero at all the other places.

Summarizing, we have proved the theorem (stated in [7]):

2.9. Theorem: Let E be the subfield of $\mathrm{End}(\phi) \otimes K$ generated over K by F, and $r_1 = [E : K]$ its degree. Then r/r_1 is an integer r_2, and $\mathrm{End}(\phi) \otimes K$ is a central division ring over E of degree r_2^2. There is a unique prime $\mathfrak{P}$ of E that divides F, and $\mathfrak{P}$ lies above p. $\mathrm{End}(\phi) \otimes K$ splits at primes different from $\mathfrak{P}$ and ∞, and has invariants $1/r_2$, $-1/r_2$ at $\mathfrak{P}$, ∞, respectively.

3. Norms of isogenies

We keep the notations of the last section.

Let N be the map from $\mathrm{End}(\phi) \otimes K$ to K obtained by composing the reduced norm $nr : \mathrm{End}(\phi) \otimes K \longrightarrow E$ with the field norm $N_K^E : E \longrightarrow K$. Then N is K–homogeneous of degree r and agrees on maximal commutative subfields H with the norm $N_K^H : H \longrightarrow K$.

3.1. Lemma: For $u \in \mathrm{End}(\phi)$, we have $\deg_\tau N(u) = r \cdot \deg_\tau u$.

Proof: Both sides define valuations on $\mathrm{End}(\phi) \otimes K$ equivalent with the ∞–adic valuation. The proportionality factor comes out by evaluating on $u = \phi_a$, $a \in A$.

For each prime $q \neq p$ of A, $i_q(H) \otimes K_q$ is a maximal commutative K_q–subalgebra of $\mathrm{End}_{K_q}(T_q(\phi) \otimes K_q)$, whose norm mapping to K_q is the determinant. Therefore, $N|_H = (\det \circ i_q)|_H$ for every maximal commutative subfield H of $\mathrm{End}(\phi) \otimes K$, so

$$N = \det \circ i_q . \tag{3.2}$$

Let $P_\phi(X)$ be the characteristic polynomial of $i_q(F)$, and $M_\phi(X)$ the minimal polynomial of F over A.

3.3. Lemma: $P_\phi(X) = M_\phi(X)^{r_2}$, $r_2 = r/[E : K]$.

Proof: It suffices to show that $P(t) = M(t)^{r_2}$ for $t \in E$. But

$P(t) = \det(t - F) = N_K^E \circ \mathrm{nr}(t - F) = N_K^E((t - F)^{r_2}) = (N_K^E(t - F))^{r_2} = M(t)^{r_2}$, the last equality coming from $E = K(F)$.

3.4. Corollary: The characteristic polynomial $P_\phi(X)$ of F in the q–adic representation i_q has coefficients in A that are independent of q.

3.5. Theorem: For two Drinfeld modules ϕ and ψ of rank r over L, the following statements are equivalent:

(a) ϕ and ψ are isogeneous;

(b) $\mathrm{End}(\phi) \otimes K$ and $\mathrm{End}(\psi) \otimes K$ are isomorphic K–algebras;

(c) $M_\phi = M_\psi$;

(d) $P_\phi = P_\psi$.

Proof: c) and d) are equivalent by the lemma, since both M and P are monic polynomials. a) $\Rightarrow$ c): Let $M_\phi(X) = \Sigma\, a_i X^i$. Then in $L\{\tau\}$, $\Sigma\, F^i \phi_{a_i} = 0$. Let $u : \phi \longrightarrow \psi$ be an L–isogeny; i.e., $u \in L\{\tau\}$ such that for each $a \in A$, we have $u \circ \phi_a = \psi_a \circ u$. Then $0 = \Sigma\, u \circ F^i \circ \phi_{a_i} = \Sigma\, F^i \circ \psi_{a_i} \circ u$, which implies $\Sigma\, F^i \circ \psi_{a_i} = 0$, in other words, $M_\phi \mid M_\psi$, thus $M_\phi = M_\psi$. c) $\Rightarrow$ b): Denote by E_ϕ, $E_\psi \subset L(\tau)$ the fields generated by the Frobenius elements, respectively, which are K–isomorphic by assumption. From Thm. 2.9, we see that an isomorphism may be extended to an isomorphism of $\mathrm{End}(\phi) \otimes K$ to $\mathrm{End}(\psi) \otimes K$. b) $\Rightarrow$ a): Let $\alpha : \mathrm{End}(\phi) \otimes K \longrightarrow \mathrm{End}(\psi) \otimes K$ be an isomorphism. By the theorem of Skolem–Noether ([1], § 10, Thm. 1), there exists $u \in L(\tau)$ such that α is conjugation

with u . But $L(\tau) = L\{\tau\} \underset{\mathbb{F}_q\{F\}}{\otimes} \mathbb{F}_q(F)$, hence, up to a central element, we may assume $u \in L\{\tau\}$, which clearly defines an isogeny $u : \phi \longrightarrow \psi$.

(3.6) Following Deuring [5], we associate an isogeny with any left ideal of the A–order $\mathrm{End}(\phi)$ in $\mathrm{End}(\phi) \otimes K$. In the given context, this generalizes a construction of Hayes [12]. (For notation and the elementary ideal theory in simple algebras, we refer to [14].)

Let u be a left ideal of $\mathrm{End}(\phi)$. Since $L\{\tau\}$ is right euclidean, the left ideal $L\{\tau\}u$ of $L\{\tau\}$ is principal, generated by $u = u(u) \in L\{\tau\}$, which is well–defined, requiring u to be monic. But $\phi(A)$ is central in $\mathrm{End}(\phi)$, so $u = u\,\phi(A)$, which for each $a \in A$ implies the existence of $\psi_a \in L\{\tau\}$ with $u \circ \phi_a = \psi_a \circ u$.

3.7. Lemma: The map $a \longmapsto \psi_a$ defines a Drinfeld module $\psi = \phi^u$, and u is an isogeny from ϕ to ψ .

Proof. Clearly, ψ is a ring homomorphism, and ψ_a satisfies the degree condition (i) of (1.1). If $f \in u$, we have $\mathrm{ht}(f) \equiv 0(d)$ by (1.4) (ii), so the same holds for $u =$ g.c. right divisor of $f \in u$ in $L\{\tau\}$. But this implies that ϕ_a and ψ_a have the same constant coefficient $\gamma(a)$, i.e., condition (ii) of (1.1).

3.8. Lemma: Let $\mathfrak{R}$ be the right order in $\mathrm{End}(\phi) \otimes K$ of the left ideal u of $\mathrm{End}(\phi)$. Then conjugation with u in $L\{\tau\}$ defines an injection of $\mathfrak{R}$ into $\mathrm{End}(\phi^u)$.

Proof: Let $r \in \mathfrak{R}$, i.e., $u\,r \subset u$, which yields the existence of $s \in L\{\tau\}$ with $u \circ r = s \circ u$. But then

$$s \circ \psi_a \circ s^{-1} = s \circ u \circ \phi_a \circ u^{-1} \circ s^{-1} = u \circ r \circ \phi_a \circ r^{-1} \circ u^{-1} = u \circ \phi_a \circ u^{-1} = \psi_a ,$$

since r commutes with ϕ_a, thus $u \circ \mathfrak{R} \circ u^{-1} \subset \mathrm{End}(\psi)$.

(3.9) Next, we associate an ideal $n(u)$ of A with each isogeny $u : \phi \longrightarrow \psi$ of Drinfeld modules of rank r over L. If M is a finite A–module, let $\chi(M)$ be the Euler–Poincaré characteristic of M, which is an ideal of A uniquely determined by the conditions

(i) $\chi(M) = q$, if $M \cong A/q$ with a prime ideal q of A;

(ii) If $0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$ is exact, then $\chi(M) = \chi(M_1)\chi(M_2)$.

Define the norm $n(u)$ of the isogeny u by

$$n(u) = p^{ht(u)/d} \cdot \chi((\ker u)(\bar{L})).$$

3.10. Lemma: Let u and v be isogenies of rank r Drinfeld modules over L that may be composed. Then

(i) $n(u \circ v) = n(u)n(v)$;

(ii) $\deg_\tau u = \deg n(u)$;

(iii) $n(u) = (N(u))$ if $u \in \mathrm{End}(\phi)$ is an endomorphism;

(iv) Let $u \subset \mathrm{End}(\phi)$ be a left ideal. Then $n(u(u)) =$ ideal generated by $N(f)$, $f \in u$.

Proof: (i) and (ii) follow directly from the definition. (iii) Let q be a prime different from p, and t a very high power of q. We calculate the q–part of $(N(u))$:

$$(N(u))_q = (\det \circ i_q(u)) \qquad \text{(by (3.1))}$$

$$= \chi\,(T_q(\phi)/\text{im } i_q(u))$$

$$= \chi({}_\tau\phi/u({}_\tau\phi))$$

$$= \chi(\ker(u) \cap {}_\tau\phi)$$

$$= \chi(\ker(u))_q$$

$$= (n(u))_q\,.$$

Furthermore, by (ii) and Lemma 3.1,

$r \cdot \deg n(u) = r \cdot \deg_\tau u = \deg_\tau N(u) = r \cdot \deg N(u)$, so $(N(u))$ and $n(u)$ agree, since they have the same q–components $(q \neq p)$ and the same degree. (iv) results from (iii) in view of $u(u) =$ g.c. right divisor in $C\{\tau\}$ of $\{f \in u\}$, so

$n(u(u)) =$ g.c.d. $\{n(f) \mid f \in u\}$.

Note that (iii) implies that the norm of an endomorphism is a principal ideal.

4. Supersingularity

We now study in detail the extreme case of Thm. 2.9 where $E = K$. Let r be the rank of ϕ. The assumption $E = K$ is equivalent with $F = \phi_f$, some $f \in A$, whose divisor (f) must be a power of p. Comparing τ–degrees yields $(f) = p^{m/r}$. (Recall that $m = [L : \mathbb{F}_p]$.) We denote by ϕ_p the isogeny from ϕ to ϕ^u associated with the left ideal $u = \mathrm{End}(\phi)p \subset \mathrm{End}(\phi)$. Then $\ker(\phi_p) = {}_p\phi$.

4.1. Proposition: The following assertions on ϕ are equivalent:

a) There exists a finite extension L' of L such that over L', the degree $[\mathrm{End}(\phi) \otimes K : K]$ equals r^2.

b) Some power of F lies in A.

c) ϕ_p is purely inseparable.

Proof: The equivalence of a) and b) comes from Thm. 2.9. By the preceding, b) says ${}_{p^{m/r}}\phi$, thus ${}_p\phi$ is local, which means that ϕ_p is purely inseparable. Conversely, let ϕ_p be purely inseparable. Then ${}_p\phi(\bar{L}) = 0$, and also ${}_{p^i}\phi(\bar{L}) = 0$, all i. If $p^i = (f)$ is principal, ϕ_f is purely inseparable, and some powers of F and of ϕ_f agree.

Drinfeld modules that satisfy the conditions of the proposition are called supersingular. All the supersingular D. modules of rank r in characteristic p are isogeneous by Thm. 3.5. Their isomorphism classes are finite in number, since all of them may be defined over a certain finite field L.

Let m_0 be the order of p in the class group of A, and L the extension of $\mathbb{F}_p$ of degree $m = m_0 \cdot r$.

4.2. Proposition: Any supersingular Drinfeld module ϕ of rank r and characteristic p is isomorphic to one defined over L .

Proof: Let ϕ be defined over a finite extension L′ of L , and $F = \tau^n$, $n = d \cdot m$ the Frobenius relative to L . Let $f \in A$ with $(f) = p^{m_0}$, thus $\phi_f = \text{const} \cdot \tau^n$. Without restriction, we may assume $\phi_f = \tau^n$, possibly replacing ϕ by an isomorphic D. module. If $a \in A$ and $\phi_a = \Sigma\, a_i \tau^i$,the commutation rule $\phi_a \circ \phi_f = \phi_f \circ \phi_a$ implies $a_i^{q^n} = a_i$ for all i , i.e., $a_i \in L$.

4.3. Theorem: Let ϕ be a supersingular rank r Drinfeld module over the finite field L , which we assume large enough such that all endomorphisms are defined over L .

(i) $\mathrm{End}(\phi)$ is a maximal order in $\mathrm{End}(\phi) \otimes K$.

(ii) The left ideal classes of $\mathrm{End}(\phi)$ correspond bijectively to the elements of the set $\Sigma(r,p)$ of isomorphism classes of supersingular rank r Drinfeld modules in characteristic p .

Proof: (i) We adapt the idea of Deuring's proof in the elliptic curve case [5] to our situation. In each order, there always exist left ideals with maximal left (and right) orders. Thus from (3.8), we see that there exists a supersingular ψ isogeneous with ϕ and such that $\mathrm{End}(\psi)$ is maximal. We are therefore reduced to showing that $\mathrm{End}(\psi)$ is maximal if ψ is isogeneous with ϕ and $\mathrm{End}(\phi)$ is maximal.

Let $u : \phi \longrightarrow \psi$ be a monic isogeny with norm $n(u) = n$ a fixed ideal in A . Decompose

$$n = p^f n' \ , \ \text{where} \ n' = \prod q_i^{f_i}$$

with different primes $q_i \neq p$ of A. Since ϕ is supersingular, the p–component of $\ker(u)$ is purely local, and u is completely determined by the number f and the A–module $\ker(u)\ (\overline{L})$, which has Euler–Poincaré characteristic n'. Thus choosing u amounts to choosing for each i an A–submodule of length f_i of

$$n_i\phi \cong (A/n_i)^r \ , \ n_i = q_i^{f_i} .$$

Next, by (3.10) (iv), for any left ideal u of $\mathrm{End}(\phi)$, the norm $n(u(u))$ agrees with the reduced norm $nr(u)$ relative to the central division algebra $\mathrm{End}(\phi) \otimes K : K$. Since the ideal theory of $\mathrm{End}(\phi)$ localizes, u is given by the choice of:

a left ideal u_p of $\mathrm{End}(\phi) \otimes A_p$ with reduced norm p^f; and for each i,
a left ideal u_i of $\mathrm{End}(\phi) \otimes A_{q_i} \cong M_r(A_{q_i})$ with reduced norm n_i.

Now there exists only one ideal u_p as above ([14], Thm. 13.2) and by the theorem of elementary divisors, there are as many ideals u_i as required as A–submodules of length f_i of $(A/n_i)^r$.

In view of $n(u(u)) = nr(u)$, this means that each isogeny u as above comes from a left ideal u. Lemma 3.8 now yields that for $\psi = \phi^u$, $\mathrm{End}(\psi)$ is a maximal order, and (i) is proved.

(ii) By (i), we have a surjective map $u \longmapsto \phi^u$ from the set of left ideal classes of $\mathrm{End}(\phi)$ to $\Sigma(r,p)$, which is also injective, as is easily seen.

In the following, let $D = D(r,p)$ be the central divison algebra of degree r^2 over K with invariants $1/r$, $-1/r$ at p, ∞, respectively. The theorem may be used in investigating the arithmetic of D.

4.4. Example: Let $K = \mathbb{F}_q(T)$ be the rational function field and "∞" the usual place at infinity, i.e., $A = \mathbb{F}_q[T]$, and p a prime of degree d. The number of supersingular isomorphism classes of rank 2 D. modules in characteristic p is given by

$$\#(\Sigma(2,p)) = \frac{q^d - 1}{q^2 - 1} \qquad (d \equiv 0(2))$$

$$= \frac{q^d - 1}{q^2 - 1} + \frac{q}{q+1} \qquad (d \equiv 1(2)).$$

Thus for $d = 1$ or 2, $\Sigma(2,p)$ consists of one element, represented by the module

$$\phi_T = \gamma(T) + \tau^2 \qquad (d = 1)$$

$$\phi_T = \gamma(T) + \tau - \gamma\left[\frac{1}{p'(T)}\right]\tau^2 \qquad (d = 2),$$

where $p(T)$ is the monic polynomial that generates p. The formula is proved in [8] by an elementary argument, which works only in the case above. In [9], a conceptual proof is given that is based on the arithmetic of Drinfeld modular curves. It has the advantage to generalize to the case of arbitrary function rings A. Combined with the results of [10], this will lead to explicit formulas for $\#(\Sigma(2,p))$ (= class number of $D(2,p)$) in terms of zeta values of the function field K under consideration. Another generalization

of (4.4) is the case where A still equals the polynomial ring $\mathbb{F}_q[T]$, but $r \geq 2$ is arbitrary. Here, the corresponding modular scheme has dimension $r-1$ over A, but is still simple enough such that the number $\#(\Sigma(r,\mathfrak{p}))$ can be determined (see forthcoming work of the author). Other interesting results concerning class numbers of $D(r,\mathfrak{p})$ (and of more general algebras, and non–maximal orders) have been obtained by Denert [3] and Denert–v. Geel [4].

(4.5) In certain cases, our methods also allow to describe the set of <u>types</u> (i.e., conjugacy classes = isomorphism classes) of maximal orders in $D(r,\mathfrak{p})$. First note that if u is a left ideal in the maximal order $\mathrm{End}(\phi)$ of $D(r,\mathfrak{p})$, u is two–sided if and only if $u(u)$ induces an isomorphism $\mathrm{End}(\phi) \xrightarrow{\simeq} \mathrm{End}(\psi)$ for $\psi = \phi^u$. The next proposition gives necessary conditions for endomorphism rings to be isomorphic.

<u>4.6. Proposition</u>: Assume the class number of the quotient ring $A[\mathfrak{p}^{-1}]$ of A is one. Then the types of maximal orders in $D(r,\mathfrak{p})$ correspond bijectively to the orbits of $\Sigma(r,\mathfrak{p})$ under the action of the Galois group $G = \mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}} : \mathbb{F}_{\mathfrak{p}})$.

<u>Proof</u>: Clearly, applying $\sigma \in G$ to the coefficients of $f \in \mathrm{End}(\phi)$ defines an isomorphism $\mathrm{End}(\phi) \xrightarrow{\simeq} \mathrm{End}(\psi)$, where $\psi = \sigma(\phi)$. Let $\phi \in \Sigma(r,\mathfrak{p})$. Since all maximal orders in $D(r,\mathfrak{p})$ appear up to conjugacy as right orders of a left ideal u of the given maximal order $\mathrm{End}(\phi)$, the assertion will follow from (ii) of the theorem and

(*) If $\psi \in \Sigma(r,\mathfrak{p})$ and $\mathrm{End}(\psi)$ is isomorphic with $\mathrm{End}(\phi)$, there exists a purely inseparable isogeny $\sigma : \phi \longrightarrow \psi$.

Namely, such a σ has the form $\sigma = \text{const} \cdot \tau^{\mathrm{id}}$, and, possibly replacing ψ by an isomorphic module, we may assume $\sigma = \tau^{\mathrm{id}}$. Then ψ will be the Galois twist $\sigma(\phi)$ of ϕ, where we now consider σ as an element of G.

Proof of (*): Let $u : \phi \longrightarrow \psi$ be an isogeny. Factorizing $u = u_s \circ u_i$ into a purely inseparable $u_i : \phi \longrightarrow \phi'$ and a separable $u_s : \phi' \longrightarrow \psi$, we have $\mathrm{End}(\phi) \xrightarrow{\cong} \mathrm{End}(\phi')$. Let u_s correspond to the left ideal u_s in $\mathrm{End}(\phi')$, having right order $\mathfrak{R}$. From the maximality of $\mathfrak{R}$ and Lemma 3.8, $\mathfrak{R} \cong \mathrm{End}(\psi)$, which by assumption is isomorphic with $\mathrm{End}(\phi') \cong \mathrm{End}(\phi)$. But this means that u_s is two–sided. Since u_s is separable, $\mathrm{nr}(u_s) = \mathfrak{n}(u_s)$ is relatively prime to $\mathfrak{p}$. In view of the known structure of two–sided ideals of the maximal order $\mathrm{End}(\phi')$ ([14], Thm. 22.4, 22.10), the class number condition forces u_s to be principal, and hence ϕ' is isomorphic with ψ.

The conditions of the proposition are in particular satisfied if A itself has class number one, e.g. if $A = \mathbb{F}_q[T]$. In the situation of Example 4.4 (suppose $p > 2$ for simplicity), the number $t(2,\mathfrak{p})$ of types of maximal orders in $D(2,\mathfrak{p})$ is related to the number w of fixed points of the Atkin–Lehner involution (see [9], Korollar 5.4) on a certain modular curve by

$$t(2,\mathfrak{p}) = \tfrac{1}{2}\,(\#(\Sigma(2,\mathfrak{p})) + w/2)\,.$$

Let e be a non–square in $\mathbb{F}_q$ and $\mathfrak{p}(T)$ the monic generator of $\mathfrak{p}$. Then w may be expressed through the class numbers $h(\sqrt{\mathfrak{p}(T)})$, $h(\sqrt{e\,\mathfrak{p}(T)})$ of the rings obtained

by adjoining square roots of $p(T)$, $e \cdot p(T)$ to A (loc. cit., Prop. 3.6). Together, this yields

$$(4.7) \qquad t(2,p) = \frac{1}{2}\left[\frac{q^d - q}{q^2 - 1} + 1 + \frac{1}{2}\left(h(\sqrt{p(T)}\right) + h(\sqrt{e\,p(T)})\right], \text{ if } d \text{ is odd,}$$

$$= \frac{1}{2}\left[\frac{q^d - 1}{q^2 - 1} + \frac{1}{2}\,h(\sqrt{e\,p(T)})\right], \text{ if } d \text{ is even.}$$

The values for $d = 1,2,3$ are $1,1,q+1$.

5. Zeta functions

We let now again ϕ be a fixed rank r Drinfeld module defined over L , where L has degree m over $\mathbb{F}_p$. Further, $F = \tau^n$, $n = m \cdot d$, is the Frobenius morphism relative to L . Let $P(X) = P_\phi(X) \in A[X]$ be the characteristic polynomial of F . For any natural number i , L_i denotes the extension of L of degree i , and $\chi(L_i,\phi)$ the Euler–Poincaré characteristic of the finite A–module L_i defined by means of ϕ .

5.1. Theorem:

(i) The principal ideal $(P(1))$ of A equals $\chi(L,\phi)$.

(ii) $(P(0)) = p^m$.

(iii) The zeroes x_i of P in an extension of K_∞ satisfy $|x_i| \leq q^{n/r}$.

Proof: From (2.9) and (3.3), we see that p is the only prime of A that divides $P(0)$. The exponent m comes from (2.4) and the product formula in K , thus (ii). Since P is a power of the minimal polynomial M of F , it suffices to prove (iii) for M instead of P . But M is also the minimal polynomial of $E_\infty = K(F) \underset{K}{\otimes} K_\infty$, hence is irreducible over K_∞ . Now the assertion follows from considering the Newton polygon of M over the local field K_∞ , thus (iii). Finally, as in (3.10), we calculate the q–primary component of the principal ideal $(P(1))$:

$$(P(1))_q = (\det \circ i_q(F-1))$$

$$= \chi\,(T_q(\phi)/\mathrm{im}\; i_q(F-1))$$

$$= \chi\,(\ker(F-1))_q\,.$$

Furthermore, $\deg(F-1) = \deg F = n/r$ (see (2.3)), which means that $P(1)$ and $N(F-1)$ have the same q–adic valuations at all places $q \neq p$ of K, including $q = \infty$. Hence by the product formula, their p–adic valuations agree too, and (i) is shown.

The theorem has some remarkable consequences. First, we get restrictions for those fields that carry a Drinfeld module.

5.2. Corollary: If there exists a Drinfeld module (rank arbitrary) over the field L of degree m over A/p, the ideal p^m is principal.

By results of D. Hayes, a finite field L carries a rank one Drinfeld module if and only if L contains some residue field of the Hilbert class field H of (K,∞) as an A–subalgebra ([12], sect. 8; H = maximal unramified abelian extension of K that splits completely at ∞). Combined with (5.2), this yields an explicit version of the principal ideal theorem of class field theory for K (see also [15]):

5.3. Corollary: Every ideal of A becomes principal over the Hilbert class field H of (K,∞).

5.4. Corollary: $\chi\,(L_i,\phi)$ is a principal ideal for all i.

5.5 Corollary: Let ϕ be supersingular with Frobenius endomorphism $F = \phi_f$, $f \in A$, and $q \neq p$ a prime of A. If ϕ has one non–trivial q–torsion point over L_i, all of its

q–torsion points will be defined over L_i .

Proof: Since $M_\phi(X) = X - f$, we have $\chi(L_i,\phi) = ((1 - f^i))^r$.

Let now for a moment F be an endomorphism of an r–dimensional vector space V over an arbitrary field K . Let $\Lambda^i V$ be the i–th exterior power and $\Lambda^i F$ the induced endomorphism. We put

$$Q_i(X) = \det(1 - X \Lambda^i F) ,$$

and denote by " $\frac{d}{dX}\log$" the operator $f \longmapsto f'/f$ on power series $f(X)$.

5.6. Lemma: We have the formal identity of power series

$$\sum_{k\geq 1} \det(1 - F^k)X^k = X \frac{d}{dX} \log \prod_{0\leq i\leq r} Q_i(X)^{(-1)^{i+1}} .$$

Proof: This results from combining the well–known identities

a) $\det(1 - XF) = \sum_{0\leq i\leq r} (-1)^i \operatorname{Tr}(\Lambda^i F)X^i$ (applied to F^k and evaluated at $X = 1$) ,

b) $-X \frac{d}{dX} \log \det(1 - XF) = \sum_{k\geq 1} \operatorname{Tr}(F^k)X^k$, and

c) $\frac{d}{dX} \log(f \cdot g) = \frac{d}{dX} \log(f) + \frac{d}{dX} \log(g)$.

The preceding motivates our

5.7. Definition: The Z–function of a rank r Drinfeld module ϕ over L is

$$Z_\phi(t) = \prod_{0 \le i \le r} Q_i(t)^{(-1)^{i+1}},$$

where $Q_i(X)$ is the inverse characteristic polynomial $\det(1 - X \Lambda^i F)$ of the i–th exterior power $\Lambda^i F$ acting on $\Lambda^i T_q(\phi)$. Note that $Q_i(X)$ is completely determined by $Q_1(X) = Q(X) = X^r P(X^{-1})$.

5.8. Example: Let $r = 1,2,3$, and $P(X)$ given by $P(X) = X - a$, $X^2 - aX + b$, $X^3 - aX^2 + bX - c$, respectively. Then

$$Z_\phi(t) = \frac{1 - at}{1 - t} \qquad (r = 1)$$

$$= \frac{1 - at + bt^2}{(1 - t)(1 - bt)} \qquad (r = 2)$$

$$= \frac{(1 - at + bt^2 - ct^3)(1 - ct)}{(1 - t)(1 - bt + act^2 - c^2t^3)} \qquad (r = 3).$$

5.9. Variant: If we have a meaningful notion of exponentiation of ideals of A with values in K_∞ (see e.g. [11]), we define the zeta function of ϕ by

$$\zeta_\phi(s) = Z_\phi(p^{-m \cdot s}).$$

Also, if ϕ is defined over a finite extension L of K with ring of A–integers B, we

may define a global zeta function

$$\zeta_\phi(s) = \prod_{q \text{ prime of } B} Q_q(t_q)^{-1},$$

where $t_q = p^{-m(q)\cdot s}$, $m(q) = [B/q : A/p]$, and the factors Q_q are constructed from the reductions of ϕ mod q. By the following corollary, we may expect that ζ_ϕ contains meaningful information about the arithmetic of ϕ. If e.g. ϕ is the Carlitz module for $A = \mathbb{F}_q[T]$, defined by $\phi_T = T + \tau$, ζ_ϕ will be the Carlitz–Goss zeta function which has values

$$\sum_{a \in A \text{ monic}} a^{-k} \text{ at } s = k, \text{ and } \lim_{i \to \infty} \sum_{\substack{a \text{ monic} \\ \deg a \le i}} a^{k} \text{ at } s = -k,$$

for natural numbers k. It is known that these values and their congruence properties are intimately connected with the arithmetic of $K = \mathbb{F}_q(T)$.

From (5.1) and (5.6) we obtain

5.10. Corollary: Let $\Sigma\, a_k\, t^k$ be the power series expansion of $t \frac{d}{dt} \log Z_\phi(t)$. Then $a_k \in A$, and (a_k) is the E.–P. characteristic $\chi(L_k, \phi)$.

In the following concluding examples, we assume that $A = \mathbb{F}_q[T]$, and that ϕ is defined over the "prime field" $\mathbb{F}_p = A/p$. Write $p(T)$ for the monic generator of p, and ν for the map composed of the norm $\mathbb{F}_p \longrightarrow \mathbb{F}_q$ and the canonical inclusion $\mathbb{F}_q \hookrightarrow A$.

5.11. Examples:

(i) $r = 1$, i.e., $\phi_T = T + c\tau$, $0 \neq c \in \mathbb{F}_p$. We have $P(X) = X - a$. Comparing coefficients yields $a = \nu(c) \cdot p(T)$, thus

$$Z_\phi(t) = \frac{1 - \nu(c)p(T)}{1 - t} .$$

(ii) $r = 2$, and suppose $\phi_T = T + g\tau + \tau^2$, $g \in \mathbb{F}_p$. Then $P(X) = X^2 - aX + b$, $b = \text{const} \cdot p(T)$, and by (iii) of (5.1), $\deg a \leq d/2$, $d = \deg p$. The precise value of a and b may be expressed through the "Deuring polynomial" of [8]. Let first $d = 1$, i.e., $\mathbb{F}_q \xrightarrow{\cong} \mathbb{F}_p$. Then $P(X) = X^2 + gX - p(T)$ and

$$Z_\phi(t) = \frac{1 + gt - p(T)t^2}{(1 - t)(1 + p(T)t)} .$$

If $d = 2$, an elementary calculation gives $P(X) = X^2 - (\nu(g) + p'(T))X + p(T)$, which leads to

$$Z_\phi(t) = \frac{1 - (\nu(g) + p'(T))t + p(T)t^2}{(1 - t)(1 - p(T)t)} .$$

The complexity of determining $P(X)$ grows rapidly with d and r increasing.

REFERENCES

[1] N. Bourbaki: Algèbre, Ch. 8: Modules et anneaux semi–simples. Masson, Paris 1981

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

[3] M. Denert: Affine and projective orders in central simple algebras over global function fields. Ph.D. Thesis Gent 1987

[4] M. Denert and J. Van Geel: The class number of hereditary orders in non–Eichler algebras over global function fields. Math. Ann. 282, 379–393, 1988

[5] M. Deuring: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Hamb. 14, 197–272, 1941

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

[7] V.G. Drinfeld: Elliptic modules II. Math. USSR–Sbornik 31, 159–170, 1977

[8] E.–U. Gekeler: Zur Arithmetik von Drinfeld–Moduln. Math. Ann. 262, 167–182, 1983

[9] E.–U. Gekeler: Über Drinfeld'sche Modulkurven vom Hecke–Typ. Comp. Math. 57, 219–236, 1986

[10] E.–U. Gekeler: Drinfeld modular curves. Lecture Notes in Mathematics 1231. Springer–Verlag, Berlin–Heidelberg–New York 1986

[11] D. Goss: On a new type of L–function for algebraic curves over finite fields. Pac. J. Math. 105, 143–181, 1983

[12] D. Hayes: Explicit class field theory on global function fields. Studies in Algebra and Number Theory. G.C. Rota ed. Academic Press, New York 1979

[13] T. Honda: Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Japan 20, 83–95, 1968

[14] I. Reiner: Maximal orders. Academic Press, London–New York–San Francisco 1975

[15] M. Rosen: The Hilbert class field in function fields. Exp. Math. 5, 365–378, 1987

[16] T. Takahashi: Good reduction of elliptic modules. J. Math. Soc. Japan 34, 475–487, 1982

[17] J. Tate: Endomorphisms of abelian varieties over finite fields Inv. 2, 134–144, 1966