"ABELIAN GROUP ACTIONS ON ALGEBRAIC VARIETIES WITH ONE FIXED POINT"

by

Amir H. Assadi [1] Rebecca Barlow [2]
Friedrich Knop [3]

(1) (2) (3) Max–Planck–Institut
für Mathematik
Gottfried–Claren–Str. 26
5300 Bonn 3
Federal Republic of Germany

(1) University of Wisconsin
Madison, WI 53706
USA

MPI/89-11

"ABELIAN GROUP ACTIONS ON ALGEBRAIC VARIETIES WITH ONE FIXED POINT"

by

Amir H. Assadi [1] [2]

Rebecca Barlow [1]

Friedrich Knop [1]

---

(1) All authors would like to thank the hospitality and financial support of Max–Planck–Institut für Mathematik (Bonn) during this research.

(2) The first author thanks professors G. Mislin, and W. Browder for stimulating conversations on this subject.

Introduction. Since early stages of its developments, the theory of transformation groups has relied on comparison of linear representations with general group actions on manifolds from algebraic as well as geometric points of view. If G is a finite group and W is an orthogonal linear representation space of G, then it is an elementary fact that the unit sphere $S(W)$ with the induced linear G–action has more than one G–fixed point if $S(W)^G \neq \phi$. The generalization of this fact to arbitrary smooth G–manifolds is neither elementary nor obvious. The first result in this direction is due to Conner–Floyd ([8] § 31) who proved that for $G = (\mathbb{Z}/2)^n$ acting smoothly on a closed manifold X, the fixed point set X^G cannot consist of one point. Conner and Floyd conjectured ([8] § 45) that the cyclic group $\mathbb{Z}/q^n$, where q is an odd prime, cannot act on a closed orientable manifold with only one fixed point. The example of Conner and Floyd for a smooth $\mathbb{Z}/4$ action on $\mathbb{RP}^2$ shows that this fixed–point property does not hold in general. The Conner–Floyd conjecture was proved by Atiyah and Bott ([4] Theorem 7.1) using their version of the Lefschetz fixed point formula for elliptic complexes (nowadays known as Atiyah–Bott–Lefschetz formula). Conner and Floyd also established their conjecture using their work on the cobordism of odd order periodic maps ([9] Theorem 8.3). They also constructed a smooth G–action on a Riemann surface with exactly one fixed point for G a cyclic odd order group with at least two dinstinct primes dividing $|G|$.

A more general form of the Conner–Floyd conjecture for smooth odd order abelian p–group actions is due to W. Browder ([6]) and Ewing and Stong ([11]) who showed that the abelian hypothesis is necessary. In fact, based on the Atiyah–Bott and Conner–Floyd Theorem, Ewing and Stong ([11]) proved that if $G \neq (\mathbb{Z}/2)^n$ is a compact Lie group, then G can act smoothly on a closed

(possibly non–orientable) manifold with one fixed point and in the orientable case, only abelian groups of odd prime power order cannot act with only one fixed point. The generalitzation and interpretation of the Conner–Floyd conjecture in an algebraic context was taken up by Assadi in [2] and [3]. Assadi's generalization to chain complexes and G–spaces with Poincaré duality provided an algebraic proof of the Conner–Floyd conjecture for $G = (\mathbb{Z}/p)^n$. For infinite dimensional Poincaré G–spaces and kG chain complexes satisfying Poincaré duality, the Conner–Floyd conjecture may be formulated in terms of the associated varieties [3]. Recently, W. Browder has extended his results in [6] to abelian p–group actions on finite dimensional simplicial complexes which are $(\mathbb{Z}/p)-$homology manifolds [7], thus giving a further generalization of the Conner–Floyd conjecture. See also Browder [6a].

In this paper, we prove that the Conner–Floyd conjecture generalizes to actions on complete non–singular algebraic varieties over an arbitrary algebraically closed field k. In particular:

Theorem 2.1. Let X be a complete algebraic variety over an algebraically closed field of characteristic $p \geq 0$, and let G be a finite abelian group of order q^r, where q is a prime different from p, acting on X via automorphisms. If the fixed point set consists of one point $x \in X$, then X is singular at the point x.

In fact, the following scheme–theoretic generalization is proved:

Corollary 3.2. Let G be a finite abelian group of prime power order acting on a complete non–singular algebraic variety V defined over an algebraically closed field of arbitrary characteristic. Then V^G cannot consist of an isolated point, i.e. $V^G \neq \mathrm{Spec}(k)$.

For varieties over $\mathbb{C}$, the underlying topological space of X in the analytic topology is triangulable according to Hironaka ([13]). Combining the above theorem and the results of Browder [6] or Assadi [2] [3] one concludes that in this case such an X is not a mod p homology manifold if G is an abelian p–group. If G is an elementary abelian group, then (by Assadi [2] [3]) X does not satisfy Poincaré duality with $\mathbf{F}_p$ – coefficients. For $G = \mathbb{Z}/p$ this result can be deduced from Bredon [5], as pointed out to us by Browder.

From the point of view of varieties, the condition $p \neq q$ in Theorem 2.1 is necessary, since the action of $\mathbb{Z}/p$ on $\mathbb{P}^1(\overline{\mathbf{F}}_p)$ given by $(x_0 ; x_1) \longrightarrow (x_0 ; x_0 + x_1)$ has precisely one fixed point. On the other hand, it is easily seen that this fixed point has multiplicity two, so that Corollary 3.2 applies to this case. Finally, one may ask to what extent the non–singularity of X plays a role for the truth of the Conner–Floyd conjecture. By means of examples (Section 3) one can see that there exists one–fixed point actions on projectively normal subvarieties of $\mathbb{P}^N$ which have only a normal singularity at the fixed point. Moreover, for $k = \mathbb{C}$, the link of the singularity at X^G could be quite complicated (see Corollary 3.3).

In the next section we discuss some preliminary notions from algebraic geometry which may not be well–known to researchers in topological transformation groups. In Section 2 we give the proof of the main theorem. In Section 3 we discuss some examples including the case of p–groups actions in characteristic p.

Section One. Preliminaries.

In the sequel, k denotes an algebraically closed field of characteristic $p \geq 0$, and G will be a finite group. If $(|G|, p) = 1$ ($|G|$ = order of G), then the element $\frac{1}{|G|} \sum_{g \in G} g$ is an idempotent in kG. Consequently, all kG–modules are kG–projective and the group algebra kG is semisimple, which shows that all kG–modules are completely reducible (i.e. kG–isomorphic to a direct sum of irreducible kG–submodules). This result (known as Maschke's Theorem, cf. Curtis–Reiner [7]), refines further when G is abelian. Namely, any n–dimensional kG–module W is G–isomorphic to a direct sum of one–dimensional (over k) kG–submodules : $W \cong \bigoplus_{i=1}^{n} L_i$, $\dim_k L_i = 1$. Further, the representation of G on L_i factors through $G \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/\ell$ where $\mathbb{Z}/\ell$ acts on L_i via an appropriate ℓ–th root of unity. Similarly for infinite dimensional representation the above idempotent may be used.

The standard reference for notation and definitions from algebraic geometry is Hartshorne [9] and the reader will find the details in [9] as appropriatly referred to them. In particular, the term variety refers to an irreducible variety. Basic properties of projective varieties are adequately covered in [9] Chapter I where the reader may replace "complete" by "projective". Let G act effectively on a projective k–variety X by automorphisms. Then the geometric orbit space X/G exists and it is a projective variety as well. In the case $k = \mathbb{C}$, this coincides with the orbit space under the usual (Euclidean) topology. We will need this fact only for curves in the positive characteristic where complete and projective are equivalent (indeed for non–singular curves only). This case is handled by the following elementary considerations. The G–action on X induces

a G–action on the field of rational functions $K(X) \overset{\text{def}}{\equiv} K$ leaving the subfield k fixed. In particular, the fixed field $L \overset{\text{def}}{\equiv} K^G$ is a finitely generated field extension of k of transcendence degree one, and the extension $L \subset K$ is Galois. It is well–known that there is a unique (up to isomorphism) projective non–singular curve X' whose function field is isomorphic to L. Moreover, there is a k–morphism $\pi : X \longrightarrow X'$ inducing the inclusion $L \subset K$ (cf. [9] Ch. I § 6).

In the classical case, i.e. $k = \mathbb{C}$, the map π is a ramified (i.e. branched) covering, and ramification occurs over the orbits whose isotropy subgroups are non–trivial. Let g and g' be the genera of X and X' respectively. Then, the Riemann–Hurwitz formula relates g and g' when X and X' are non–singular:

(GRH) $$2g - 2 = |G|(2g' - 2) + \deg R .$$

Here R is the ramification divisor ([9] Chapter IV, § 2).

The proof of this theorem for $k = \mathbb{C}$ is an elementary Euler–Poincaré characteristic count, and simplifies to the following:

(RH) $$2g - 2 = |G|(2g' - 2) + \sum_{x \in X} (|G| - |G(x)|)$$

where $|G(x)|$ is the number of points in the orbit of $x \in X$ which is equal to $|G|$ except for finitely many x.

In the general case, the above formula (GRH) is valid, and the only delicate point is the computation of deg R . However, when $(|G_x|,p) = 1$ for all points $x \in X$ with non–trivial isotropy groups, the ramification is called tame, and deg $R = \sum_{x \in X} (|G| - |G(x)|)$ so that (RH) holds in the following discussion (cf. [9] Ch. IV, § 2).

We will also need to consider desingularization of curves and an equivariant analogue. Suppose X is a possibly singular projective curve on which G acts by automorphisms. Then the set of singular points of X is a finite G–invariant set, i.e. a G–set. Also, G acts on the function field $K(X) \equiv K$ by k–automorphisms as above. Let Y be the unique non–singular projective curve such that $K(Y) \overset{\text{def}}{\equiv} K$. Then the G–action on K induces a G–action on the set of discrete valuation rings of K (which is the underlying set of Y). Thus G acts on Y by isomorphisms. Every local ring $\mathcal{O}_{X,x}$, $x \in X$, when regarded as a subring of K , is dominated by a discrete valuation ring $\mathcal{O}_{Y,y}$ ([9] Ch. I, § 6). The inclusions $\mathcal{O}_{X,x} \subset \mathcal{O}_{Y,y}$ for various $x \in X$ and $y \in Y$ give rise to a map $f : Y \longrightarrow X$ which turns out to be a morphism. Clearly, f will be equivariant with respect to the given G–actions. Further, Y is the normalization of X , and in the complement of the singular set, say $X_{reg} = X - X_{sing}$, $f : f^{-1}(X_{reg}) \longrightarrow X_{reg}$ is an isomorphism, and $f : f^{-1}(X_{sing}) \longrightarrow X_{sing}$ is a G–map of G–sets.

Remark. Although we will not need the following, it is interesting to notice that Y/G is the normalization of X/G , and the suitable generalization of the Hurwitz formula for singular curves should agree with the standard one for $Y \longrightarrow Y/G$.

Section Two.

We will keep the hypotheses and notation of the previous section.

2.1. Theorem. Let X be a complete algebraic variety over an algebraically closed field of characteristic $p \geq 0$, and let G be a finite abelian group of order q^r, where q is a prime different from p. Suppose that G acts on X via automorphisms, and X^G consists of one point. Then X^G is a singular point of X.

As a corollary of this theorem we have the following analogue of the Conner–Floyd conjecture and its generalitzation by Browder [5] [6].

2.2. Corollary. Let X be a complete non–singular variety over an algebraically closed field of characteristic $p \geq 0$. Suppose G is an abelian group of order q^r, where q is a prime different from p, and G acts on X via automorphisms. Then X^G cannot consist of one point.

Proof.: To get a contradiction, assume that $X^G = \{x_0\}$, X is smooth at x_0, and the action on $X - \{x_0\}$ is fixed–point free, i.e. for all $x \neq x_0$, the isotropy subgroup $G_x \neq G$. Notice that $T_{x_0}X$ is a G–representation. Choose a basis $e_1, \ldots, e_n$ of eigenvectors of $T_{x_0}X$ and let $x_1, \ldots, x_n$ be the corresponding coordinate functions. Let $\mathfrak{m}$ be the maximal ideal of the local ring $\mathcal{O}_{X,x_0}$ at x_0. Then we have a projection $\mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \cong (T_{x_0}X)^*$. Choose a G–equivariant splitting (using semisimplicity) $\varphi : (T_{x_0}X)^* \longrightarrow \mathfrak{m}$ and let $f_i := \varphi(x_i) \in \mathcal{O}_{X,x_0}$. Let $V_0 \subseteq X$ be an open neighborhood of x_0 where all f_i

are defined, and let $V := \bigcap_{g \in G} g\,V_0$ be a G–invariant open neighborhood. This induces a G–equivariant morphism $\psi : V \longrightarrow T_{x_0}X : \psi(v) = \Sigma\, f_i(v)e_i$. Since $x_i \equiv f_i \pmod{\mathfrak{m}^2}$, the differential $d\psi$ induces an isomorphism of the Zariski cotangent spaces, which implies that ψ is étale at x_0 . Now let $C := \{v \in V \mid f_2(v) = \ldots = f_n(v) = 0\}$. C is smooth at x_0 by the Jacobian criterion. Let $\Sigma_0 :=$ component of C passing through x_0 . Thus Σ_0 is a curve passing through x_0 and non–singular at x_0 . Moreover, Σ_0 is G–invariant and $\Sigma_0^G = \{x_0\}$. Let Σ_1 be the closure of Σ_0 in X , (i.e. add the finitely many possibly missing closed points to Σ_0 to get a complete, possibly singular curve Σ_1). It follows that Σ_1 is also non–singular at x_0 and the G–invariant finite set of singular points of Σ_1 lies in the fixed–point free part of Σ_1 . Now let $\pi_1 : \Sigma \longrightarrow \Sigma_1$ be the equivariant normalization of Σ_1 as described in Section One. Thus, π_1 is a finite proper morphsim which restricts to a G–isomorphism onto the open subset of regular points of Σ_1 , i.e. an open G–invariant neighborhood of x_0 . Hence, Σ^G consists of one point, namely $\pi_1^{-1}(x_0)$.

To summerize, we have produced a nonsingular complete curve Σ on which g acts by automorphisms and Σ^G consists of one point, call it x_0 again. Let $\Sigma' = \Sigma/G$ and $\pi : \Sigma \longrightarrow \Sigma/G$ be the projection onto the orbit space (cf. Section One), and let $x_0' = \pi(x_0)$. Since $(|G|, p) = 1$, the ramifications of π are all tame, and we may apply the Riemann–Hurwitz formula (RH) of Section One. For each branch point $x' \neq x_0'$, $x' \in \Sigma'$, and each ramification point $x \in \pi^{-1}(x')$ lying above x' , the ramification index is $|G_x| \neq |G|$. Let $g = \text{genus}(\Sigma)$ and $g' = \text{genus}(\Sigma')$. Thus (RH) becomes

$$2g - 2 = |G|(2g' - 2) + \sum_{x \neq x_0} |G| \cdot \left[1 - \frac{1}{|G_x|}\right] + |G| \cdot \left[1 - \frac{1}{|G|}\right] \quad .$$

Hence $2g-2 \equiv -1 (\mathrm{mod}\ q)$.

On the other hand, consider the space of differential one–forms $\Omega^1_{\Sigma/k}$ which is a g–dimensional k–vector space on which G acts linearly. From the above conclusion of (RH), we conclude that $g \neq 1$. For $g = 0$, $\Sigma \cong \mathbb{P}^1(k)$ and it is well–known that the automorphism group of $\mathbb{P}^1(k)$ is $PGL(2,k)$ and as a result, up to G–isomorphism, the G–action on $\mathbb{P}^1(k)$ is linear. It follows that any such effective linear G–action on $\mathbb{P}^1(k)$ must have at least two fixed points. Hence $g \geq 2$, and $\Omega^1_{\Sigma/k} \neq 0$. According to Section One, $\Omega^1_{\Sigma/k} \cong \bigoplus_{i=1}^{g} L_i$, where $\dim_k L_i = 1$ and the G–action on L_i factors through a projection $G \xrightarrow{\theta_i} \mathbb{Z}/q^{s_i} \cong \langle \zeta_i \rangle$, where ζ_i is a primitive q^{s_i}–th root of unity. Thus, we have a basis $T = \{t_1, \ldots, t_g\}$ of G–invariant differential one–forms on which $(\zeta_j, t_j) \longrightarrow \zeta_j^{n_j} \cdot t_j$ where $n_j \not\equiv 0 (\mathrm{mod}\ q^{s_j})$ and $q^{s_i} > 1$ since the action of G on Σ is not trivial. At least one element of T, say t_1, must not vanish at x_0. Since the degree of the divisor (t_1) is $2g-2 > 0$, t_1 must vanish at some point $y \neq x_0$. Let $\varphi : \Sigma \longrightarrow \Sigma$ be the isomorphism which represents the generator of $\mathbb{Z}/q^{s_1} \cong \theta_1(G)$ so that $\varphi^* t_1 = \zeta^{n_1} \cdot t_1$. Let $y_1 = f^{-1}(y) \in G(y) \equiv$ orbit of y. Then $t_1(y_1) = t_1(f^{-1}(y)) \overset{\mathrm{def}}{\equiv} (f^* t_1)(y) = \zeta^{n_1} \cdot t_1(y) = 0$, and we conclude that the order of vanishing of t_1 at all points of the orbit of y are the same. Hence, the degree of the divisor (t_1) is divisible by $\gcd\left\{ \left| \frac{G}{G_y} \right| : t_1(y) = 0 \right\} \equiv 0 \ (\mathrm{mod}\ q)$. It follows that $2g-2 \equiv 0 \ (\mathrm{mod}\ q)$, contradicting the conclusion of the Hurwitz formula above. This contradiction proves the theorem. □

Section Three. In this section we discuss some consequences of the main theorem as well as the case of p–group actions on varieties in characteristic p, where a scheme–theoretic version of Corollary 2.2 is valid. As before, let k be algebraically closed of characteristic p, and let X be an affine k–scheme with coordinate ring $k[X]$. The fixed–point scheme X^G is the closed subscheme defined by the ideal $I = \{f^g - f \mid g \in G, f \in k[X]\}$. Thus, the k–algebra $R := k[X]/I$ is the largest quotient of $k[X]$ on which G acts trivially, and $X^G = \mathrm{Spec}(R)$.

3.1. Theorem. Let X be an irreducible k–scheme of positive dimension on which a finite p–group G acts by k–isomorphisms. Then the fixed–point scheme X^G cannot consist of an isolated point, i.e. $X^G \neq \mathrm{Spec}(k)$.

3.2 Corollary. Let G be a finite group of prime power order acting on a complete non–singular algebraic variety V defined over an algebraically closed field of arbitrary characteristic. Then V^G cannot consist of an isolated point, i.e. $V^G \neq \mathrm{Spec}(k)$.

The above corollary follows from 3.1 and Corollary 2.2.

Proof of 3.1. We may assume $X^G(k) \neq \phi$. Let $x_0 \in X^G(k)$, and let U be an affine open neighborhood of x_0. Then $U_0 := \bigcap_{g \in G} gU$ is a G–invariant affine open neighborhood of x_0, and we may prove the theorem for U_0. Therefore, we may assume that X is affine. Let m be the maximal ideal of the local ring $\mathcal{O}_{X,x_0}$, and consider the finite dimensional k–vector space m/m^2 on which G acts linearly. Since G is a p–group and $\mathrm{char}(k) = p$, there is a non–zero vector

$\alpha_0 \in (m/m^2)^*$ which is fixed under G . The pair consisting of the closed point x_0 and the non–zero tangent vector α_0 at x_0 which is fixed under G is equivalent to a surjective k–homomorphism $R \longrightarrow k[\varepsilon]/(\varepsilon^2)$, where $\mathrm{Spec}(R) = X^G$ as discussed above. Therefore $\mathrm{Spec}(R) \neq \mathrm{Spec}(k)$ as claimed. □

A version of 3.1 has been proved for unipotent actions in a different context by Meyer–Oberst [13].

As pointed out in the Introduction, the case $k = \mathbb{C}$ implies that if a complete variety X has a G–action with X^G = one point , then the link of the singularity at the fixed point X^G is not (mod q)–homology equivalent to a sphere, provided that $X - X^G$ is regular.

3.3. Corollary. Suppose $k = \mathbb{C}$ and X is a complete variety on which G (as in Theorem 2.1) acts with $X^G = \{x_0\}$. Suppose that X is non–singular in the complement of x_0 . Then the link of the singularity at x_0 is not (mod q)–homology equivalent to a sphere.

Proof: According to Hironaka [10], X is triangulable, and we may choose x_0 to be a vertex of an underlying symplicial structure. Further, by triangulating the orbit space X/G , we may assume that G acts simplicialy on X . Passing to the second barycentric subdivision, results in a G–CW–structure for X . Therefore the cellular chain complex $C_*(X)$ becomes a finite–dimensional permutation G–chain complex (cf. Assadi [1] Ch. I). If the link of the singularity at x_0 is a (mod q)–homology sphere, then X becomes a (mod q)–homology manifold, and consequently, the permutation G–chain

complex $C_*(X) \otimes \mathbb{F}_q$ satisfies duality. According to the construction, in the G–sets providing permutation bases for $C_i(X)$, only x_0 has isotropy subgroup G. But this contradicts Browder's Theorem [6] (see the Introduction).

In the same direction, the combination of Theorem 2.1 above, Browder [6], and Hironaka's triangulation Theorem [10] yields the following:

3.4. Corollary. Suppose $k = \mathbb{C}$, and X is a complete variety and G acts on X as in Theorem 2.1 above with X^G = one point. Then the underlying topological space of X in the analytic (i.e. Euclidean) topology does not satisfy Poincarè duality with mod q coefficients (and hence $\mathbb{Z}$–coefficients). □

Note: (1) When $G = (\mathbb{Z}/q)^r$, then we can also apply Assadi [2] [3] in conjunction with Hironka's result [10] to obtain this special case of Corollaries 3.3 and 3.4 above. This was the original form of 3.3 and 3.4 in the first version of this paper. We would like to thank Bill Browder for communicating his results to us, as well as bringing to our attention the following result of G. Bredon [14]. Bredon has shown that if $G = \mathbb{Z}/p$ acts on a connected finite Poincaré complex X of positive formal dimension, then X^G cannot be mod p acyclic. Thus, for $G = \mathbb{Z}/p$, Brendon's Theorem also implies 3.3 and 3.4.

To point out a concrete example confirming the above results, we consider an example of a complex projective surface X on which the group $G = \mathbb{Z}/p$ acts with only one fixed point. The link of this point is a rational homology sphere, in fact the 3–dimensional classical Lens space $L^3(\mathbb{Z}/5)$, which is not a $(\mathbb{Z}/5)$ – homology sphere.

3.5. Example. Let X be the quintic hypersurface in $\mathbb{P}^3(\mathbb{C})$ given by the equation $x_1^5 + x_2^5 + x_3^5 + x_1x_2x_4^3 = 0$ where (x_1,x_2,x_3,x_4) are the homogeneous coordinates of $\mathbb{P}^3(\mathbb{C})$. The action of $\mathbb{Z}/5$ on $\mathbb{P}^3$ is given by $(\varepsilon,x_i) \longmapsto \varepsilon^i x_i$ where ε is a fifth root of unity generating $\mathbb{Z}/5$. As one computes easily, X is invariant under $\mathbb{Z}/5$ and of the four fixed points in $\mathbb{P}^3$, exactly one point lies in X , namely $P = (0,0,0,1)$. At P , X is analytically isomorphic to the affine hypersurface $xy = z^5$ near the origin, by the Morse Lemma. This is a rational double point of type A_4 and it is a quotient $\mathbb{C}^2/(\mathbb{Z}/5)$ where $\mathbb{Z}/5$ acts by $(\varepsilon,(s,t)) \longmapsto (\varepsilon s,\varepsilon^4 t)$. Here, $x = s^5$, $y = t^5$, $z = st$. On the other hand, X is nonsingular at any point different from P . Thus, the link of the singularity is the classical lens space $L^3(1,4)$ with fundamental group $\mathbb{Z}/5$ which is a rational homology sphere, but not a $(\mathrm{mod}\ 5)$ – homology sphere. In particular, X does not satisfy Poincaré duality with $(\mathbb{Z}/5)$ – coefficients, although it is a rational Poincaré complex.

Finally, it appears that the analogues of Corollary 2.3 and 2.4 for varieties defined over fields of positive characteristic remain true when we formulate them in terms of local cohomology.

REFERENCES

[1] Assadi, A.: "Finite Group Actions on Simply–Connected Manifolds and CW Complexes", Memoirs A.M.S. No. 256 (1982).

[2] Assadi, A.: "An Algebraic Invariant for Finite Group Actions and Applications" (Submitted).

[3] Assadi, A.: "An Algebraic Variation on a Theorem of Atiyah–Bott" (Preprint ICTP 1988).

[4] Atiyah, M.F. – Bott, R.: "A Lefschetz Fixed Point Formula for Elliptic Complexes: II. Applications", Ann. Math. 88 (1968), 451–491.

[5] Bredon, G.: "Fixed Point Sets of Actions on Poincaré Duality Spaces", Topology 12 (1973) 159–175.

[6] Browder, W.: "Pulling Back Fixed Points", Inven. Math. 87 (1987), 331–342.

[6a] Browder, W.: "Actions of Elementary Abelian p–Groups" Topology 1989.

[7] Browder, W.: (to appear).

[8] Conner, P.E. – Floyd, E.E.: "Differentiable Periodic Maps", Ergeb. Math., Springer–Verlag 1964.

[9] Conner, P.E. – Floyd, E.E.: "Maps of Odd Period", Ann. Math. 84 (1966), 132–156.

[10] Curtis, C. – Reiner, I.: "Methods of Representation Theory Vol. I", Prentice Hall (1981).

[11] Ewing, J. – Stong, R.: "Group Actions Having One Fixed Point", Math. Z. 191 (1986) 159–164.

[12] Hartshorne, R.: "Algebraic Geometry" GTM 52 Springer–Verlag (1987).

[13] Hironka, H.: "Triangulations of Algebraic Sets" in Algebraic Geometry, Arcata 1974, A.M.S. Proc. Symp. Pure Math. 29 (1975), 165–184.

[14] Meyer, H.M. – Oberst, U.: "Fixpunkt– und Struktursätze für affine algebraische Gruppenschemata in Charakteristik p ", Math. Ann. 227, 67–96 (1977).

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 $\mathrm{End}(\phi) \underset{A}{\otimes} K$ (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 $\deg: A \longrightarrow \mathbb{N}$ (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 $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$, $\bar{L}$ 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 $\mathrm{End}(\phi)$ 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 $n/r \cdot d_\infty$ at ∞ with respect to the field K_∞.

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

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

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

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

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

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

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 $\mathfrak{p} = \mathrm{char}(L)$ 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 $\mathfrak{p}$. $\mathrm{End}(\phi) \otimes K$ 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 $\mathrm{nr} : \mathrm{End}(\phi) \otimes K \longrightarrow E$ 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 $\mathfrak{w}$–adic valuation. The proportionality factor comes out by evaluating on $u = \phi_a$, $a \in A$.

For each prime $\mathfrak{q} \neq \mathfrak{p}$ 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 $u \circ \mathfrak{N} \circ u^{-1} \subset \mathrm{End}(\psi)$.

(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

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

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 $\mathfrak{p}$, and r a very high power of q. We calculate the q–part of $(N(u))$:

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

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

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

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

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

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

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 $\mathfrak{p}$. Comparing τ–degrees yields $(f) = \mathfrak{p}^{m/r}$. (Recall that $m = [L : \mathbb{F}_p]$.) We denote by $\phi_{\mathfrak{p}}$ the isogeny from ϕ to ϕ^u associated with the left ideal $u = \mathrm{End}(\phi)\mathfrak{p} \subset \mathrm{End}(\phi)$. Then $\ker(\phi_{\mathfrak{p}}) = {}_{\mathfrak{p}}\phi$.

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) $\phi_{\mathfrak{p}}$ is purely inseparable.

Proof: The equivalence of a) and b) comes from Thm. 2.9. By the preceding, b) says ${}_{\mathfrak{p}^{m/r}}\phi$, thus ${}_{\mathfrak{p}}\phi$ is local, which means that $\phi_{\mathfrak{p}}$ is purely inseparable. Conversely, let $\phi_{\mathfrak{p}}$ be purely inseparable. Then ${}_{\mathfrak{p}}\phi(\bar{L}) = 0$, and also ${}_{\mathfrak{p}^i}\phi(\bar{L}) = 0$, all i. If $\mathfrak{p}^i = (f)$ 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 $\mathfrak{p}$ 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 $\mathfrak{p}$ 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 $\mathfrak{p}$ 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 $(f) = \mathfrak{p}^{m_0}$, 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 $\Sigma(r,\mathfrak{p})$ of isomorphism classes of supersingular rank r Drinfeld modules in characteristic $\mathfrak{p}$.

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 $D = D(r,\mathfrak{p})$ be the central divison algebra of degree r^2 over K with invariants $1/r$, $-1/r$ at $\mathfrak{p}$, ∞, 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 $\mathfrak{p}$ a prime of degree d. The number of supersingular isomorphism classes of rank 2 D. modules in characteristic $\mathfrak{p}$ is given by

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

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

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

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

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

where $\mathfrak{p}(T)$ is the monic polynomial that generates $\mathfrak{p}$. 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 $\#(\Sigma(2,\mathfrak{p}))$ (= class number of $D(2,\mathfrak{p})$) 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 types (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 $\mathrm{End}(\phi) \xrightarrow{\sim} \mathrm{End}(\psi)$ for $\psi = \phi^u$. The next proposition gives necessary conditions for endomorphism rings to be isomorphic.

4.6. Proposition: 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 $G = \mathrm{Gal}(\overline{\mathbb{F}}_p : \mathbb{F}_p)$.

Proof: Clearly, applying $\sigma \in G$ to the coefficients of $f \in \mathrm{End}(\phi)$ defines an isomorphism $\mathrm{End}(\phi) \xrightarrow{\sim} \mathrm{End}(\psi)$, 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 $\sigma = \text{const} \cdot \tau^{id}$, and, possibly replacing ψ by an isomorphic module, we may assume $\sigma = \tau^{id}$. 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, $\mathrm{nr}(u_s) = n(u_s)$ 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

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

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) $(P(0)) = \mathfrak{p}^m$.

(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 $\mathfrak{p}$ 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

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

where $t_\mathfrak{q} = p^{-m(\mathfrak{q}) \cdot s}$, $m(\mathfrak{q}) = [B/\mathfrak{q} : A/\mathfrak{p}]$, and the factors $Q_\mathfrak{q}$ are constructed from the reductions of ϕ mod $\mathfrak{q}$. 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

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

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" $\mathbb{F}_p = A/\mathfrak{p}$. Write $p(T)$ for the monic generator of $\mathfrak{p}$, 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., $\mathbb{F}_q \xrightarrow{\simeq} \mathbb{F}_p$. 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