Available online at www.sciencedirect.com

ScienceDirect

C. R. Acad. Sci. Paris, Ser. I 346 (2008) 305–308

COMPTES RENDUS MATHEMATIQUE

http://france.elsevier.com/direct/CRASS1/

Algebraic Geometry

The A-module structure induced by a Drinfeld A-module of rank 2 over a finite field

Mohamed-Saadbouh Mohamed-Ahmed

Département de mathématiques, Université du Maine, avenue Olivier-Messiaen, 72085 Le Mans cedex 9, France

Received 13 March 2006; accepted after revision 15 January 2008

Available online 12 February 2008

Presented by Gérard Laumon

Abstract

Let $\mathbf{F}_q$ be a finite field and let $L/\mathbf{F}_q$ be a finite extension. Let $\mathbf{F}$ be the Frobenius of L ($\mathbf{F}: x \mapsto x^{\#L}$) and let (P) be the $\mathbf{F}[T]$-characteristic of $\mathbf{F}$. Let m be the degree of the extension $L/\mathbf{F}_q[T]/(P)$. There exists then $c \in \mathbf{F}_q[T]$ and $\mu \in \mathbf{F}_q$ such that the characteristic polynomial $P_\mathbf{F}$ of $\mathbf{F}$ is equal to $P_\mathbf{F}(X) = X^2 - cX + \mu P^m$. Our main result is an analogue of Deuring's Theorem on elliptic curves: let $M = \frac{\mathbf{F}_q[T]}{(i_1)} \oplus \frac{\mathbf{F}_q[T]}{(i_2)}$, where i_1 and i_2 are two polynomials of $\mathbf{F}_q[T]$ such that $i_2 \mid i_1$ and $i_2 \mid (c-2)$, there exists an ordinary Drinfeld $\mathbf{F}_q[T]$-module Φ of rank 2 over L such that the structure of the finite $\mathbf{F}_q[T]$-module L^Φ induced by Φ over L is isomorphic to M. ***To cite this article: M.-S. Mohamed-Ahmed, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

La structure de A-module induite sur un A-module de Drinfeld de rang 2 sur un corps fini. Soit $\mathbf{F}_q$ un corps fini et $L/\mathbf{F}_q$ une extension finie. Soit $\mathbf{F}$ le Frobenius de L ($\mathbf{F}: x \mapsto x^{\#L}$) et (P) la $\mathbf{F}[T]$-caractéristique de $\mathbf{F}$. Soit m le degré de l'extension $L/\mathbf{F}_q[T]/(P)$. Il existe alors $c \in \mathbf{F}_q[T]$ et $\mu \in \mathbf{F}_q$ tels que le polynôme caractéristique $P_\mathbf{F}$ de $\mathbf{F}$ soit égal à $P_\mathbf{F}(X) = X^2 - cX + \mu P^m$. Notre résultat principal est un parfait analogue du théorème de Deuring pour les courbes elliptiques : soit $M = \frac{\mathbf{F}_q[T]}{(i_1)} \oplus \frac{\mathbf{F}_q[T]}{(i_2)}$, où i_1 et i_2 sont deux polynômes de $\mathbf{F}_q[T]$ tels que $i_2 \mid i_1$ et $i_2 \mid (c-2)$. Il existe alors un $\mathbf{F}_q[T]$-module de Drinfeld Φ ordinaire de rang 2 sur L tel que la structure du $\mathbf{F}_q[T]$-module fini L^Φ induite par Φ sur L soit isomorphe à M. ***Pour citer cet article : M.-S. Mohamed-Ahmed, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

1. Introduction

Let K be a global field of characteristic p (namely a rational function field of one indeterminate over a finite field $\mathbf{F}_q$ with p^s elements). We fix a place of K, denoted by ∞, and we call A the ring of elements regular away from the place ∞. Let L be a commutative field of characteristic p, $\gamma : A \to L$ be a morphism of rings. The kernel of this

E-mail address: mohamedsaadbouh@yahoo.fr.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.01.012

morphism is denoted by the principal ideal (P). We put $m=[L,\ A/P]$ (the extension degree of L over A/P) and $d=\deg P$.

Let τ be the Frobenius of $\mathbf{F}_q$ ($\tau : x\mapsto x^q$). We denote by $L\{\tau\}$ the ring of polynomials in τ (namely the ring of Ore's polynomials) with the usual addition and the product given by the commutation rule $\tau\lambda=\lambda^q\tau$ for all $\lambda\in L$. A Drinfeld A-module $\Phi : A\to L\{\tau\}$ is a morphism of rings of A into $L\{\tau\}$ such that for all $a\in A$ non-invertible (i.e. $a\notin \mathbf{F}_q^*$) we have $\deg_\tau \Phi_a>0$ and for all $a\in A$, there exists a rational number r such that $\deg_\tau \Phi_a=r\deg a(\deg a=\dim_{\mathbf{F}_q}\frac{A}{a.A})$. This number r is called the rank of Φ. The morphism Φ defines an A-module structure over the field L, noted L^Φ, where the name of a Drinfeld A-module for a morphism Φ. This structure of A-module depends on Φ and, especially, on its rank (see [1,4,2]).

Let Φ be a Drinfeld A-module of rank 2 over a finite field L and let $P_\Phi(X)$ be its characteristic polynomial. J.-K. Yu [8] proved that, for an ordinary Drinfeld modules of rank 2, $P_F(X)=X^2-cX+\mu P^m$ where $\mu\in\mathbf{F}_q^*$, $c\in A$ and $\deg c\leqslant \frac{m.d}{2}$, which is the Hasse–Weil analogy, in this case. Let χ be the Euler–Poincaré characteristic of A (i.e. an ideal of A). We can consider the ideal $\chi(L^\Phi)=(P_{\mathbf{F}}(1))$, denoted henceforth by χ_Φ, which is by definition a divisor of A corresponding for the elliptic curves to the number of points of the variety over their base field.

We will be interested in Drinfeld A-module structures L^Φ of rank 2 and we will prove that for an ordinary Drinfeld $\mathbf{F}_q[T]$-module, this structure is always the sum of two cyclic and finite $\mathbf{F}_q[T]$-modules: $\frac{A}{(i_1)}\oplus\frac{A}{(i_2)}$ where (i_1) and (i_2) are two ideals of A such that $i_2\mid i_1$. Let $P_F(X)$ the characteristic polynomial of Φ. We will show that $\chi_\Phi=(P_{\mathbf{F}}(1))=(i_1)(i_2)$, so if we put $i=\gcd(i_1,i_2)$, then $i^2\mid P_F(1)$. We give a following analogy of Deuring's theorem for elliptic curves:

Theorem 1.1. *Let $c\in A$, and $M=\frac{A}{(i_1)}\oplus\frac{A}{(i_2)}$ where i_1, i_2 are two polynomials of A such that $i_2\mid i_1$ and $i_2\mid(c-2)$. Then there exists an ordinary Drinfeld A-module Φ over L, of rank 2, such that the coefficient of X in $P_\Phi(X)$ is $-c$ and $L^\Phi\simeq M$.*

We first recall Deuring's theorem for elliptic curves (see [3]):

Theorem 1.2 *(Deuring's Theorem). Let $M=\begin{pmatrix} c-1 & -A\\ B & 1\end{pmatrix}\in\mathcal{M}_{2\times2}(\mathbb{Z}/N\mathbb{Z})$ and q be a power of a prime number. If we suppose that $|c|\leqslant 2.\sqrt{q}$, $B\mid A$, $B\mid c-2$, $A.B=N:=q+1-c$ and $(c,q)=1$, then there exists an ordinary elliptic curve E over $\mathbf{F}_q$ such that $E(\mathbf{F}_q)\simeq\mathbb{Z}/A\oplus\mathbb{Z}/B$.*

2. Structure of the A-module L^Φ

A Drinfeld A-module of rank 2 has the form (if an isomorphism $A\simeq\mathbf{F}_q[T]$ and $K\simeq\mathbf{F}_q(T)$ is chosen) $\Phi(T)=a_1+a_2\tau+a_3\tau^2$, where $a_i\in L$, $1\leqslant i\leqslant 2$ and $a_3\in L^*$. Let Φ and Ψ be two Drinfeld modules over an A-field L. A morphism from Φ to Ψ over L is an element $p(\tau)\in L\{\tau\}$ such that $p\Phi_a=\Psi_a p$, for all $a\in A$. A non-zero morphism is called an isogeny. We note that this is possible only between two Drinfeld modules of the same rank. The set of all morphisms forms an A-module denoted by $\mathrm{Hom}_L(\Phi,\Psi)$.

In particular, if $\Phi=\Psi$ the L-endomorphism ring $\mathrm{End}_L\,\Phi=\mathrm{Hom}_L(\Phi,\Phi)$ is a subring of $L\{\tau\}$ and an A-module which contains $\Phi(A)$. Let $\bar L$ be a fix algebraic closure of L and (P) the A-characteristic of L. $\Phi_a(\bar L):=\Phi[a](\bar L)=\{x\in\bar L,\Phi_a(x)=0\}$ and $\Phi_{(P)}(\bar L)=\bigcap_{a\in(P)}\Phi_a(\bar L)$. We say that Φ is supersingular if the A-module constituted by a (P)-division points $\Phi_{(P)}(\bar L)$ is trivial, otherwise Φ is said to be an ordinary module (see [4]). We have the following result about the A-module structure of L^Φ:

Proposition 2.1. *The Drinfeld A-module Φ gives a finite A-module L^Φ which is isomorphic to $\frac{A}{(i_1)}\oplus\frac{A}{(i_2)}$ where (i_1) and (i_2) are two ideals of A such that $\chi_\Phi=(i_1)(i_2)$.*

Proof. The A-module Φ induces a finite A-module structure L^Φ of the same rank than Φ over the finite field L. Since Φ is of rank 2, L^Φ is also of rank 2. Let i_1, i_2 be two unitary polynomials in A such that $L^\Phi=\frac{A}{(i_1)}\oplus\frac{A}{(i_2)}$. We know that L^Φ is included in or equal to $\Phi(\chi_\Phi)\simeq\frac{A}{\chi_\Phi}\oplus\frac{A}{\chi_\Phi}$. Since the Euler–Poincaré characteristic χ is multiplicative on exact sequences, we have $\chi_\Phi=(i_1)(i_2)$.

Let $i = \gcd(i_1, i_2)$. It is clear, by the Chinese lemma, that the non-cyclicity of the A-module L^{Φ} impose (i_1) and (i_2) to be not coprime, which means that $i \neq 1$ and implies that $i^2 \mid P_{\Phi}(1)$ (because $\chi_{\Phi} = (P_F(1)) = (i_1)(i_2)$). □

In the rest of this Note, we suppose that $i_2 \mid i_1$ ($i_2 \notin \mathbf{F}_q^*$), otherwise L^{Φ} is a cyclic A-module and it can be written on the form A/χ_{Φ}. Let be $c \in \mathbf{F}_q[T]$ and $\mu \in \mathbf{F}_q$ such that $P_F(X) = X^2 - cX + \mu P^m$.

Proposition 2.2. *If $L^{\Phi} \simeq \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$, then $i_2 \mid c - 2$.*

Proof. We know that the A-module structure L^{Φ} is stable by the endomorphism Frobenius F of L. We choose a basis for A/χ_{Φ} for which the A-module L^{Φ} is generated by $(i_1, 0)$ and $(0, i_2)$ and we consider $M_F = \begin{pmatrix} a & b \\ a_1 & b_1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(A/\chi_{\Phi})$ the matrix of F according to this basis.

Now, since $\operatorname{Tr} M_F = a + b_1 = c$, $M_F((i_1, 0)) = (i_1, 0)$ and $M_F((0, i_2)) = (0, i_2)$, we have $a \cdot i_1 \equiv i_1 (\mathrm{mod}\ \chi_{\Phi})$ implying that $a - 1$ is divisible by i_1. Similarly, since $b_1 \cdot i_2 \equiv i_2 (\mathrm{mod}\ \chi_{\Phi})$ implying that $b_1 - 1$ is divisible by i_2. It follows that $c - 2 = a - 1 + b_1 - 1$ is divisible by i_2 (since we always have $i_2 \mid i_1$). □

Let (ρ) be a prime ideal of A, different from the A-characteristic (P). We define the finite A-module $\Phi((\rho))$ as being the A-module $(A/(\rho))^2$.

Let g be an ideal of A, F be the Frobenius of L and $O_{K(F)}$ the maximal A-order in $K(F)$. The discriminant of the A-order $A + g.O_{K(F)}$ is $\Delta.g^2$, where Δ is the discriminant of the characteristic polynomial $P_F(X) = X^2 - cX + \mu P^m$. So each order is defined by its discriminant and will be noted by $O(disc)$ (see [6,7,5]). According to Proposition 2.2, the inclusion $\Phi((\rho)) \subset L^{\Phi}$ implies clearly that $\rho^2 \mid P_{\mathbf{F}}(1)$ and $(\rho) \mid c - 2$. We have the following:

Proposition 2.3. *Let Φ be an ordinary Drinfeld A-module of rank 2 and let (ρ) be an ideal of A, different from the A-characteristic (P) of L, such that $\rho^2 \mid P_F(1)$ and $\rho \mid c - 2$. Then the inclusion $\Phi((\rho)) \subset L^{\Phi}$ holds if and only if we have $O(\Delta/\rho^2) \subset End_L \Phi$.*

To prove this proposition we need the following lemma:

Lemma 2.4. *The assertion $\Phi((\rho)) \subset L^{\Phi}$ is equivalent to the assertion $\frac{F-1}{\rho} \in \mathrm{End}_L \Phi$.*

Proof. Since L^{Φ} is stable by the isogeny F, $L^{\Phi} = \mathrm{Ker}(F - 1)$. Next, by definition we have $\Phi((\rho)) = \mathrm{Ker}((\rho))$. It follows, according to Theorem 4.7.8 of [4], that the inclusion $\Phi((\rho)) \subset L^{\Phi}$ holds if and only if there exists $g \in \mathrm{End}_L \Phi$ such that $F - 1 = g.\rho$, that is $\frac{F-1}{\rho} \in \mathrm{End}_L \Phi$, confirming the lemma. □

Proof of Proposition 2.3. Let $N(\frac{F-1}{\rho})$ denote the norm of the isogeny $\frac{F-1}{\rho}$ which is a principal ideal generated by $\frac{P_{\Phi}(1)}{(\rho)^2}$ and let Tr be the trace of the same isogeny which is equal to $\frac{c-2}{\rho}$. Then the discriminant of the A-module $A[\frac{F-1}{\rho}]$ is given by $\operatorname{disc} A([\frac{F-1}{\rho}]) = \mathrm{Tr}(\frac{F-1}{\rho})^2 - 4N(\frac{F-1}{\varrho}) = \frac{c^2 - 4\mu P^m}{\rho^2} = \Delta/\rho^2$, implying the required inclusion.

Now assume that $O(\Delta/\rho^2) \subset \mathrm{End}_L \Phi$ and prove that $\Phi(\rho) \subset L^{\Phi}$. The order corresponding of the discriminant Δ/ρ^2 is $A[\frac{F-1}{\rho}]$, which means that $\frac{F-1}{\varrho} \in \mathrm{End}_L \Phi$ and we conclude (by using Lemma 2.4) that $\Phi((\rho)) \subset L^{\Phi}$. The proof is complete. □

Corollary 2.5. *If $O(\Delta/\rho^2) \subset \mathrm{End}_L \Phi$, then L^{Φ} is not cyclic.*

Proof. Since $\Phi((\rho))$ is not cyclic (by construction) and since the non-cyclicity of the A-module L^{Φ} is equivalent to have $\Phi((\rho)) \subset L^{\Phi}$, the corollary follows from Proposition 2.3. □

Now, we are able to prove the following theorem:

Theorem 2.6. *Let $M = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$ be a A-module such that $i_2 \mid i_1$, $i_2 \mid (c - 2)$. Then there exists an ordinary Drinfeld A-module Φ over L of rank 2 such that $L^{\Phi} \simeq M$.*

Proof. Let us denote by Φ the Drinfeld A-module for which the characteristic of Euler–Poincaré is given by $\chi_\Phi = (i_1).(i_2)$ and having as endomorphisme ring $O(\Delta/i_2^2)$ (where Δ always denotes the discriminant of the characteristic polynomial of the Frobenius F). Since (by construction) $O(\Delta/(i_2^2)) \subset \mathrm{End}_L \Phi$, then Proposition 2.3 (applied with $\rho = i_2$) implies $\Phi(i_2) \simeq (A/i_2)^2 \subset L^\Phi$. However, since on other hand $L^\Phi \subseteq \Phi(\chi_\Phi) \simeq \frac{A}{\chi_\Phi} \oplus \frac{A}{\chi_\Phi}$, it finally follows that $L^\Phi = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$. The theorem is proved. □

We end this Note by conjecturing the following:

Conjecture 2.7. *Let L be a finite field, and $M \in \mathcal{M}_{2\times 2}(A/\chi_\Phi)$ and $\overline{P} = P$* (mod χ_Φ). *Suppose that* ($\det M = \overline{P}^m$, $\mathrm{Tr}(M) = c$ *and* $c \nmid P$. *Then there exists an ordinary Drinfeld A-module over L, of rank* 2, *for which the associated Frobenius matrix M_F is equal to M.*

Note that the Theorem 2.6 is an immediate consequence of Conjecture 2.7. Indeed, it suffices to apply the conjecture to the matrix $M = \begin{pmatrix} c-1 & i_1 \\ i_2 & -1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(A/\chi_\Phi)$.

References

[1] B. Angles, One some subring of Ore polynomials connected with finite Drinfeld modules, J. Algebra 181 (2) (1996) 507–522.
[2] V.G. Drinfeld, Elliptique modules, Math. USSR Sb. 94 (136) (1974) 594–627, 656.
[3] M. Deuring, Die Typen der Multiplikatorenringe Ellipticher Funktionenkorper, Abh. Math. Sem. Univ. Hamburg 14 (1941) 197–272.
[4] D. Goss, Basic Structures of Function Field Arithmetic, A Series of Modern Surveys in Mathematics, vol. 35, Springer, 1996.
[5] I. Reiner, Maximal Orders, Academic Press, 1975.
[6] R. Shoof, Nonsingular plane cubic curves over finite fields, J. Combinatory Theory Ser. A 46 (1987) 183–211.
[7] M.A. Tsfasman, S.G. Vladut, Algebraic-Geometric Codes, Math. Appl., Kluwer, Dordrecht, 1991.
[8] J.-K. Yu, Isogenis of Drinfeld modules over finite fields, J. Number Theory 54 (1) (1995) 161–171.