Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 343 (2006) 737–740
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Algebraic Geometry

# Endomorphism rings and isogenies classes for Drinfeld $A$-modules of rank 2 over finite fields

Mohamed-Saadbouh Mohamed-Ahmed

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

Received 1 March 2006; accepted after revision 27 October 2006

Available online 1 December 2006

Presented by Christophe Soulé

**Abstract**

For a Drinfeld module of rank 2, we discuss many analogy points with elliptic curves. More precisely, we study the characteristic polynomial of a Drinfeld module of rank 2 and use it to calculate the number of isogeny classes for such modules. ***To cite this article: M.-S. Mohamed-Ahmed, C. R. Acad. Sci. Paris, Ser. I 343 (2006).***


**Résumé**

**Anneaux d'endomorphismes et classes d'isogénies de modules de Drinfeld de rang 2 sur un corps fini.** Pour un module de Drinfeld de rang 2, on étudie plusieurs points d'analogie avec les courbes elliptiques. Plus précisément, on étudie la charactéristique polynômiale d'un module de Drinfeld de rang 2 et en l'utilisant, on calcule le nombre de classes d'isogénies d'un module de Drinfeld de rang 2 sur un corps fini. ***Pour citer cet article : M.-S. Mohamed-Ahmed, C. R. Acad. Sci. Paris, Ser. I 343 (2006).***


## 1. Introduction

Let $K$ be a non-empty global field of characteristic $p$ (namely a rational functions field of one indeterminate over a finite field) together with a constant field, the finite field $\mathbf{F}_q$ with $p^s$ elements. We fix one place of $K$, denoted by $\infty$, and call $A$ the ring of regular elements away from the place $\infty$. Let $L$ be a commutative field of characteristic $p$, $\gamma : A \to L$ be a ring $A$-homomorphism. The kernel of this $A$-homomorphism is denoted by $P$. We put $m = [L,\ A/P]$, the extension degrees of $L$ over $A/P$.

We denote by $L\{\tau\}$ the Ore polynomial ring, namely, the polynomial ring of $\tau$, where $\tau$ is the Frobenius of $\mathbf{F}_q$ with the usual addition and where the product is given by the commutation rule: for every $\lambda \in L$, we have $\tau\lambda = \lambda^q\tau$. A Drinfeld $A$-module $\Phi : A \to L\{\tau\}$ is a non-trivial ring homomorphism and a non-trivial embedding of $A$ into $L\{\tau\}$ different from $\gamma$. This homomorphism $\Phi$, once defined, defines an $A$-module structure over the $A$-field $L$, noted $L^{\Phi}$, where is come the name of a Drinfeld $A$-module for a homomorphism $\Phi$. This structure of $A$-module depends on $\Phi$ and, especially, on his rank.

*E-mail address:* mohamed-saadbouh.mohamed-ahmed@univ-lemans.fr (M.-S. Mohamed-Ahmed).

1631-073X/$ – see front matter 
doi:10.1016/j.crma.2006.10.026

Let $\chi$ be the Euler–Poincaré characteristic (i.e. it is an ideal from $A$). So we can speak about the ideal $\chi(L^{\Phi})$, denoted henceforth by $\chi_{\Phi}$, which is by definition a divisor of $A$, corresponding for the elliptic curves to a number of points of the variety over their base field. In this paper, we will work on the special case $K = \mathbf{F}_q(T)$, $A = \mathbf{F}_q[T]$. Let $P_{\Phi}(X)$ be the characteristic polynomial of the $A$-module $\Phi$, which is also a characteristic polynomial of the Frobenius $F$ of $L$. We can prove that this polynomial can be given as: $P_{\Phi}(X) = X^2 - cX + \mu P^m$, such that $\mu \in \mathbf{F}_q^*$, and $c \in A$, where $\deg c \leqslant \frac{m.d}{2}$ by the Hasse–Weil analogue in this case. We will be interested in the endomorphism ring and the number of isogeny classes of Drinfeld $A$-modules of rank 2. For more information see [1,2,5], and [3].

### 1.1. The endomorphism ring

A Drinfeld $A$-module of rank 2 is of the form $\Phi(T) = a_1 + a_2\tau + a_3\tau^2$, where $a_i \in L$, $1 \leqslant i \leqslant 2$, and $a_3 \in L^*$. Let $\Phi$ and $\Psi$ be two Drinfeld modules over an $A$-field $L$. A morphism from $\Phi$ to $\Psi$ 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 having the same rank. The set of all morphisms between $\Phi$ and $\Psi$ forms an $A$-module denoted by $\mathrm{Hom}_E(\Phi, \Psi)$.

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 contained in $\Phi(A)$. Let $F$ be the Frobenius of $L$ we have: $\Phi\ (A) \subset \mathrm{End}_L \Phi$ and $F \in \mathrm{End}_L \Phi$.

Let $\bar{L}$ be a fix algebraic closure 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 $\Phi$ is supersingular if and only if the $A$-module constituted by a $P$-division points $\Phi_P(\bar{L})$ is trivial, otherwise $\Phi$ is said a ordinary module.

**Proposition 1.1.** *Let $P_{\Phi}(X) = X^2 - cX + \mu P^m$ be the characteristic polynomial of the Frobenius $F$ of a finite field $L$ and let $\Delta = c^2 - 4\mu P^m$ be the discriminant of $P_{\Phi}$, and $O_{K(F)}$ the maximal $A$-order of the algebra $K(F)$.*

(i) *For every $g \in A$ such that $\Delta = g^2.\omega$, there exists a Drinfeld $A$-module $\Phi$ over $L$ of rank 2 such that $O_{K(F)} = A[\sqrt{\omega}]$ and*: $\mathrm{End}_L \Phi = A + g.A[\sqrt{\omega}]$.
(ii) *If there no polynomial $g$ of $A$ such that $g^2$ divide $\Delta$, then there exists an ordinary Drinfeld $A$-module $\Phi$ over $L$ of rank 2 such that* $\mathrm{End}_L \Phi = O_{K(F)}$.

### 1.2. Isogeny classes

Let $\bar{K}$ be an algebraic closure of $K$ and let $\infty$ be a place of $K$ which divides $\frac{1}{T}$. Let us put $K_\infty = F_q((\frac{1}{T}))$ and denote by $\mathbb{C}_\infty$ the completude of the algebraic closure of $K_\infty$. We fix an embedding $\bar{K} \hookrightarrow \mathbb{C}_\infty$. For every $\alpha \in \mathbb{C}_\infty$, we denote by $|\alpha|_\infty$ the normalized valuation of $\alpha$ ($|\frac{1}{T}|_\infty = \frac{1}{q}$).

Let $\theta \in \bar{K}$, we say that $\theta$ is an ordinary number if:

(i) $\theta$ is integral over $A$;
(ii) $|\theta|_\infty = q^{md/2}$;
(iii) $K(\theta)/K$ is imaginary and $[K(\theta), K] = 2$;
(iv) there is only one place of $K(\theta)$ which divides $\theta$ and $\mathrm{Tr}_{K(\theta)/K}(\theta) \neq 0(P)$.

We say that $\theta$ is an ordinary Weil number if $\theta^\sigma$ is an ordinary number for all $\sigma \in \mathrm{col}(\bar{K}/K)$. We denote by $\mathrm{W}^{\mathrm{ord}}$ the set of conjugacy class of ordinary Weil numbers of rank 2. We have the important result, for a proof see [6]:

**Theorem 1.2.** *There exists a bijection between $W^{\mathrm{ord}}$ and isogeny classes of ordinary Drinfeld $A$-modules of rank 2 defined over $L$.*

Let $\theta$ be an ordinary Weil number. We put $P(x) = Hr(\theta, K; x)$. By using (1), (2), (3) and (4) we have $P(x) = x^2 - cx + \mu P^m$, where $\mu \in \mathbf{F}_q^*$ and $c \in A$ but $c \neq 0(P)$ and also $\deg_T c \leqslant \frac{md}{2}$. Let us put

$$\Gamma = \left\{ c \in A \text{ such that } c \neq 0(P) \text{ and } \deg_T c \leqslant \frac{md}{2} \right\}.$$

We need the following lemma:

**Lemma 1.3.** *For $\mu \in \mathbf{F}_q^*$, $c \in \Gamma$ denote by $E$ the filed of decomposition of $P(x) = x^2 - cx + \mu P^m$ over $K$. Let $\theta$ be a root of $P(x)$. Then $\theta$ verifies* (1), (2), (3) *and* (4) *together with* $[K(\theta), K] = 2$.

**Corollary 1.4.**

(1) *Let $\mu \in \mathbf{F}_q^*$ and $c \in \Gamma$ and let $\theta$ be a root of $x^2 - cx + \mu P^m$. Then $\theta$ is an ordinary Weil number if and only if $K(\theta)/K$ is imaginary.*
(2) *If $md \equiv 1(2)$, then the roots of $x^2 - cx + \mu P^m$ are Weil numbers for all $\mu \in \mathbf{F}_q^*$ and for all $c \in \Gamma$.*

To simplify, let us suppose $p \neq 2$ and put $md \equiv 0(2)$.

**Lemma 1.5.** *Let $\mu \in \mathbf{F}_q^*$ and $c \in \Gamma$ with $\deg_T c \leqslant \frac{md}{2}$. Let $\theta$ be a root of $x^2 - cx + \mu P^m$. Then $\theta$ is a Weil number if and only if $-\mu \notin (\mathbf{F}_q^*)^2$.*

**Lemma 1.6.** *Let $\mu \in \mathbf{F}_q^*$ and $c \in \Gamma$ with $\deg_T c = \frac{md}{2}$. Denote by $c_0$ the term of higher degree of $c$. We suppose that $c_0^2 \neq -4\mu$. Let $\theta$ be a root of $x^2 - cx + \mu P^m$. Then $\theta$ is a Weil number if and only if $x^2 - c_0 x + \mu$ is irreducible in $\mathbf{F}_q[X]$.*

The roots of the characteristic polynomial are a Weil numbers, so we need this result, for a proof see [6]:

**Proposition 1.7.** *Let $\Phi$ be a Drinfeld $A$-module of rank 2 over the finite field $L = \mathbf{F}_{q^n}$ and let $P$ be the characteristic of $L$. We put $m = [L : A/P]$ and $d = \deg P$. The characteristic polynomial $P_\Phi$ can take only the following forms*:

(i) *In the case of ordinary Drinfeld $A$-modules, we have $P_\Phi(X) = X^2 - cX + \mu P^m$, where $c^2 - 4\mu P^m$ is imaginary, $c \in A$, $(c, P) = 1$ and $\mu \in \mathbf{F}_q^*$.*
(ii) *In the case of supersingular $A$-modules, we distinguish three cases*:
   (a) *If $m$ is odd, then $P_\Phi(X) = X^2 + \mu P^m$, with $\mu \in \mathbf{F}_q^*$.*
   (b) *If $m$ is even and $d = \deg P$ is odd, then $P_\Phi(X) = X^2 + c_0 X + \mu P^m$, with $\mu \in \mathbf{F}_q^*$ and $c_0 \in \mathbf{F}_q$.*
   (c) *If $m$ is even, then $P_\Phi(X) = (X + \mu P^{\frac{m}{2}})^2$.*

We can recapitulate all the cases above as follows:

(i) For the ordinary case, the characteristic polynomial is of the form : $P_\Phi(X) = X^2 - cX + \mu P^m$, such that $2\deg c < \deg P.m$ or $2 \deg c = \deg P.m$ and $X^2 - a_0 X + \mu$ is irreducible over $\mathbf{F}_{q^n}$ where $a_0$ is the coefficient of the greatest degree of $c$. For the supersingular case, we have the two following cases:
(ii) The $\deg P$ is even or $-\mu \notin (\mathbf{F}_q^*)^2$.
(iii) The polynomial $X^2 + c_0 X + \mu$ is irreducible over $\mathbf{F}_q$.

We are in position to compute the number of characteristic polynomials which corresponds to the number of isogeny classes, for proof see [4].

**Lemma 1.8.** $\#\{$*Isogeny classes*$\} = \#\{P_\Phi\}$.

So we can compute the cardinal of the isogeny classes of Drinfeld modules of rank 2 as follows:

**Proposition 1.9.** *Let $\Phi$ a Drinfeld $A$-module of rank 2 over a finite field $L = F_{q^n}$ and let $P$ be the $A$-characteristic of $L$. We put $m = [L : A/P]$ and $d = \deg P$*:

(i) *If $m$ and $d$ are both odd, then* $\#\{P_\Phi\} = (q-1)(q^{[\frac{m}{2}d]+1} - q^{[\frac{m-2}{2}d]+1} + 1)$.

(ii) *If $m$ is even and $d$ is odd, then* $\#\{P_\Phi\} = (q-1)[\frac{q-1}{2} q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d+1} + q]$.

(iii) *If $m$ and $d$ are both even, then* $\#\{P_\Phi\} = (q-1)[\frac{q-1}{2} q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d} + 1]$.

*1.2.1. Euler–Poincaré characteristic*

Let $\Phi$ be a Drinfeld $A$-module of rank 2 over a finite field $L = \mathbf{F}_{q^n}$ and denote by $P_\Phi$ the characteristic polynomial. Let $\chi_\Phi = (P_\Phi(1))$. This is the Euler–Poincaré characteristic.

We can have an expression for the cardinal of the set of Euler–Poincaré characteristic as follows:

**Proposition 1.10.** *Let $\Phi$ be a Drinfeld $A$-module of rank 2 over the finite field $L = \mathbf{F}_{q^n}$, and let $P$ be the characteristic of $L$. We put $m = [L : A/P]$ and $d = \deg P$. There exists $H, B \in L$, such that $\#\{\chi_\Phi\} = H + B$, where $H$ and $B$ satisfies $\#\{P_\Phi\} = (q-1)H + (q-2)B$.*

The value of $\#\{\chi_\Phi\}$ can be deduced accordingly:

**Proposition 1.11.** *Let $\Phi$ be a Drinfeld $A$-module of rank 2 over a finite field $L = \mathbf{F}_{q^n}$ and let $P$ be the $A$-characteristic of $L$. We put $m = [L : A/P]$ and $d =$deg $P$. We have*:

(i) *If $m$ and $d$ are both odd, then* $\#\{\chi_\Phi\} = \frac{q}{q-1} q^{[\frac{m}{2}d]+1} - \frac{q}{q-1} q^{[\frac{m-2}{2}d]+1} + 1$.

(ii) *If $m$ is even and $d$ is odd, then* $\#\{\chi_\Phi\} = \frac{q^2+1}{2q-2} q^{\frac{m}{2}d} - \frac{q}{q-1} q^{\frac{m-2}{2}d+1} + q$.

(iii) *If $m$ and $d$ are both even, then* $\#\{\chi_\Phi\} = \frac{q^2+1}{2q-2} q^{\frac{m}{2}d} - \frac{q}{q-1} q^{\frac{m-2}{2}d+1} + 1$.

## References

[1] Bruno Angles, Modules de Drinfeld sur les corps finis, Thése de Doctorat, Université Paul Sabatier-Toulous III, no d'ordre 1872, 1994.
[2] Bruno Angles, One some subring of Ore polynomials connected with finite Drinfeld modules, J. Algebra 181 (2) (1996) 507–522.
[3] V.G. Drinfeld, Modules elliptiques, Math. USSR-Sb. 94(136) (1974) 594–627, 656.
[4] E.-U. Gekeler, B.A. Snyder, Drinfeld modules over finite fields, in: Drinfeld Modules, Modular Schemes and Application, Alden-Biesen, 1996.
[5] D. Goss, Basic Structures of Function Field Arithmetic, Ergebnise der Mathematik und ihrer Grenzgebiete, vol. 35, Springer, 2006.
[6] J.-K. Yu, Isogenies of Drinfeld modules over finite fields, J. Number Theory 54 (1) (1995) 161–171.