La Structure de $A$-Module induite par un $A$-Module de Drinfeld de Rang 2 sur un corps fini
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

Résumé

Soit $\Phi$ un $\mathbb{F}_q[T]$-module de Drinfeld de rang 2, sur un corps fini $L$, extension de degré $n$ d’un corps fini $\mathbb{F}_q$. Soit $P_\Phi(X) = X^2 - cX + \mu P^m$ (où $c \in \mathbb{F}_q[T]$, $\mu$ est un élément non nul de $\mathbb{F}_q$, $m$ est le degré de l’extension $L$ sur $\mathbb{F}_q[T]/P$, et $P$ est la $\mathbb{F}_q[T]$-caractéristique de $L$ et $d$ le degré du polynôme $P$) le polynôme caractéristique du Frobenius $F$ de $L$. On s’intéressera à la structure de $\mathbb{F}_q[T]$-module fini $L^\Phi$ induite par $\Phi$ sur $L$. Notre résultat principal est le parfait analogue du théorème de Deuring (voir [6]) pour les courbes elliptiques : soit $M = \mathbb{F}_q[T]_1 \oplus \mathbb{F}_q[T]_2$, où $I_1 = (i_1)$ et $I_2 = (i_2)$ ($i_1, i_2$ étant deux polynômes de $\mathbb{F}_q[T]$) tels que : $i_2 \mid (c - 2)$. Il existe alors un $\mathbb{F}_q[T]$-module de Drinfeld ordinaire $\Phi$ sur $L$ de rang 2 tel que : $L^\Phi \simeq M$.

Pour citer cet article : Mohamed-saadbouh.Mohamed-Ahmed, C. R. Acad. Sci. Paris, Ser. I ... (...).

Abstract

Let $\Phi$ be a Drinfeld $\mathbb{F}_q[T]$-module of rank 2, over a finite field $L$. Let $P_\Phi(X) = X^2 - cX + \mu P^m$ (c an element of $\mathbb{F}_q[T]$, $\mu$ be a non-vanishing element of $\mathbb{F}_q$, $m$ the degree of the extension $L$ over the field $\mathbb{F}_q[T]/P$, and $P$ the $\mathbb{F}_q[T]$-characteristic of $L$ and $d$ the degree of the polynomial $P$) the characteristic polynomial of the Frobenius $F$ of $L$. We will be interested in the structure of finite $\mathbb{F}_q[T]$-module $L^\Phi$ induced by $\Phi$ over $L$. Our main result is analogue to that of Deuring (see [6]) for elliptic curves : Let $M = \mathbb{F}_q[T]_1 \oplus \mathbb{F}_q[T]_2$, where $I_1 = (i_1)$, $I_2 = (i_2)$ ($i_1, i_2$ being two polynomials of $\mathbb{F}_q[T]$) such that : $i_2 \mid (c - 2)$. Then there exists an ordinary Drinfeld $\mathbb{F}_q[T]$-module $\Phi$ over $L$ of rank 2 such that : $L^\Phi \simeq M$. To cite this article: Mohamed-Saadbohu Mohamed-Ahmed , C. R. Acad. Sci. Paris, Ser. I ... (...).
1 Introduction

Let $K$ a no 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 $F_q$ 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 commutator 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 degree of $L$ over $A/P$, and $d = \text{degP}$.

We denote by $L[\tau]$ the polynomial ring of $\tau$, namely the Ore polynomial ring, where $\tau$ is the Frobenius of $F_q$ 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, define an $A$-module structure over the $A$-field $L$, noted $L^\Phi$, where the name of a Drinfeld $A$-module for a homomorphism $\Phi$. This structure of $A$-module depends on $\Phi$ and, especially, on his rank, for more information see [1], [2], and [3].

We will be interested in a Drinfeld $A$-module structure $L^\Phi$ in the case of rank 2, and we will prove that for an ordinary Drinfeld $F_q[T]$-module, this structure is always the sum of two cyclic and finite $F_q[T]$-modules: $A_{I_1} \oplus A_{I_2}$ where $I_1 = (i_1)$ and $I_2 = (i_2)$ such that $i_1$ and $i_2$ are two ideals of $A$, which verifies $i_2 | i_1$. Let $P_\Phi(X) = X^2 - cX + \mu P^m$, such that $\mu \in F_q^*$ and $c \in A$, the characteristic polynomial of $\Phi$. We will show that $\chi_\Phi = I_1 I_2 = (P_\Phi(1))$, so if we put $i = \text{pgcd}(i_1, i_2)$, then $i^2 | P_\Phi(1)$. We will give an analogue of Deuring theorem for elliptic curves:

**Theorem 1.1** Let $M = \frac{1}{i_1} \oplus \frac{1}{i_2}$, where $I_1 = (i_1)$, $I_2 = (i_2)$ and such that: $i_2 | i_1, i_2 | (c - 2)$. Then there exists an ordinary Drinfeld $A$-module $\Phi$ over $L$ of rank 2, such that: $L^\Phi \simeq M$.

2 Structure de $A$-module de Drinfeld $L^\Phi$

The Drinfeld $A$-module of rank 2 is of the form $\Phi(T) = a_1 + a_2 \tau + a_3 \tau^2$, where $a_i \in L$, $1 \leq i \leq 2$ 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 $p \Phi_a = \Psi_{aP}$ for all $a \in A$. A non-zero morphism is called an isogeny. We note that this is possible only between two Drinfeld modules with the same rank. The set of all morphisms forms an $A$-module denoted by $\text{Hom}_L(\Phi, \Psi)$.

(Mohamed-Saadbouh MOHAMED-AHMED).
In particular, if $\Phi = \Psi$ the $L$-endomorphism ring $\text{End}_L \Phi = \text{Hom}_L(\Phi, \Phi)$ is a subring of $L[\tau]$ and an $A$-module contained in $\Phi(A)$. Let $\mathcal{L}$ be a fix algebraic closure of $L$, $\Phi_a(\mathcal{L}) := \Phi[a](\mathcal{L}) = \{ x \in \mathcal{L}, \Phi_a(x) = 0 \}$, and $\Phi_P(\mathcal{L}) = \cap_{a \in P} \Phi_a(\mathcal{L})$. We say that $\Phi$ is supersingular if and only if the $A$-module constituted by a $P$-division points $\Phi_P(\mathcal{L})$ is trivial, otherwise $\Phi$ is said an ordinary module, see [2].

Let $\Phi$ be a Drinfeld $A$-module of rank $2$, over a finite field $L$ and let $P_\Phi$ his characteristic polynomial, $P_\Phi(X) = X^2 - cX + \mu P^m$, such that $\mu \in \mathbb{F}_q^*$, and $c \in A$, where $\deg c \leq \frac{m \mu}{2}$ by the Hasse-Weil analogue in this case. 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 basic field. About the $A$-module structure $L^\Phi$, we have the following result:

**Proposition 2.1** The Drinfeld $A$-module $\Phi$ give a finite $A$-module structure $L^\Phi$, which is on the form $\frac{A}{I_1} \oplus \frac{A}{I_2}$ where $I_1$ and $I_2$ are two ideals of $A$, such that : $\chi_\Phi = I_1 I_2$.

We put $I_1 = (i_1)$ and $I_2 = (i_2)$ ( $i_1$ and $i_2$ two unitary polynomials in $A$).

Let $i = \text{pgcd} (i_1, i_2)$, it is clear by the Chinese lemma, that the no cyclicity of the $A$-module $L^\Phi$, needs that $I_1$ and $I_2$ are not a prime between them, that means that $i \neq 1$, and since the relation $\chi_\Phi = I_1 I_2$, we will have : $i^2 \mid P_\Phi(1)$ ($\chi_\Phi = (P_\Phi(1))$).

In all the next of this paper, the condition above, will be considered verified, and more precisely we suppose that $I_2 \mid I_1$ (i.e : $i_2 \mid i_1$) otherwise $L^\Phi$ is a cyclic $A$-module and can be writing on this form $A/\chi_\Phi$.

**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 $L^\Phi$ is stable by the endomorphisme Frobenius $F$ of $L$. We choose a basis for $A/\chi_\Phi$, for which the $A$-module $L^\Phi$ will be generated by $(i_1, 0)$ and $(0, i_2)$. Let $M_F \in M_2(A/\chi_\Phi)$ the matrix of the endomorphism Frobenius $F$ in this basis. Then $M_F = \begin{pmatrix} a & b \\ a_1 & b_1 \end{pmatrix}$, where $a, b, a_1, b_1 \in A/\chi_\Phi$.

Although since : $\text{Tr} M_F = a + b_1 = c$ and $M_F(i_1, 0) = (i_1, 0)$ and $M_F(0, i_2) = (0, i_2)$, we will have $a.i_1 \simeq i_1 (\mod \chi_\Phi)$ and then $a - 1$ is divisible by $i_1$, of same for $b_1.i_2 \simeq i_2 (\mod \chi_\Phi)$, that means that $b_1 - 1$ is divisible by $i_2$ and then : $c - 2 = a - 1 + b_1 - 1$ is divisible by $i_2$ (since we have always $i_2 \mid i_1$).
Let \( \rho \) be a prime ideal from \( A \), different from the \( A \)-characteristic \( P \), we define the finite \( A \)-module \( \Phi(\rho) \) as been the \( A \)-module \((A/\rho)^2\).

The discriminant of the \( A \)-order : \( A + g.O_{K(F)} \) is \( \Delta.g^2 \), where \( \Delta \) is the discriminant of the characteristic polynomial \( P_\Phi(X) = X^2 - cX + \mu P^m \). So each order is defined by this discriminant and will be noted by \( \mathcal{O}(\text{disc}) \), see [8], and [7]. It is clear, by the Propositions 2.1 that the inclusion \( \Phi(\rho) \subset L^\Phi \) implies that \( \rho^2 \mid P_\Phi(1) \) and \( \rho \mid c - 2 \). We have:

**Proposition 2.3** Let \( \Phi \) be an ordinary Drinfeld \( A \)-module of rank 2, and let \( \rho \) an ideal from \( A \) different from the \( A \)-characteristic \( P \) of \( L \), such that \( \rho^2 \mid P_\Phi(1) \) and \( \rho \mid c - 2 \). Then \( \Phi(\rho) \subset L^\Phi \), if and only if, the \( A \)-order \( \mathcal{O}(\Delta/\rho^2) \subset \text{End}_L \Phi \).

To prove this proposition we need the following lemma:

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

Proof : We know that \( L^\Phi \) is satble by the isogeny \( F \) so \( L^\Phi = \text{Ker}(F - 1) \), and by definition \( \Phi(\rho) = \text{Ker}(\rho) \) ( we confuse by commodity the ideal \( \rho \) with this generator in \( A \)), and we know by [2], Theorem 4.7.8, that for two isogenies, let by example \( F - 1 \) and \( \rho \), we have \( \text{Ker}(F - 1) \subset \text{Ker}(\rho) \), if and only if, there exists an element \( g \in \text{End}_L \Phi \) such that \( F - 1 = g.\rho \) and then \( \Phi(\rho) \subset L^\Phi \), if and only if, \( \frac{F-1}{\rho} = g \in \text{End}_L \Phi \).

We prove now the Proposition 2.3 :

Proof : Let \( N(\frac{F-1}{\rho}) \) the norm of the isogeny \( \frac{F-1}{\rho} \), which is a principal ideal generated by \( \frac{P_\Phi(1)}{\rho^2} \), and the trace (Tr) of this isogeny is \( \frac{c-2}{\rho} \) then we can calculate the discriminant of the \( A \)-module \( A[\frac{F-1}{\rho}] \) by :

\[
\text{disc}A(\frac{F-1}{\rho}) = Tr(\frac{F-1}{\rho})^2 - 4N(\frac{F-1}{\rho}) = \frac{c^2-4\mu P^m}{\rho^2} = \Delta/\rho^2 \Rightarrow
\]

\( O(\Delta/\rho^2) \subset \text{End}_L \Phi. \)

We suppose now that : \( O(\Delta/\rho^2) \subset \text{End}_L \Phi \) and we prove that \( \Phi(\rho) \subset L^\Phi \). The Order corresponding of the discriminant \( \Delta/\rho^2 \) is \( A[\frac{F-1}{\rho}] \) this means that : \( \frac{F-1}{\rho} \in \text{End}_L \Phi \) and so, by lemma 2.1 : \( \Phi(\rho) \subset L^\Phi \).

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

Proof : We know that \( \Phi(\rho) \) is not cyclic (since it is a \( A \)-module of rank 2), and then the necessary and sufficient conditions need for non cyclicitiy of \( A- \)
module \( L^\Phi \) are equivalent to the necessary and sufficient conditions to have \( \Phi(\rho) \subset L^\Phi \).

We can so prove the following important theorem:

**Theorem 2.6** Let \( M = \frac{A}{I_1} \oplus \frac{A}{I_2} \), \( I_1 = (i_1) \) and \( I_2 = (i_2) \) such that: \( i_2 \mid i_1 \), \( i_2 \mid (c - 2) \). Then there exists an ordinary Drinfeld \( A \)-module \( \Phi \) over \( L \) of rank 2, such that: \( L^\Phi \simeq M \).

Proof: In fact, if we consider the Drinfeld \( A \)-module \( \Phi \), for which the characteristic of Euler-Poincare is giving by \( \chi_\Phi = I_1.I_2 \) and his endomorphism ring is \( O(\Delta/i_2^2) \) where \( \Delta \) is always the discriminant of the characteristic polynomial of the Frobenius \( F \). We remind that \( \Phi(\rho) \subset L^\Phi \) for every \( \rho \) an ideal, different from \( P \) and verify \( \rho^2 \mid P_\Phi(1) \) and \( \rho \mid (c - 2) \), if and only if, the \( A \)-order \( O(\Delta/\rho^2) \subset \text{End}_L\Phi \). Let now \( \rho = i_2 \). Since by construction the \( A \)-order \( O(\Delta/i_2^2) \subset \text{End}_L\Phi \) we have that \( \Phi(i_2) \simeq (A/i_2)^2 \subset L^\Phi \). We know that \( L^\Phi \) is included or equal to \( \Phi(\chi_\Phi) \simeq \frac{A}{\chi_\Phi} \oplus \frac{A}{\chi_\Phi} \), we have so: \( L^\Phi = \frac{A}{I_1} \oplus \frac{A}{I_2} \).

The above theorem can be proved by using the following conjecture:

**Conjecture 2.7** Let \( M \in M_2(A/\chi_\Phi) \), \( P = P( \mod P, \chi_\Phi) \). We suppose : \( \det M = \overline{P^n} \), \( \text{Tr}(M) = c \) and \( c \nmid P \). There exists an ordinary Drinfeld \( A \)-module over a finite field \( L \) of rank 2, for which the Frobenius matrix associated, is \( M_F \), and such that: \( M_F = M \in M_2(A/\chi_\Phi) \).

We put the following matrix: \( M_F = \begin{pmatrix} c - 1 & i_1 \\ i_2 & -1 \end{pmatrix} \in M_2(A/\chi_\Phi) \).

We can see that the three conditions of the conjecture are realized then there exists an ordinary Drinfeld \( A \)-modules \( \Phi \) over \( L \) of rank 2, such that: \( L^\Phi \simeq M \).

**References**

[1] Bruno Angles. *One Some Subring of Ore Polynomials Connected with Finite Drinfeld Modules*, J. Algebra 181 (1996) no.2, 507–522.

[2] David Goss. *Basic Structures of Function Field Arithmetic*, Volume 35 Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer.

[3] V.G. Drinfeld. *Modules Elliptiques*. Math, USSR Sbornik, 94 (136), 594-627, 656, (1974).
[4] V.G. Drinfeld. *Modules Elliptiques II Math.* USSR Sbornik, 102 (144), No 2, 182-194, 325, (1977).

[5] Joseph. H. Silverman *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, 106.

[6] M. Deuring. *Die Typen der Multiplikatorenringe Elliptischer Funktionenkörper,* Abh. Math. sem. Univ. Hamburg, 14 (1941), 197-272.

[7] M. A. Tsfasman-S. G. Vladut. *Algebraic-Geometric Codes,* Mathematics and Applications, Dordrecht et al, (1991).

[8] R. Shoo. *Nonsingular Plane Cubic Curves Over Finite Fields,* Journal of combinatorial theory, series A 46, (1987), 183-211.

[9] I. Reiner. *Maximal Orders.* Academic Press, (1975).

[10] H.G. Ruck. *A Note on Elliptic Curves Over Finite Fields.* Math. Comp. 49, no179, (1987), 301–304.

[11] W. C. Waterhouse. *Abelian Varieties Over Finite Fields.* Ann. Sci. Ecole Norm. Sup2, (1969), 521-560.