The $A$-Module Structure Induced by a Drinfeld $A$-Module of Rank 2 over a Finite Field

MOHAMED AHMED Mohamed Saadbouh
Institut de Mathématiques de Luminy, CNRS-UPR 9016
Case 907, 163 Avenue de Luminy, 13288 Marseille, Cedex 9. France.

Abstract
Let $\Phi$ be a Drinfeld $F_q[T]$-module of rank 2 over a finite field $F_q(T)$, and $L$ a finite field of $n$ degrees for a finite field with $q$ elements $F_q$. Let $P_\Phi(X) = X^2 - cX + \mu P^m (c$ an element of $F_q[T]$ and $\mu$ a non null element of $F_q$, $m$ the degree of the extension $L$ over the field $F_q[T]/P$ and $P$ is the characteristic of $L$) the characteristic polynomial of the Frobenius $F$ of $L$. We will interested to the structure of finite $F_q[T]$-module $L^\Phi$ deduct by $\Phi$ over $L$ and will proof our main result, the analogue of Deuring theorem for the elliptic curves : Let $M = \frac{F_q[T]}{I_1} \oplus \frac{F_q[T]}{I_2}$, where $I_1 = (i_1), I_2 = (i_2)$ ( $i_1, i_2$ two polynomials of $F_q[T]$) and such that : $i_2 \mid (c - 2)$. Then there exists an ordinary Drinfeld $F_q[T]$-module $\Phi$ over $L$ of rank 2, such that : $L^\Phi \simeq M$. We finish by a statistic about the cyclicity of such structure $L^\Phi$, and we prove that is cyclic only for the trivial extensions of $F_q$.

1 Introduction
Let $E$ be an elliptic curve over finite field $F_q$, we know, see [12], [15], [16] and [19], that the endomorphism ring of $E$, $\text{End}_{F_q} E$, is an $\mathbb{Z}$-order in a division
This algebra is: \( \mathbb{Q} \) and in this case \( \text{End}_{\mathbb{F}_q} E = \mathbb{Z} \), or a quadratic complex field and in this case: \( \text{End}_{\mathbb{F}_q} E = \mathbb{Z} + c \mathcal{O}_K \) where \( c \) is an element of \( \mathbb{Z} \) and \( \mathcal{O}_K \) is the maximal \( \mathbb{Z} \)-order in this quadratic complex field, or is a Quaternion Algebra over \( \mathbb{Q} \) and in this case \( \text{End}_{\mathbb{F}_q} E \) is a maximal order in this Quaternion Algebra. We put \( E(\mathbb{F}_q) \) the abelian group of \( \mathbb{F}_q \)-rational points of \( E \). The cardinal of this abelian group is equal to \( N = q + 1 - c \), and by Hasse-Weil \( |c| \leq 2\sqrt{q} \). The structure of this group in the ordinary case is:

\[
E(\mathbb{F}_q) \simeq \mathbb{Z}/A \oplus \mathbb{Z}/B, \quad \text{if } (c, q) = 1, \quad B \mid A, \quad B \mid (c - 2) \quad \text{and } A.B = N
\] (1)

Conversely, for every abelian group \( \mathbb{Z}/A \oplus \mathbb{Z}/B \), with \( B \mid A, \quad B \mid (c - 2) \quad \text{and} \quad A.B = N \), there is an elliptic curve \( E \) such that: \( E(\mathbb{F}_q) \simeq \mathbb{Z}/A \oplus \mathbb{Z}/B \), we note that in the supersingular case, this structure is also known, see [15].

Over this structure, S. Vladut, in [20], has effected a statistic about the report of elliptic curves for which the \( E(\mathbb{F}_q) \) is cyclic over the number of classes of \( \mathbb{F}_q \)-endomorphisms of elliptic curves over finite field \( \mathbb{F}_q \), this report will depend on \( q \) and will be noted \( c(q) \), and we have:

\[
c(q) = \frac{\# \{E, \ E(\mathbb{F}_q) \text{ cyclic} \}}{\# \{E\}},
\]

where \( \# \{E\} \) is the number of classes of \( \mathbb{F}_q \)-endomorphisms of elliptic curve over a finite field \( \mathbb{F}_q \), and we know, see [20], that:

\( c(q) = 1 \) if and only if \( q = 2^l \) where \( l \neq 2 \) is a prime or equal at 1 and one of the following conditions is satisfied:

1. \( q - 1 \) is prime, \( q \neq 4 \) (the case \( q = 2 \) is included, thus we consider 1 as prime),
2. \( q - 1 = l_1 l_2 \) with primes \( l_1 \) and \( l_2 \) is not a "small" divisors of \( q - 1 \);
3. \( q - 1 = l_1 l_2 l_3 \) with primes \( l_1, l_2 \) and \( l_3 \) are not a "small" divisors of \( q - 1 \).

The case \( l_1 = l_2 \) is not exclude.

In general case, the number \( c(q) \) is given in [20], by:

Let \( \varepsilon > 0 \) we have:

\[
c(q) = \prod_l \left( 1 - \frac{1}{l(l^2 - 1)} \right) + O(q^{-1/2 + \varepsilon}),
\]

where the product is taken over all prime divisors of \( q - 1 \). Our goal here is to give an analog of the above mentioned results in the case of Drinfeld Modules of rank 2. We recall quickly what is it: let \( K \) a no empty global field of characteristic \( p \) (that means a rational functions field of one indeterminate over a finite field) with a constant field the finite field \( \mathbb{F}_q \) with \( p^s \) elements. We fix one place of \( K \), noted \( \infty \) and we call \( A \) the ring of regular elements away...
from the place \( \infty \). Let \( L \) be a commutative field of characteristic \( p \), and let \( \gamma : A \to L \), be a \( A \)-ring homomorphism, the kernel of this homomorphism is noted \( P \) and \( m = [L, A/P] \) is the extension degrees of \( L \) over \( A/P \).

We note \( L\{\tau\} \) the Ore’s polynomial ring, that means the polynomial ring of \( \tau \), \( \tau \) is the Frobenius of \( F_q \), with the usual addition and the product is given by the computation rule : for every \( \lambda \) of \( L \), \( \tau \lambda = \lambda^{q} \tau \). We say a Drinfeld \( A \)-module \( \Phi \) for a non trivial homomorphism of ring, from \( A \) to \( L\{\tau\} \) which is different of \( \gamma \). this homomorphism \( \Phi \), once defined, gives a \( A \)-module structure over the \( A \)-field \( L \), noted \( L^\Phi \), where the name of a Drinfeld \( A \)-module for a homomorphism \( \Phi \). This structure \( A \)-module is depending on \( \Phi \) and especially on this rank.

Let \( \chi \) be the characteristic of Euler-Poincare ( it is a ideal from \( A \) ), so we can speak about the ideal \( \chi(L^\Phi) \), will be noted by \( \chi_\Phi \), which is by Definition a divisor for \( A \), corresponding for the elliptic curves to a number of points of the variety over their basic fields.

We will work, in this paper, in the special case \( K = F_q(T), \ A = F_q[T] \). Let \( P_\Phi(x) : \) the characteristic polynomial of the \( A \)-module \( \Phi \), it is also a characteristic polynomial of Frobenius \( F \) of \( L \). We can prove that this polynomial can be given by : \( P_\Phi(x) = x^2 - cX + \mu P^m \), such that \( \mu \in F_q^* \), \( c \in A \) and \( \deg c \leq m \frac{2}{d} \), the Hass-Weil’s analogue in this case.

We will interest to 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 : \( \frac{A}{I_1} \oplus \frac{A}{I_2} \) where \( I_1 \equiv (i_1) \) and \( I_2 \equiv (i_2) \) such that \( i_1 \) and \( i_2 \) is two ideals of \( A \), which verifies \( i_2 \mid i_1 \). We will show that \( \chi_\Phi = I_1I_2 = (P_\Phi(1)) \), and if we put \( i = \gcd(i_1, i_2) \), then : \( i^2 \mid P_\Phi(1) \). We will give now some appears of our results proved in this paper :

**Proposition 1.1.** With the above notations, we have :
\[ L^\Phi \cong \frac{A}{I_1} \oplus \frac{A}{I_2}. \]
And if we have an ordinary module \( \Phi \), then :
\[ i_2 \mid (c - 2). \]

We note by \( \text{End}_L \Phi \) the endomorphism ring of a Drinfeld \( A \)-module \( \Phi \), we have:

**Proposition 1.2.** Let \( \Phi \) be an ordinary Drinfeld \( A \)-module of rank 2 and let \( \rho \) a prime ideal of \( A \) different from \( P \) the \( A \)-characteristic 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 \( \mathcal{O}(\Delta/\rho^2) \subset \text{End}_L \Phi \).

Finally, we come to our main result, which is a complete analog of (1), the Deuring-Waterhous theorem for the elliptic curves :

**Theorem 1.1.** Let \( M = \frac{A}{I_1} \oplus \frac{A}{I_2} \), where \( I_1 \equiv (i_1) \), \( I_2 \equiv (i_2) \) and 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 :
\[ L^\Phi \cong M. \]

Lastly, we will make a statistic about the ordinary Drinfeld \( A \)-modules such that the \( A \)-modules \( L^\Phi \) are cyclic, we note by \( C(d, m, q) \) the proportion of the number (of isomorphisms of) ordinary Drinfeld \( A \)-modules, of rank 2 such that the \( A \)-modules structures \( L^\Phi \) are cyclic, this means : if we note by \( \#(\Phi, \text{isomorphism, ordinary} \} \) the number of classes of \( L \)-isomorphisms of an ordinary Drinfeld Modules of rank 2, we have:
\[ C(d, m, q) = \frac{\# \{\Phi, L^\Phi \text{ cyclic}\}}{\# \{\Phi, \text{ isomorphism, ordinary}\}} \]

and we note by \( C_0(d, m, q) \) the proportion of the number ( of isogeny classes of) ordinary Drinfeld \( A \)-modules, of rank 2 such that the \( A \)-modules \( L^\Phi \) are cyclic, otherwise, if we note by \( \# \{\Phi, \text{ isogeny, ordinary}\} \) the number of isogeny classes, of ordinary Drinfeld modules of rank 2, we have:

\[ C_0(d, m, q) = \frac{\# \text{isogeny Classes of } \Phi, L^\Phi \text{ cyclic}}{\# \{\Phi, \text{ isogeny, ordinary}\}}. \]

Of course, these numbers are depending on \( q \) and also on \( d, m \).

One of our important results is:

**Proposition 1.3.** \( C(d, m, q) = C_0(d, m, q) = 1 \) if and only if \( m = d = 1 \).

This means that, to have a Cyclic Drinfeld \( A \)-modules we must have a trivial extension \( L \), we give also some values for \( C(d, m, q) \) and \( C_0(d, m, q) \) corresponding to some given values of \( d \) and \( m \), for example:

**Proposition 1.4.** We put \( d = 2 \) and \( m = 1 \). Let \( H(O(D)) \) the Hurwitz’s number of classes for an order \( O \) which the imaginary determinant is \( D \):

\[ C_0(2, 1, q) = \frac{q(q-1) - 5}{q(q-1) - 2}. \]

\[ C(2, 1, q) = \frac{q^3 - q^2 - q + 1 - \left[ \frac{q-1}{2} \sum_{P} \sum_{i=0}^{a-4\mu P} H(O(\frac{2^{a}+\mu P}{2})) \right] + (q-1) \sum_{P} \sum_{i=0}^{a-4\mu P} H(O(\frac{2^{a}+\mu P}{2}))}{q^3 - q^2 - q + 1}. \]

And we let think, in conjecture form, that for a big \( q \) the values of \( C(d, m, q) \) and \( C_0(d, m, q) \) will tend to 1.

## 2 Drinfeld Modules

Let \( E \) be an extension of \( F_q \), and let \( \tau \) Frobenius of \( F_q \). We put \( E \{ \tau \} \) the polynomial ring in \( \tau \) with the usual addition and the multiplication defined by:

\[ \forall e \in E, \ \tau e = e^q \tau. \]

**Definition 2.1.** Let \( R \) be the \( E \)-linearly polynomials set with the coefficient in \( E \), that means that these elements are on the following form:

\[ Q(x) = \sum_{K>0} l_k x^k, \]

where \( l_k \in E \) for every \( k > 0 \), and only a finite number of \( l_k \) is not null. The ring \( R \) is a ring by addition and the polynomial composition.
Lemma 2.1. $E\{\tau\}$ and $R$ are isomorphic rings.
If we put $A = \mathbb{F}_q[T]$, $f(\tau) = \sum_{i=0}^{u} a_i \tau^i \in E\{\tau\}$ and $Df := a_0 = f'(\tau)$.
It is clear that the application:

$$E\{\tau\} \mapsto E$$

$$f \mapsto Df,$$

is a morphism of $\mathbb{F}_q$-algebras.

Definition 2.2. An $A$-fields $E$ is a field $E$ equipped with a fix morphism
$\gamma : A \rightarrow E$. The prime ideal $P = \text{Ker} \gamma$ is called the characteristic of $E$. We
say $E$ has generic characteristic if and only if $P = (0)$; otherwise (i.e $P \neq (0)$) we said $P$ is finite and $E$ has finite characteristic.

We then have the following fundamental definition:

Definition 2.3. Let $E$ an $A$-field and $\Phi : A \rightarrow E\{\tau\}$ be homomorphism of algebra. Then $\Phi$ is a Drinfeld $A$-module over $E$ if and only if:

1. $D \circ \Phi = \gamma$;
2. for some $a \in A$, $\Phi_a \neq \gamma(a) \tau^0$.

As was proved by Drinfeld in [6], such modules always exist.

Remark 2.1. 1. The above normalization is analogous to the normalization used in complex multiplication of elliptic curves. The last condition is obviously a non-triviality condition.

2. By $\Phi$, every extension $E_0$ of $E$ became an $A$-module by:

$$E_0 \times A \rightarrow E_0,$$

$$(k,a) \rightarrow k.a := \Phi_a(k).$$

We will note this $A$-module by $E_0^\Phi$.

Let $\overline{E}$ be a fix algebraic closure of $E$ and $\Phi$ a Drinfeld module over $E$ and $I$ an ideal of $A$. As $A$ is a Dedekind domain, one know that $I$ may be generated by ( at most ) two elements $\{i_1, i_2\} \subset I$.

Since $E\{\tau\}$ has a right division algorithm, there exists a right greatest common divisor in $E\{\tau\}$. It is the monic generator of the left ideal of $E\{\tau\}$ generated by : $\Phi_{i_1}$ et $\Phi_{i_2}$.

Definition 2.4. We set $\Phi_I$ to be the monic generator of the left ideal of $E\{\tau\}$ generated by $\Phi_{i_1}$ and $\Phi_{i_2}$.

Definition 2.5. Let $E_0$ an extension of $E$ and $I$ an ideal of $A$. We define by : $\Phi[I]\{E\}$ the finite subgroup of $\Phi[\overline{E}]$ given by the roots of $\Phi_I$ in $\overline{E}$.
If \( a \in A \), then we set \( \Phi[a] := \Phi((a)) \). We can see it as:

\[
\Phi_a(E) := \Phi[a](E) = \{ x \in E, \Phi_a(x) = 0 \}.
\]

And for every ideal \( Q \subset A \),

\[
\Phi_Q(E) := \Phi_Q(E) = \bigcap_{a \in Q} \Phi_a(E).
\]

**Remark 2.2.** The groups \( \Phi[I](E) \) and \( \Phi[I](E) \) are clearly stable under \( \{ \Phi_a \}_{a \in A} \).

**Definition 2.6.** Let \( \Phi \) be a Drinfeld \( A \)-module over an \( A \)-field \( E \). We say that \( \Phi \) is supersingular, if and only if, the \( A \)-module constituted by a \( P \)-division points \( \Phi_P(E) \) is trivial.

### 2.1 The Height and Rank of a Drinfeld Module \( \Phi \)

Let \( \Phi \) be a Drinfeld \( A \)-module over the \( A \)-field \( E \). We note by \( \deg_{\tau} \) the degree in indeterminate \( \tau \).

**Definition 2.7.** An element of \( E \{ \tau \} \) is called separable, if this constant coefficient is not null. It called purely inseparable if it is on the form \( \lambda \tau^n, n > 1 \) and \( \lambda \in E, \lambda \neq 0 \).

Let \( H \) be a global field of characteristic \( p > 0 \), and let \( \infty \) one place (a Prime ideal) of \( H \), we will note by \( H_\infty \) the completude of \( H \) at the place \( \infty \). We define the degree of function over \( A \) by:

**Definition 2.8.** Let \( a \in A \), \( \deg a = \dim_{F_q A} \frac{A}{aA} \) if \( a \neq 0 \) and \( \deg 0 = -\infty \).

We extend \( \deg \) to \( K \) by putting \( \deg x = \deg a - \deg b \) if \( 0 \neq x = \frac{a}{b} \in K \). If \( A = F_q[T] \), then the degree function is the usual polynomial degree. Let \( Q \) be a no null ideal of \( A \), we define the ideal degrees of \( Q \), noted \( \deg Q \), by:

\[
\deg Q = \dim_{F_q} \frac{A}{Q}.
\]

**Lemma 2.2.** There exists a rational number \( r \) such that:

\[
\deg_{\tau}, \Phi_a = r \deg a.
\]

**Proof.** It is easy to see that \( \Phi \) is an injection, otherwise since \( K \{ \tau \} \) is an integre ring, \( \ker \Phi \) is a prime ideal non null, so maximal in \( A \) and by consequence \( \im \Phi \) is a field, so \( \Phi = \gamma \). Since \( -\deg_{\tau} \) define a no trivial valuation over \( \text{Frac}(\Phi(A)) \) (the fractions field of \( \Phi(A) \)) which is isomorphic to \( K \), so \( -\deg_{\tau} \) and \( \deg \) are equivalent valuations over \( K \). There is rational number \( r > 0 \), such that:

\[
r \deg = \deg_{\tau}.
\]
Corollary 2.1. Let $\Phi : A \mapsto E\{\tau\}$ be a Drinfeld $A$-module, so $\Phi$ is injective.

Proposition 2.1. The number $r$ is a positive integer.

Definition 2.9. The number $r$ is called the rank of the Drinfeld $A$-module $\Phi$.

For example if $A = F_q[T]$, a Drinfeld $A$-module of rank $r$ is on the form : $\Phi(T) = a_1 + a_2\tau + ... + a_r\tau^r$, where $a_i \in E$, $1 \leq i \leq r - 1$ and $a_r \in E^*$.

In this case char $E = P \neq (0)$ we can define the notion of height of a Drinfeld module $\Phi$.

For this, we put $v_P : K \mapsto \mathbb{Z}$, an associate normalized valuation at $P$, this means, if $a \in K$ has a root over $P$ of order $t$, we have $v_P(a) = t$.

For every $a \in A$, let $w(a)$ the most small integer $t > 0$, where $\tau^t$ occurs at $\Phi_a$ with a no null coefficient.

Lemma 2.3. There exists a rational number $h$ such that :

$$w(a) = hv_P(a) \deg P.$$ 

Proposition 2.2. The number $h$ is a positive integer.

Definition 2.10. the integer $h$ is called the height of $\Phi$.

For example if $A = F_q[T]$, a Drinfeld $A$-module of height $h$ of rank $r$ is on the form : $\Phi(T) = a_0 + a_h\tau^h + ... + a_r\tau^r$, where $a_i \in E$, $0 \leq i \leq r - 1$ and $a_r \in E^*$.

Definition 2.11. Let $\Phi$ and $\Psi$ two Drinfeld $A$-modules over an $A$-field $E$ and $p$ an isogeny over $E$ from $\Phi$ to $\Psi$.

1. We say that $p$ is separable if and only if $p(\tau)$ is separable.

2. We say that $p$ is purely no separable if and only if $p(\tau) = \tau^j$ for one $j > 0$.

2.2 Norm of Isogeny

Definition 2.12. Let $F$ an integer over a ring $A$, with fractions field $K$. we note by $N_{K/K}(F)$ the determinant of the $K$-linearly application of multiplication by $F$ to $K(F)$ (it is the usual norm if the extension $K(F)/K$ is separable.

We can see that there is a morphism $N_{K/K(F)} : I_A \rightarrow I_A$ from the fractional ideals groups of $A$ to functionary ideals group of $A$, by this morphism we have:

Proposition 2.3. The norm of isogeny is a principal ideal.

Proposition 2.4. Let $M_{fin}(A)$ the category of primes ideals of $A$ and let $D(A)$ the monoide of ideals of $A$. There exists an unique function :

$$\chi : M_{fin}(A) \rightarrow D(A),$$

multiplicative over the exact sequence and such that $\chi(0) = 1$ and $\chi(A/\varphi) = \varphi$ for every prime ideal $\varphi$ of $A$. 

7
Definition 2.13. The function $\chi$ is called the Euler-Poincare characteristic.

We can see $\chi(E^\Phi)$ and we note it by $\chi_\Phi$.

Proposition 2.5. The ideals $\chi_\Phi$ and $P^m$ are principals (in $A$), and more clearly $\chi_\Phi = (P^\Phi(1))$ and $P^m = P^\Phi(0)$.

1. We know that the norm of isogeny is a principal ideal, indeed $N(F) = P^\Phi(0)$ and $N(1 - F) = (P^\Phi(1))$ since $F$ and $1 - F$ are a $K$-isogenys.

2. We can call $\chi_\Phi$ the divisor of $E$-points, this divisor is analogue at the number of $E$-points for elliptic curves.

3. $\chi_\Phi$ is the annulator of $A$-module $E^\Phi$. We can deduct that : $E^\Phi \subset (\frac{A}{\chi_\Phi})^r$.

4. The structure of $A$-module $E^\Phi$ is stable by the Frobenius endomorphism $F$.

Corollary 2.2. If there are a Drinfeld $A$-module $\Phi$, over a field $E$, of characteristic $P$ and of degree $m$ over $A/P$, then the ideal $P^m$ is a principal ideal.

Remark 2.3. The above Corollary shows that there exists a restriction of the existence of Drinfeld $A$-modules.

3 Drinfeld Modules over Finite Fields

We substitute the Field $E$, by $L$ a finite extension of degree $n$ of the finite field $F_q$. Let $\tau : x \mapsto x^q$ be the Frobenius of $F_q$, so the Frobenius $F$ of $L$ is $F = \tau^n$ and $F_q[F]$ is the center of $L\{\tau\}$. We put $m = [L : A/P]$ and $d = \deg P$, then $n = m.d$. The function $-\deg$ define a valuation over $K$, the field of fractions of $A$. We put $r_1 = [K(F) : K]$ and $r_2$ the degree of the left field $\text{End}_L \Phi \otimes_A K$ over this center $K(F)$.

So a Drinfeld $A$-module $\Phi$ over $L$ give a structure of $A$-module over the additive finite group $L$, this structure will be noted $L^\Phi$. Let $\gamma$ the application of $A$ to $L$ which an element $a$ for $A$ associate the constant of $\Phi_a$, then it is easy to see that $\gamma$ is a ring homomorphism, and that $\Phi$ and $\gamma$ are equal over $A^* = F_q^*$ the set of reversible elements of $A$.

Definition 3.1. Let $\Phi$ be a Drinfeld $A$-module over a finite field $L$. We note by $M_\Phi(X)$ the unitary minimal polynomial of $F$ over $K$.

Proposition 3.1. With the above notations : $M_\Phi(X)$ is an element of $A[X]$, equal to $P^\Phi_{1/r}$. 

Corollary 3.1. For two Drinfeld $A$-modules $\Phi$ and $\Psi$, of rank $r$ over a finite field $L$, then the following are equivalent :

1. $\Phi$ and $\Psi$ are isogenous,
2. \( M_\Phi(X) = M_\Psi(X) \),

3. \( P_\Phi = P_\Psi \).

**Proposition 3.2.** Let \( L \) be a finite extension of degree \( n \) over a finite field \( F_q \) and \( F \) the Frobenius of \( L \). Then \( L(\tau) \) is a central division algebra over \( F_q(F) \) of dimension \( n^2 \).

**Definition 3.2.** Every \( u \in L\{\tau\} \) can be writing on this form \( u = \tau^hu' \) (since \( L \) is a perfect field) where \( u' \in L\{\tau\} \) separable. The integer \( h \) is called the height of \( u \) and will be noted by \( \text{ht} \ u \).

In the finite field case, we can see the height of a Drinfeld \( A \)-module \( \Phi \) over finite field \( L \), the integer \( H_\Phi \), as been:

\[
H_\Phi = \frac{1}{r} \inf \{ \text{ht} \ A_a, 0 \neq a \in P \}.
\]

**Remark 3.1.** It is easy to see that \( H_\Phi \) is invariant under isogeny and that

\[
1 \leq H_\Phi \leq r.
\]

**Proposition 3.3.** Let \( \Phi \) be a Drinfeld \( A \)-module of rank \( r \) over a finite field \( L \), the following assertions are equivalent:

1. There exists a finite extension \( L' \) of \( L \), such that the endomorphism ring \( \text{End}_{L'}\Phi \otimes_A K \), has dimension \( r^2 \) over \( K \).

2. Some power of the Frobenius \( F \) of \( L \) lies in \( A \).

3. \( \Phi \) is supersingular.

4. The field \( K(F) \) has only one prime above \( P \).

**Proposition 3.4.** Let \( \Phi \) be a Drinfeld \( A \)-module of rank \( r \) and let \( Q \) be an ideal from \( A \) prime with \( P \), then:

\[
\Phi_Q(L) = (A_Q)^r.
\]

**Corollary 3.2.** Then we can deduct that: \( \Phi_P(L) = (A_P)^{r-H_\Phi} \).

We can deduct from above mentioned Proposition the following important result, which characterize the supersingularity:

**Proposition 3.5.** The Drinfeld \( A \)-module \( \Phi \) is supersingular (\( \Phi_P(L) = 0 \)), if and only if, \( r = H_\Phi \).

**Definition 3.3.** We say that the field \( L \) is so big if all endomorphism rings defined over \( \mathcal{L} \) are also defined over \( L \), i.e: \( \text{End}_L\Phi = \text{End}_{\mathcal{L}}\Phi \).
Two Drinfeld modules Φ and Ψ are isomorphic, if and only if, there exists an \( a \in L \) such that: \( a^{-1} \Phi a = \Psi a \).

**Lemma 3.1.** Let \( \Phi \) be a Drinfeld \( A \)-module of rank \( r \), over a finite field \( L \), of characteristic \( P \). The characteristic polynomial of Frobenius endomorphism \( F \) is:

\[
P_\Phi(X) = X^r + c_1 X^{r-1} + \ldots + c_{r-1} X + \mu P^m, \quad c_1, \ldots, c_{r-1} \in A \text{ et } \mu \in F_q^*.
\]

**Remark 3.2.** The fact that constant of the polynomial \( P \) is \( \mu P^m \) comes from the fact that \( P_\Phi(0) = P^m \) in \( A \).

The following Proposition is an analogue of the Riemann’s hypothesis for elliptic curves:

**Proposition 3.6.** Let \( \Phi \) be a Drinfeld \( A \)-module of rank \( r \) over finite field \( L \) which is a finite extension of degree \( n \) of \( F_q \). Then \( \deg(w) = n r \) for every root \( w \) of characteristic polynomial \( P_\Phi(X) \).

The following result is the Hasse-Weil’s analogue for the elliptic curves:

**Corollary 3.3.** Let \( P_\Phi(X) = X^r + c_1 X^{r-1} + \ldots + c_r X + \mu P^m \) be the characteristic polynomial of a Drinfeld Module \( \Phi \), of rank \( r \), over a finite field \( L \). Then:

\[
\forall 1 \leq i \leq r-1, \deg c_i \leq \frac{i}{r} m \deg P.
\]

**Proof.** The proof can be deducted immediately by the above Proposition. \( \square \)

4 Drinfeld Modules of rank 2

In all next of this paper, \( \Phi \) will be considered a Drinfeld \( A \)-module of rank 2, and \( A = F_q[T] \) for proof and more details see [1], [12] and [6].

4.1 Structure of \( A \)-module \( L_\Phi \)

Let \( \Phi \) be a Drinfeld \( A \)-module of rank 2, over a finite field \( L \) and let \( P \) this characteristic polynomial. About the \( A \)-module structure \( L_\Phi \), we have the following result:

**Proposition 4.1.** 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: \( \chi_\Phi = I_1 I_2 \).

**Proof.** Since the \( A \)-module \( L_\Phi \) is a sub\( A \)-module of \( \Phi(\chi_\Phi) \simeq \frac{A}{\chi_\Phi} \oplus \frac{A}{\chi_\Phi} \), then there are \( I_1 \) and \( I_2 \) in \( A \) such that: \( L_\Phi \simeq \frac{A}{I_1} \oplus \frac{A}{I_2} \) and since the Euler-Poincare’s Characteristic is multiplicative over the exact sequence we will have \( \chi_\Phi = I_1 I_2 \). \( \square \)
We put \( I_1 = (i_1) \) and \( I_2 = (i_2) \) \((i_1 \text{ and } i_2 \text{ two unitary polynomials in } A)\).

Let \( i = \text{gcd} \ (i_1, i_2) \), it is clear by the Chinese lemma, that the non 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 \( \chi_\Phi = I_1I_2 \), 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 \( I_2 \mid I_1 \) \((\text{i.e: } i_2 \mid i_1)\) otherwise \( L^\Phi \) is a cyclic \( A \)-module and can be writing on this form \( A/\chi_\Phi \).

**Proposition 4.2.** 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 endomorphisme Frobenius \( F \) in this basis. Then \( M_F = \begin{pmatrix} a & b \\ \overline{a} & \overline{b} \end{pmatrix} \), where \( a, b, \overline{a}, \overline{b} \in A/\chi_\Phi \).

Although since: \( \text{Tr } M_F = a + b = c \) and \( M_F(i_1,0) = (i_1,0) \) and \( M_F(0,i_2) = (0,i_2) \), we will have \( a.i_1 \simeq i_1( \text{ mod } \chi_\Phi ) \) and then \( a - 1 \) is divisible by \( i_1 \), of same for \( b_1,i_2 \simeq i_2( \text{ mod } \chi_\Phi ) \), 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 \( i_2 \mid i_1 \)). \( \square \)

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 \( P_\Phi(X) = X^2 - cX + \mu P^n \). So each order is defined by this discriminant and will be noted by \( O(\text{disc}) \). It is clear, by the Propositions 4.1 that the inclusion \( \Phi(\rho) \subset L^\Phi \) implies that \( \rho^2 \mid P_\Phi(1) \) and \( \rho \mid c - 2 \). And if we note by \( \text{End}_L \Phi \) the endomorphism ring of the Drinfeld \( A \)-module \( \Phi \), we have:

**Proposition 4.3.** 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 \( O(\Delta /\rho^2) \subset \text{End}_L \Phi \).

To prove this Proposition we need the following lemma :

**Lemma 4.1.** \( \Phi(\rho) \subset L^\Phi \) is equivalent to \( F - 1 \in \text{End}_L \Phi \).

**Proof.** Since \( L^\Phi = \text{Ker}(F - 1) \) and \( \Phi(\rho) = \text{Ker}(\rho) \) (We confuse by commodity the ideal \( \rho \) with this generator in \( A \)) and we know by [3], Proposition 4.7.9, that for two isogenys, 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, \( \frac{F - 1}{\rho} = g \in \text{End}_L \Phi \). \( \square \)

We prove now the Proposition 4.3 :
Proof. Let \( N(F_{\rho}) \) the norm of the isogeny \( F_{\rho}^{-1} \), which is a principal ideal generated by \( P_{\rho}(1) \), and the trace (Tr) of this isogeny is \( z_{\rho}^{-2} \), then we can calculate the discriminant of the \( A \)-module \( A[F_{\rho}^{-1}] \) by:

\[
\text{disc}A((F_{\rho}^{-1})) = \text{Tr}(F_{\rho}^{-1})^2 - 4N(F_{\rho}^{-1}) = \frac{c^2 - 4\mu}{\rho^2} = \Delta/\rho^2 \Rightarrow \\
O(\Delta/\rho^2) \subset \text{End}_L\Phi.
\]

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 \( A[F_{\rho}^{-1}] \) this means that:

\[
F_{\rho}^{-1} \in \text{End}_L\Phi \quad \text{and so, by lemma 4.1} : \quad \Phi(\rho) \subset L^\Phi.
\]

\( \square \)

**Corollary 4.1.** 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 cyclicity of \( A \)-module \( L^\Phi \) are equivalent to the necessary and sufficient conditions to have \( \Phi(\rho) \subset L^\Phi \). \( \square \)

We can so prove the following important Theorem :

**Theorem 4.1.** Let \( M = \frac{A}{i_1} \oplus \frac{A}{i_2} \), \( I_1 = (i_1) \) and \( I_2 = (i_2) \) 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:

\[
L^\Phi \simeq M.
\]

**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 this 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 \( A \), different from \( P \) and verify \( \rho^2 \mid P(1) \) 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 : \( L^\Phi = \frac{A}{i_1} \oplus \frac{A}{i_2} \). \( \square \)

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

**Conjecture 4.1.** Let \( M \in M_2(A/\chi_\Phi) \), \( \overline{P} = P( \mod \chi_\Phi) \).

We suppose : \( (\det M) = \overline{P}^n \), \( \text{Tr} \ (M) = c \) and \( c \nmid P \). There exists a ordinary Drinfeld \( A \)-module \( \Phi \) 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 : \( L^\Phi \simeq M \).
4.2 Deuring Theorem

The following Theorem, proved by Max-Deuring in [15] and [19] is used for the proof of the analogue of our principal result, in elliptic curves case:

**Theorem 4.2.** Let $E_0$ be an elliptic curve over a finite field of characteristic $p$, with a no trivial endomorphism $F_0$. Then there exists an elliptic curve $E$ over a field of numbers and an endomorphism $F$ from $E$ such $E_0$ is isomorphic to $E$ and $F_0$ corresponding to $F$ under this isomorphism.

From the previous Theorem, we can deduct the following Theorem:

**Theorem 4.3.** Let $N \in \mathbb{N}$, $M = \begin{pmatrix} a & b \\ a_1 & b_1 \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z})$ and $F_q$ a finite field with $q$ elements, we suppose:

1. $(\det M) = q \pmod{N}$;
2. $|a + b_1| \leq 2\sqrt{q}$.

There exists a Frobenius endomorphism $F$ which verifies: $F^2 - cF + q = 0 \pmod{N}$, such that $c = a + b_1$ and this matrix $M_F \in M_2(\mathbb{Z}/N\mathbb{Z})$ is exactly $M$.

This Theorem is used to prove the following Theorem:

**Theorem 4.4.** Let $M = \begin{pmatrix} c - 1 & -A \\ B & 1 \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z})$ and $F_q$ a finite field with $q$ elements, such that $|c| \leq 2\sqrt{q}$, $B | A$, $B | c - 2AB = N = q + 1 - c$, we suppose: $(c, q) = 1$. Then there exists an ordinary elliptic curve $E$ over $F_q$, such that:

$$E(F_q) \simeq \mathbb{Z}/A \oplus \mathbb{Z}/B.$$ 

5 Cyclicity Statistics for the $A$-module $L^\Phi$

In this section, we make a statistic about the Drinfeld Modules $\Phi$ of rank 2, whose the structures $L^\Phi$ are cyclic, for this, we define $C(d, m, q)$ as been the ration of the number of (isomorphism classes of) Drinfeld modules of rank 2 with cyclic structure $L^\Phi$ to the number of $L$-isomorphisms classes of ordinary Drinfeld modules of rank 2, noted by $\#\{\Phi, \text{isomorphism, ordinary}\}$:

$$C(d, m, q) = \frac{\#\{\Phi, L^\Phi \text{ cyclic}\}}{\#\{\Phi, \text{isomorphism, ordinary}\}}.$$ 

As same, we define $N(d, m, q)$ as been the ration of the number of (isogeny classes of) Drinfeld modules of rank 2 with not cyclic structure $L^\Phi$ to the number of $L$-isomorphisms isogeny of ordinary Drinfeld modules of rank 2, noted by $\#\{\Phi, \text{isogeny, ordinary}\}$:
We remark that: $0 \leq C(d, m, q), N(d, m, q) \leq 1$. Since the no cyclicity of the structure $L^\Phi$ needs the fact that $i^2 | P^\Phi(1)$ and $i_2 | (c-2)$, it is natural to introduce $i$ (so $i_2$) in the calculus of $C(d, m, q)$ and $N(d, m, q)$.

We fix the characteristic polynomial $P^\Phi$, this means that we fix the isogeny classes of $\Phi$, and we define:

**Definition 5.1.** We note by
\[
\# \{ \Phi : L^\Phi = A_{(i_1)} \oplus A_{(i_2)} \}.
\]

**Remark 5.1.** The number $n(P^\Phi, i_2)$ is equal to the number of isomorphisms classes of $\Phi$ whole the $A$-module $L^\Phi \cong A_{(i_1)} \oplus A_{(i_2)}$, in one isogeny classes, from where is coming the correspondence between $\Phi$ and $i_2$.

For $n(P^\Phi, i_2)$ we have by the Theorem 3.1:

**Lemma 5.1.** Let $P^\Phi(X) = X^2 - cX + \mu P^m$ be the characteristic polynomial of an ordinary Drinfeld $A$-module $\Phi$ of rank 2, and let $i_2$ be an unitary polynomial of $A$. Then if $i_2 \mid c - 2$ we have: $n(P^\Phi, i_2) \geq 1$, else $n(P^\Phi, i_2) = 0$.

We can deduct:

**Corollary 5.1.** with the above notations:
\[
\# \{ \Phi, L^\Phi \text{ non cyclic} \} = \sum_{P^\Phi} \sum_{i_2, i_2^2 \mid P^\Phi(1)} n(P^\Phi, i_2).\# \{ i_2, i_2^2 \mid P^\Phi(1) \text{ and } i_2 \mid (c - 2) \},
\]
\[
\# \{ \Phi, L^\Phi \text{ cyclic} \} = \sum_{P^\Phi} \sum_{i_2, i_2^2 \mid P^\Phi(1)} n(P^\Phi, i_2).\# \{ i_2, i_2^2 \mid P^\Phi(1) \text{ and } i_2 \mid (c - 2) \};
\]

And if we note by $n_0(P^\Phi, i_2) = \# \{ \text{isogeny classes of } \Phi : L^\Phi = A_{(i_1)} \oplus A_{(i_2)} \}$, we have:
\[
n_0(P^\Phi, i_2) = 1.
\]

We note now by $\# \{ \Phi, \text{isogeny, ordinary} \}$ the number of isogeny classes, for an ordinary module $\Phi$, then we define:
\[
N_0(d, m, q) = \frac{\# \{ \text{isogeny classes of } \Phi, L^\Phi \text{ not cyclic} \}}{\# \{ \Phi, \text{isogeny, ordinary} \}},
\]
the same for
\[
C_0(d, m, q) = \frac{\# \{ \text{isogeny Classes of } \Phi, L^\Phi \text{ cyclic} \}}{\# \{ \Phi, \text{isogeny, ordinary} \}},
\]
We can so announce the following lemma:
Lemma 5.2. With the notations above, we have:

\[ N_0(d, m, q) = \frac{\#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 \mid (c-2)\}}{\#\{\Phi, \text{isogeny, ordinary}\}}, \]

\[ N(d, m, q) = \frac{\sum_{P_\Phi} \sum_{i_2, i_2^2 | P_\Phi(1)} n(\Phi, i_2).\#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 \mid (c-2)\}}{\#\{\Phi, \text{isomorphism, ordinary}\}}, \]

\[ C_0(d, m, q) = \frac{\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\}}{\#\{\Phi, \text{isogeny, ordinary}\}}, \]

\[ C(d, m, q) = \frac{\sum_{P_\Phi} \sum_{i_2, i_2^2 | P_\Phi(1)} n(\Phi, i_2).\#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 \mid (c-2)\}}{\#\{\Phi, \text{isomorphism, ordinary}\}}, \]

and \( N(d, m, q) + C(d, m, q) = 1, N_0(d, m, q) + C_0(d, m, q) = 1. \)

The calculus of \( \#\{\Phi, \text{isogeny, ordinary}\} \), for an ordinary \( A \)-module \( \Phi \), has been calculated in [3] and [4], as been:

Proposition 5.1. Let \( L = F_{q^n} \) and \( P \) the \( A \)-characteristic of \( L \).

We put \( m = [L : A/P] \) and \( d = \deg P \):

1. \( m \) is odd and \( d \) is odd:
   \[ \#\{\Phi, \text{isogeny, ordinary}\} = (q-1)(q^{\frac{m}{2}d}+1) - q^{\frac{m}{2}d}. \]

2. \( m.d \) even:
   \[ \#\{\Phi, \text{isogeny, ordinary}\} = (q-1)(q^{\frac{m}{2}d}+1 - q^{\frac{m}{2}d} - q^{\frac{m}{2}d}). \]

As for the number \( L \)-isomorphisms classes, we will need the following result, for the proof and more details see [9]:

Proposition 5.2. Let \( L \) be a finite extension of degree \( n \) over \( F_q \), then the number of \( L \)-isomorphisms classes of a Drinfeld \( A \)-module of rank 2 over \( L \) is \((q-1)q^n\) if \( n \) is odd and \( q^{n+1} - q^n + q^2 - q \) else.

And to calculate the number of \( L \)-isomorphisms classes for an ordinary Drinfeld modules, we will need to calculate the number of \( L \)-isomorphisms classes for a supersingular Drinfeld modules and subtract it from the global number of \( L \)-isomorphisms classes, for this, we have by [10]:

Proposition 5.3. Let \( L \) be a finite extension of \( n \) degrees over \( F_q \), then the number of \( L \)-isomorphisms classes of an supersingular Drinfeld \( A \)-module of rank 2, over \( L \) is \((q^{n^2})\), where \( n_2 = \text{pgcd}(2, n) \).

The calculus of \( C(d, m, q) \) will be calculated in function of the values of \( d \) and \( m \) which are two major values to determinate \( c \) because \( \deg c \leq \frac{m.d}{2} \).

And to calculate the number of \( L \)-isomorphisms classes existing in each isogeny classes, we need the following Definition for more information, see [13]:
Definition 5.2. Let $L$ be a finite extension of degree $n$ over $F_q$, we define $W(F)$ as been:

$$W(F) = \sum_{\Phi, F=Frobenius(\Phi)} \text{Weigh}(\Phi)$$

where:

$$\text{Weigh}(\Phi) = \frac{q-1}{\#\text{Aut}_L\Phi}.$$

$W(F)$ is the sum of weights (noted Weigh(Φ)) of number of $L$-isomorphisms classes existing in each isogeny classes of the module $\Phi$ which the Frobenius is $F$.

And to calculate $\#\text{Aut}_L\Phi$ we have the following lemma:

Lemma 5.3. Let $\Phi$ be an ordinary Drinfeld $A$-module of rank 2, over a finite field $L = F_{q^n}$, then:

$$\#\text{Aut}_L\Phi = q - 1.$$ By the previous lemma, we can see that Weight ($\Phi$) = $\frac{q-1}{\#\text{Aut}_L\Phi}$ = 1, that means:

Corollary 5.2. In the case of ordinary Drinfeld modules of rank 2, $W(F)$ is the number of $L$-isomorphisms classes existing in each isogeny classes.

Definition 5.3. Let $D$ be an imaginary discriminant and let $l$ a polynomial for which the square is a divisor of $D$ and let $h(D)$ the number of classes of the order for which the discriminant is $D$. We define the number of classes of Hurwitz for an imaginary discriminant $D$, noted $H(D)$ by:

$$H(D) = \sum_{l \mid D} h\left(\frac{D}{l^2}\right).$$

For more definitions and information about the numbers classess of Hurwitz, see [13] and [20].

Lemma 5.4. If $\alpha$ is an integral element over $A$, for which $O = A[\alpha]$ is an $A$-order, then $\text{disc}(A[\alpha])$ is equal to the discriminant of the minimal polynomial of $\alpha$.

What is interesting for us is the calculus of the $\text{disc}(A[F])$ and since $\text{disc}(A[F]) = \text{disc}(P_{\Phi})$. To calculate the number of classes $W(F)$, we have the following result, for proof see [13].

Proposition 5.4. Let $L$ be a finite extension of degree $n$ of a field $F_q$ and $F$ the Frobenius of $L$, then:

$$W(F) = H(\text{disc}(A[F])).$$

It remains for us to calculate $n(\Phi, i_2)$:
Lemma 5.5. Let $P_\Phi$ be the characteristic polynomial of an ordinary Drinfeld $A$-module of rank 2, over a finite field $L$ such that $L^\Phi = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$, and let $\Delta$ the discriminant of the characteristic polynomial of the Frobenius $F$, then :

$$n(P_\Phi, i_2) = H(O(\Delta/i_2^2)).$$

Proof. We know that to have $L^\Phi = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$, we have certainly :

$$\Phi(i_2) \simeq (A/i_2)^2 \subset L^\Phi,$$

that is equivalent to say, by the Proposition 4.3, that the $A$-order $O(\Delta/i_2^2) \subset \text{End}_L \Phi$ where $\Delta$ is always the discriminant of the characteristic polynomial of $F$, $P_\Phi$, and that :

$$n(P_\Phi, i_2) = H(O(\Delta/i_2^2)).$$

\[\square\]

We can calculate some values of $C(d, m, q)$ for some $d$ and $m$ :

6 The case : $d = m = 1$

In this case $L = A/P = F_q$, the $A$-module $L^\Phi = A/P$, so it is cyclic, that means that $C(1, 1, q) = 1$.

We can find this result by more explicit way :

Proposition 6.1. Let $L = F_{q^n}$ and $P$ the $A$-characteristic of $L$, $m = [L, A/P]$ and $d = \deg P$. We suppose $m = d = 1$. then :

$$C(1, 1, q) = C_0(1, 1, q) = 1.$$

Proof. $P_\Phi(1) = 1 - c + \mu P^m = 1 - c + \mu P$, $i_2^2 | P_\Phi(1) = i_2$ is a non null constant, then an element of $F_q^*$ so $(i_2) = A$ and $\frac{A}{i_1} \oplus \frac{A}{i_2} = \frac{A}{i_1}$, then $L^\Phi$ is cyclic, that means that $C(1, 1, q) = 1 \Rightarrow N(1, 1, q) = 0$.

To calculate $\#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 | (c - 2)\}$, we must have $i_2$ an element of $F_q^*$ and $\deg i_2 > 0$ \Rightarrow \#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 | (c - 2)\} = 0 and then :

$$N_0(1, 1, q) = \frac{\#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 | (c - 2)\}}{\#\{\Phi, \text{ isogeny, ordinary}\}} = 0$$

$\Rightarrow C_0(1, 1, q) = 1$. \[\square\]

By more precise way, we can announce :

Theorem 6.1. Let $L = F_{q^n}$ and $P$ the $A$-characteristic of $L$, $m = [L, A/P]$ and $d = \deg P$. Then:

$$C_0(d, m, q) = C(d, m, q) = 1 \Leftrightarrow m = d = 1.$$
Proof. We have just seen that \( C_0(1,1,q) = C(1,1,q) = 1 \).

Conversely and by the absurd : \( m.d > 1 \) (this means \( m.d \geq 2 \)), we take for example \( m = 1 \) and \( d = 2 \).

To have \( C_0(d,m,q) = C(d,m,q) = 1 \), we must have
\[
\# \{ i_2, i_2^2 \mid P_\Phi(1) \text{ and } i_2 \mid (c-2) \} = 0,
\]
what is not true, since if \( c = aT + b \), where \( a \in \mathbb{F}_q^* \) and \( b \in \mathbb{F}_q \), it is sufficient to have an unitary \( i_2 \) and such that : \( i_2 \mid (c-2) \).

Then for \( i_2 = a^{-1}(c-2) \) this stays compatible with the fact that \( a^{-2}(c-2)^2 \mid 1-c+\mu P \), since there are many solutions for the equation in \( i_2 \), i.e in \( a \) and \( b \):
\[
a^{-2}(c-2)^2 \mid 1-c+\mu P \Rightarrow a^{-2}(aT + b - 2)^2 \mid 1 - aT - b + \mu(T^2 + pT + p_0),
\]
which implies the equations : \( 2a^{-1}_1(b - 2) = \mu p_1 - a + \mu[a^{-1}(b-2)]^2 = 1 - b + \mu p_0 \Rightarrow 2^{-1} \mu [\mu p_1 - a] = 1 - b + \mu p_0 \) this gives a values of \( a \) for each value of \( b \), from where the many possibilities of \( i_2 \), for example \( i_2 = T - (\mu(2p_0 - p_1))^{-1} \), so it is more easy in the case which \( m.d > 2 \) to find an \( i_2 \), such that : \( i_2^2 \mid P_\Phi(1) \) and \( i_2 \mid (c-2) \).

7 The case: \( m = 1 \) and \( d = 2 \)

In this case \( n = m.d = 2 \), and \( n_2 = 2 \Rightarrow \# \{ \Phi, \text{isomorphism, ordinary} \} = q^3 - q - (q^2 - 1) = q^3 - q^2 - q + 1 \).

Proposition 7.1. Let \( L = \mathbb{F}_q^m \) and \( P \) the A-characteristic of \( L \), \( m = [L, A/P] \) and \( d = \deg P \). We suppose \( m = 1 \) and \( d = 2 \). Then:
\[
C_0(2,1,q) = \frac{q(q-1) - 5}{q(q-1) - 2}.
\]

\[
C(2,1,q) = \frac{q^3 - q^2 - q + 1 - \sum_{P \in \mathbb{F}_q^2} \sum_{2P \in \mathbb{F}_q^2} H(O(\frac{4^P}{4P})) + (q-1) \sum_{P \in \mathbb{F}_q^2} \sum_{2P \in \mathbb{F}_q^2} H(O(\frac{2^P}{4P}))}{q^3 - q^2 - q + 1}.
\]

Proof. We start by calculating :
\[
\frac{\# \{ i_2, i_2^2 \mid P_\Phi(1) \}}{\# \{ \Phi, \text{isogeny} \}}.
\]

For this, we distinguish between two cases, the case where \( c = 2 \) and the case where \( c \neq 2 \).

Then for \( c = 2 \) : \( i_2^2 \mid P_\Phi(1) \Rightarrow i_2^2 \mid \mu P \) this implies that if we put \( i_2 = T + j_2, j_2 \in \mathbb{F}_q \) and \( P(T) = T^2 + p_1 T + p_0 \) where \( p_1, p_0 \in \mathbb{F}_q \), are irreducibles, we will have \( p_1 = 2j_2 \) and \( \mu p_0 - 1 = \mu j_2 \) we will have then the equation \( \mu(p_0 - \frac{p_0}{4}) = 1 \Rightarrow \mu(p_0^2 - 4p_0) = -4 \), since the fact that \( p_0^2 - 4p_0 \) is not a square \( P \) is irreducible in \( A \), we will have -\( \mu \) no square, that means that...
the number of possible $\mu$ is $\frac{q-1}{2}$, if we consider the fact that $p_0, p_1$ are fixe, we will have $\frac{(q-1)}{2}$ solutions, then it remains to calculate : for the case $c \neq 2$, for this, we put : $i_2 = T + j_2$, $j_2 \in \mathbb{F}_q$ and $c = aT + b$ where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. The fact that $i_2 \mid (c - 2) \Rightarrow j_2 = \frac{b-2}{a}$ and since $i_2 \mid P_\Phi(1)$ we will have : $1 - (aT + b) + \mu(T^2 + p_1T + p_0) = \mu(T + j_2)^2 \Rightarrow 1 - b + \mu p_0 = \mu j_2^2$ and $\mu p_1 - a = 2\mu j_2$, then : $\mu = \frac{a}{p_1-2j_2} = \frac{a}{p_1-2\left(\frac{b-2}{a}\right)}$ and then :

$$\frac{a}{p_1-2\left(\frac{b-2}{a}\right)}[p_0 - \left(\frac{b-2}{a}\right)^2] + 1 - b = 0.$$ 

The solution numbers of this equation in $(a, b)$ ( $p_0, p_1$ are fixe ) give us $\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c - 2)\}$, then we will have $(q - 1)$ possible cases for $i_2$. Then :

$$N_0(2, 1, q) = \frac{\#\{i_2, i_2^2 \mid P_\Phi(1)\}}{\#\{\Phi, \text{ isogeny, ordinary}\}}$$

$$= \frac{(q - 1) + (q - 1)}{(q - 1)[(\frac{q-1}{2})q - 1]}$$

$$= \frac{3(q-1)}{(q-1)[(\frac{q-1}{2})q - 1]}$$

$$= \frac{3}{q(q-1) - 2} \Rightarrow$$

$$C_0(2, 1, q) = 1 - \frac{3}{q(q-1) - 2}$$

$$= \frac{q(q-1) - 5}{q(q-1) - 2}.$$

And for $N(2, 1, q)$ :

$$N(2, 1, q) = \frac{\sum\sum n(\Phi, i_2).\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ and } i_2 \mid (c - 2)\}}{\#\{\Phi, \text{ isomorphism, ordinary}\}}$$

$$= \frac{\sum\sum H(O(\frac{4-4\mu P}{i_2^2})) \cdot \frac{q-1}{2} + \sum\sum H(O(\frac{4-4\mu P}{i_2}))(q-1)}{q^3 - q^2 - q + 1}$$

$$= \frac{q-1}{2} \sum\sum H(O(\frac{4-4\mu P}{i_2^2})) + (q-1) \sum\sum H(O(\frac{4-4\mu P}{i_2}))$$

$$= \frac{q^3 - q^2 - q + 1}{q^3 - q^2 - q + 1}.$$ 

Finally : $C(2, 1, q) = 1 - N(2, 1, q)$

$$1 - \frac{q-1}{2} \sum\sum H(O(\frac{4-4\mu P}{i_2^2})) + (q-1) \sum\sum H(O(\frac{4-4\mu P}{i_2}))$$

$$= \frac{q^3 - q^2 - q + 1}{q^3 - q^2 - q + 1}.$$
and we remark first:

\[ p \text{ which is an equation in } (a, b, p) \]

In this case \( c = 2, i_2^2 | P_\Phi(1) = \mu P^2 - 1 \) we will have: \( 2\mu p = 2\mu j_2 \mu P^2 - 1 = \mu j_2^2 \) that means that \( p = j_2 \) and \( \mu(p^2 - j_2^2) = 1 \) so the contradiction, and then \( \#\{i_2, i_2^2 | P_\Phi(1)\} = 0 \). For \( c \neq 2 \) we calculate \( \#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 \mid (c - 2)\} \) and we remark first: \( i_2 \mid (c - 2) \Rightarrow j_2 = \frac{b - 2a}{a} \) and \( i_2^2 \mid P_\Phi(1) \) implies that: \( 2p\mu - a = 2\mu j_2 \) and \( p^2 + 1 - b = \mu j_2^2 \), finally we will have the equation:

\[ p^2 + 1 - b = \frac{a}{2p - 2(\frac{b - 2a}{a})} \frac{b - 2a}{a} j^2 \]

which is an equation in \( (a, b, p) \) and accept \( (q - 1) \) solutions, since the fact that \( p \) is fix, then:

\[
\begin{align*}
q^3 - q^2 - q + 1 - & \frac{1}{2p} \sum_{\Phi,i_2,i_2^2} H(O(\frac{\mu P}{i_2^2} + (q - 1) \sum_{\Phi,i_2,i_2^2} H(O(\frac{\mu P}{i_2^2}))}{q^3 - q^2 - q + 1}. 
\end{align*}
\]

\( \square \)

8 the case: \( m = 2 \) and \( d = 1 \)

In this case \( n = m.d = 2, \) and \( n_2 = 2 \Rightarrow \#\{\Phi, \text{ isomorphism, ordinary}\} = q^3 - q - (q^2 - 1) = q^3 - q^2 - q + 1 \).

**Proposition 8.1.** Let \( L = F_q^n \) and \( P \) the \( A \)-characteristic of \( L, m = [L, A/P] \) and \( d = \deg P \). We suppose that \( m = 2 \) and \( d = 1 \). Then:

\[
C_0(1, 2, q) = \frac{(q - 1)q - 4}{(q - 1)q - 2},
\]

\[
C(1, 2, q) = \frac{q^3 - q^2 - q + 1 - \sum_{\Phi,i_2,i_2^2} \sum_{i_2^2} H(O(\frac{\mu P}{i_2^2}))}{q^3 - q^2 - q + 1}.
\]

**Proof.** We put \( i_2 = T + j_2, j_2 \in F_q \) and \( P(T) = T + p \) where \( p \in F_q \). We start by calculate:

\[
N_0(1, 2, q) = \frac{\#\{i_2, i_2^2 | P_\Phi(1)\}}{\#\{\Phi, \text{ isomorphism, ordinary}\}}.
\]

In this case \( c = 2, i_2^2 | P_\Phi(1) = \mu P^2 - 1 \) we will have: \( 2\mu p = 2\mu j_2 \mu P^2 - 1 = \mu j_2^2 \) that means that \( p = j_2 \) and \( \mu(p^2 - j_2^2) = 1 \) so the contradiction, and then \( \#\{i_2, i_2^2 | P_\Phi(1)\} = 0 \). For \( c \neq 2 \) we calculate \( \#\{i_2, i_2^2 | P_\Phi(1) \text{ and } i_2 \mid (c - 2)\} \) and we remark first: \( i_2 \mid (c - 2) \Rightarrow j_2 = \frac{b - 2a}{a} \) and \( i_2^2 \mid P_\Phi(1) \) implies that: \( 2p\mu - a = 2\mu j_2 \) and \( p^2 + 1 - b = \mu j_2^2 \), finally we will have the equation:

\[
p^2 + 1 - b = \frac{a}{2p - 2(\frac{b - 2a}{a})} \frac{b - 2a}{a} j^2
\]

which is an equation in \( (a, b, p) \) and accept \( (q - 1) \) solutions, since the fact that \( p \) is fix, then:

\[
N_0(1, 2, q) = \frac{\#\{i_2, i_2^2 | P_\Phi(1)\}}{\#\{\Phi, \text{ isomorphism, ordinary}\}} = \frac{q - 1}{(q - 1)((\frac{q - 1}{2})q - 1)}
\]

\[
= \frac{1}{(\frac{q - 1}{2})q - 1}
\]

\[
\Rightarrow C_0(1, 2, q) = 1 - N_0(1, 2, q)
\]

\[
= 1 - \frac{1}{(\frac{q - 1}{2})q - 1}
\]

\[
= \frac{(q - 1)q - 4}{(q - 1)q - 2}
\]

\[ 20 \]
And for $N(1, 2, q)$:

$$N(1, 2, q) = \sum_{P \Phi} \sum_{i_2 \lfloor q, c-2 \rfloor} n(\Phi, i_2) \cdot \# \{ i_2, i_2^2 \mid P(1) \text{ and } i_2 \mid (c-2) \}$$

$$= \sum_{P \Phi \ i_2 \ i_2^2 \lfloor q, c-2 \rfloor} H(O(c^2 - 4\mu P)) \frac{(q-1)}{q(q+1)}.$$

In end:

$$C(1, 2, q) = 1 - \frac{\sum_{P \Phi \ i_2 \ i_2^2 \lfloor q, c-2 \rfloor} H(O(c^2 - 4\mu P))}{q(q+1)}.$$

### 8.1 \( \lim_{q \to \infty} C_0(d, m, q) \) and \( \lim_{q \to \infty} C(d, m, q) \) for \( m.d \leq 2 \)

By the calculus of \( C_0(d, m, q) \) and \( C(d, m, q) \) for \( m.d \leq 2 \), we have:

**Corollary 8.1.** Let \( L = F_q^n \) and \( P \) the \( A \)-characteristic of \( L \), \( m = [L, A/P] \) and \( d = \deg P \). Then:

$$\lim_{q \to \infty} C_0(1, 2, q) = \lim_{q \to \infty} C_0(2, 1, q) = 1,$$

$$\lim_{q \to \infty} C(1, 2, q) = \lim_{q \to \infty} C(2, 1, q) = 1.$$

**Proof.** Since \( C_0(1, 2, q) = \frac{q(q-1)-1}{q(q-1)/2} \), \( C_0(2, 1, q) = \frac{q(q-1)-5}{q(q-1)/2} \) et \( C_0(1, 1, q) = 1 \), where we can see that: \( m.d \leq 2 \), \( \lim_{q \to \infty} C_0(d, m, q) = 1 \). By other way, since \( C_0(d, m, q) \leq C(d, m, q) \leq 1 \) and by passing to the limit, we have: \( \lim_{q \to \infty} C(d, m, q) = 1 \), pour \( m.d \leq 2 \).

By the results above, we can give the following conjecture:

**Conjecture 8.1.** Let \( L = F_q^n \) and \( P \) the \( A \)-characteristic of \( L \), \( m = [L, A/P] \) and \( d = \deg P \). Then:

$$\lim_{q \to \infty} C(d, m, q) = \lim_{q \to \infty} C_0(d, m, q) = 1.$$
8.2 Discussion and open Questions

By the last conjecture we can ask whether for a big values of \(d\) and \(m\), we will have a cyclic modules? otherwise:
\[
\lim_{d \to \infty} C(d, m, q) = \lim_{d \to \infty} C_0(d, m, q) = 1?
\]
of same:
\[
\lim_{m \to \infty} C(d, m, q) = \lim_{m \to \infty} C_0(d, m, q) = 1?
\]
We can also ask whether the rank of a Drinfeld \(A\)-module \(\Phi\) is decisive for the cyclicity of \(A\)-module \(L^\Phi\)?

Lastly, it is legitimate to ask if we can generalize the Theorem 4.1 for a Drinfeld \(A\)-modules \(\Phi\) such that \(A\) is not \(F_q[T]\) and such that the rank of \(\Phi\) is more bigger than 2?

References

[1] Bruno Angles. Thèse de Doctorat : Modules de Drinfeld sur les corps finis, Université Paul Sabatier-Toulouse III, no d’ordre 1872, (1994).

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

[3] M. S M. AHMED. Endomorphism Rings and Isogenies Classes for a Drinfeld \(A\)-Modules of Rank 2 over Finite Fields, preprint IML, 2004.

[4] M. S M. AHMED. Modules de Drinfeld de rang 2 sur un corps fini, thèse de Doctorat, IML 2004.

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

[6] V.G. Drinfeld. Modules Elliptiques. Math, USSR Sbornik, 94 (136), 594-627, 656, (1974).

[7] V.G. Drinfeld. Modules Elliptiques II Math, USSR Sbornik, 102 (144), No 2, 182-194,325, (1977).

[8] Ernst-Ulrich Gekeler. On Finite Drinfeld Module. J. Algebra 141, (1991), 187-203.

[9] Ernst-Ulrich Gekeler and Brian A. Snyder. Drinfeld Modules Over Finite Fields. Drinfeld Modules, Modular Schemes and Application. Aldenbriesen, (1996).

[10] Igor Potemine. Thèse de Doctorat : Arithmétiques des Corps Globaux de Fonctions et Géométrie des Schémas Modulaires de Drinfeld, de l’Université Joseph Fourier(Grenoble I), (1997)

[11] J.P. Serre. Corps Locaux, Hermann (1968).
[12] Joseph. H. Silverman *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 106.

[13] J.K.Yu. *A Classe Number Relation Over Functions Fields*, J. Number Theory, 54, (1995), 318–340.

[14] J-K. Yu. *Isogenis of Drinfeld Modules Over Finite Fields*, J. Number of Theory 54 (1995), no 1, 161–171.

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

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

[17] R. Shoof. *Nonsingular Plane Cubic Curves Over Finite Filelds*, Journal of combinatoric theory, series A 46, (1987), 183-211.

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

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

[20] S.G. Vladut. *Cyclicity Statistics for Elliptic Curves Over Finite Fields*, Finite Fields Appl. 5 (1999), no 4, 354–363.

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