PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 7, July 1998, Pages 1955–1961
S 0002-9939(98)04337-8

SOME RESULTS ON FINITE DRINFELD MODULES

CHIH-NUNG HSU

(Communicated by William W. Adams)

Abstract. Let K be a global function field, ∞ a degree one prime divisor of K and let A be the Dedekind domain of functions in K regular outside ∞. Let H be the Hilbert class field of A, B the integral closure of A in H. Let ψ be a rank one normalized Drinfeld A -module and let $\mathfrak{P}$ be a prime ideal in B. We explicitly determine the finite A-module structure of $\psi(\mathrm{B}/\mathfrak{P}^N)$. In particular, if $\mathrm{K} = \mathbb{F}_q(t)$, q is an odd prime number and ψ is the Carlitz $\mathbb{F}_q[t]$-module, then the finite $\mathbb{F}_q[t]$-module $\psi(\mathbb{F}_q[t]/\mathfrak{P}^N)$ is always cyclic.

1. Introduction

Recall that $\mathrm{G}_m(\mathbb{Z}/p^N\mathbb{Z}) = (\mathbb{Z}/p^N\mathbb{Z})^\times$ is always cyclic except for the case that $p = 2$ and $N \geq 3$; if $N \geq 3$, then $(\mathbb{Z}/2^N\mathbb{Z})^\times$ is the direct product of two cyclic groups, one of order 2, the other of order 2^{N-2}. Let X be a smooth, projective, geometrically connected curve defined over the finite field $\mathbb{F}_q$ with q elements and let ∞ be a rational point on X. We set K to be the function field of X over $\mathbb{F}_q$ and $\mathrm{A} \subset \mathrm{K}$ to be the Dedekind domain of functions regular outside ∞. We will consider the Drinfeld A-modules. From the view point of class field theory, these modules are interesting arithmetic objects over function fields. In particular, the rank one Drinfeld A-modules play a role entirely analogous to the important role played by G_m over number fields. This naturally leads us to explore an analogous phenomenon for rank one Drinfeld A-modules.

Let K_∞ be the completion of K with respective to ∞ and let C_∞ be the completion of the algebraic closure of K_∞ with respect to ∞. Let $\mathrm{C}_\infty\{\tau\} = \mathrm{End}_{\mathbb{F}_q}(\mathrm{G}_a/\mathrm{C}_\infty)$ be the twisted polynomial ring in the q^{th} power Frobenius mapping τ. A rank one Drinfeld A-module ψ over C_∞ is an injective ring homomorphism $\psi : \mathrm{A} \to \mathrm{C}_\infty\{\tau\}$ such that the constant coefficient of $\psi_a(\tau)$ is equal to a and $\deg_\tau \psi_a(\tau) = -\mathrm{Ord}_\infty a$ for all $a \in \mathrm{A}$. A sign-function (cf. [5] and [3]) $\mathrm{sgn} : \mathrm{K}_\infty^\times \to \mathbb{F}_q^\times$ is a co-section of the inclusion map $\mathbb{F}_q^\times \hookrightarrow \mathrm{K}_\infty^\times$ such that $\mathrm{sgn}(\alpha) = 1$ for all $\alpha \in \mathrm{K}_\infty^\times$ with $\alpha - 1$ vanishing at ∞. A Drinfeld A-module ψ of rank one over C_∞ is said to be sgn-normalized if the leading coefficient of $\psi_a(\tau)$ in τ is equal to $\mathrm{sgn}(a)$ for all $0 \neq a \in \mathrm{A}$. It is known [5] that any Drinfeld A-module of rank one over C_∞ is isomorphic to a sgn-normalized A-module ψ over H, where H is the Hilbert class field of A, i.e., H is the maximal abelian extension of K such that the extension H / K completely splits over ∞ and is unramified over every finite place of K.

Received by the editors July 23, 1996 and, in revised form, December 26, 1996.
1991 *Mathematics Subject Classification.* Primary 11G09; Secondary 11A05.
Key words and phrases. Drinfeld modules, Hilbert class field.

Let B be the integral closure of A in H and let ψ be a rank one sgn-normalized Drinfeld A-module. Let $\mathfrak{M}$ be an ideal in B. Via the action of $\psi \pmod{\mathfrak{M}}$, $\mathrm{B}/\mathfrak{M}$ becomes a finite A-module. We denote this by $\psi(\mathrm{B}/\mathfrak{M})$. This finite A-module plays the role of $\mathrm{G}_m(\mathbb{Z}/p^N\mathbb{Z})$. The purpose of this note is to determine the A-module structure of $\psi(\mathrm{B}/\mathfrak{M})$. It is sufficient to consider the case $\psi(\mathrm{B}/\mathfrak{P}^N)$, where $\mathfrak{P}$ is a prime ideal in B. The structure of $\psi(\mathrm{B}/\mathfrak{P}^N)$ is obtained in Theorems 2.1 and 2.2. In particular, if ψ is the Carlitz $\mathbb{F}_q[t]$-module ([3], chapter 3) and $q \neq 2$, then $\psi(\mathrm{B}/\mathfrak{P}^N)$ is always cyclic (cf. Corollaries 2.1 and 2.2). The Carlitz case is completely analogous to the classical case.

In section 3, we discuss the relations between $\mathrm{B}_{\mathfrak{P}}$ and $\varprojlim \psi(\mathrm{B}/\mathfrak{P}^N)$ via the exponential and logarithm functions of the sgn-normalized Drinfeld module ψ.

2. The structure of $\psi(\mathrm{B}/\mathfrak{P}^N)$

Let the notation $X, \mathbb{F}_q, \infty, \mathrm{K}, \mathrm{A}, \mathrm{H}, \mathrm{B}$ and sgn be as in the introduction. If M is a commutative $\mathbb{F}_q$-algebra, we let $\mathrm{M}\{\tau\}$ denote the composition ring of Frobenius polynomials in τ, where τ is the q^{th} power mapping. From now on, we let ψ be a sgn-normalized rank one Drinfeld A-module over H, i.e., $\psi : \mathrm{A} \to \mathrm{H}\{\tau\}$ is a rank one Drinfeld A-module over H such that for any $a \in \mathrm{A}$, the leading coefficient of $\psi_a(\tau)$ is equal to $\mathrm{sgn}(a)$. It is known that $\psi_a(\tau) \in \mathrm{B}\{\tau\}$ for all $a \in \mathrm{A}$. Thus, via ψ, B becomes an A-module. We denote this module by $\psi(\mathrm{B})$ and denote the action $\psi_a(\tau)(b)$ by b^a for all $a \in \mathrm{A}, b \in \mathrm{B}$. Let $\mathfrak{M}$ be an ideal in B. Since $\psi(\mathrm{A}) \subset \mathrm{B}\{\tau\}$, it follows that, via $\psi \pmod{\mathfrak{M}}$, $\mathrm{B}/\mathfrak{M}$ becomes a finite A-module. We denote this finite module by $\psi(\mathrm{B}/\mathfrak{M})$. If the decomposition of $\mathfrak{M}$ is equal to $\mathfrak{P}_1^{N_1}\mathfrak{P}_2^{N_2}\cdots\mathfrak{P}_L^{N_L}$, where $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_L$ are prime ideals in B, then, by the Chinese remainder theorem, we have

$$\psi(\mathrm{B}/\mathfrak{M}) \cong \bigoplus_{i=1}^{L} \psi(\mathrm{B}/\mathfrak{P}_i^{N_i}).$$

Thus to determine the A-module structure of $\psi(\mathrm{B}/\mathfrak{M})$, it is sufficient to consider the case $\psi(\mathrm{B}/\mathfrak{P}^N)$, where $\mathfrak{P}$ is a prime ideal in B. Let $\wp = \mathfrak{P} \cap \mathrm{A}$ and let f be the dimension of the vector space $\mathrm{B}/\mathfrak{P}$ over $\mathrm{A}/\wp$. It follows from class field theory that $\mathrm{Norm}_{\mathrm{K}}^{\mathrm{H}}\mathfrak{P} = \wp^f$ is a principal ideal in A. We let $\wp^f = (\pi_\wp)$ for the unique element $\pi_\wp \in \mathrm{A}$ with $\mathrm{sgn}(\pi_\wp) = 1$. It is known that $\psi(\mathrm{B}/\mathfrak{P})$ is a cyclic A-module with Euler-Poincaré characteristic $\pi_\wp - 1$ (cf. [3], chapter 4), i.e., as A-module,

$$\psi(\mathrm{B}/\mathfrak{P}) \cong \mathrm{A}/(\pi_\wp - 1).$$

We let $\psi_\wp(\tau)$ be the monic generator of the left ideal of $\mathrm{H}\{\tau\}$ generated by $\psi_a(\tau)$ for all $a \in \wp$. We also denote the polynomial $\psi_\wp(\tau)(x)$ in x by $x^\wp$ for all $x \in \mathrm{H}$. The important property of the polynomial $\psi_\wp(\tau)$, $\wp \subset \mathrm{A}$ a prime ideal, is the following (cf. [5], Proposition 11.4):

$$f(x) = \psi_\wp(\tau)(x)/x = x^\wp/x$$

is an Eisenstein polynomial over B at any prime ideal $\mathfrak{P}$ above $\wp$. Let $c_\wp = f(0) \in \mathrm{B}$. Then we have $\deg_{\mathfrak{P}} c_\wp = 1$. If $\wp$ is a rational point on the curve X (i.e., $\wp$ is a prime ideal in A of degree one) defined over $\mathbb{F}_2$, then $\psi_\wp(\tau) = c_\wp\tau^0 + \tau^1 \in \mathrm{B}\{\tau\}$, i.e., $x^\wp = \psi_\wp(\tau)(x) = c_\wp x + x^2$, where $c_\wp \in \mathfrak{P}$ but $c_\wp \notin \mathfrak{P}^2$.

Lemma 2.1. *Suppose that N is a positive integer, $\mathfrak{P}$ and $\wp$ are as above. Then for any $b_1, b_2 \in \psi(\mathrm{B})$, if $b_1 \equiv b_2 \pmod{\mathfrak{P}^N}$, then $b_1^\wp \equiv b_2^\wp \pmod{\mathfrak{P}^{N+1}}$.*

Proof. We may write $b_1 = b_2 + x$ for some $x \in \mathfrak{P}^N$. Then, by the Eisenstein polynomial property,

$$b_1^{\wp} = (b_2 + x)^{\wp} = b_2^{\wp} + x^{\wp} \equiv b_2^{\wp} \pmod{\mathfrak{P}^{N+1}}. \quad \square$$

Lemma 2.2. *Suppose that $\mathfrak{P}$, $\wp$ and $c_\wp$ are as above. Then*:

(1) *If $N \geq 2$ is a positive integer, then $x^{\wp^{N-2}} \equiv x \cdot c_\wp^{N-2} \pmod{\mathfrak{P}^N}$ for all $x \in \mathfrak{P}$ except for the case that $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$.*

(2) *If $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$ (i.e., $\wp$ is a prime ideal of* A *of degree one) and $N \geq 3$ is a positive integer, then*

$$x^{\wp^{N-3}} \equiv x \cdot c_\wp^{N-3} \pmod{\mathfrak{P}^N}$$

for all $x \in \mathfrak{P}^2$.

(3) *If $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$, then for all $x \in \mathfrak{P}, x \not\equiv 0, c_\wp \pmod{\mathfrak{P}^2}$, we have $x^{\wp} \in \mathfrak{P}^2$ but $x^{\wp} \notin \mathfrak{P}^3$.*

Proof. Assertion (1) is obvious for $N = 2$. Now suppose that it is true for $N \geq 2$, i.e.,

$$x^{\wp^{N-2}} \equiv x \cdot c_\wp^{N-2} \pmod{\mathfrak{P}^N}.$$

We show that it is true for $N + 1$. Applying Lemma 2.1 and the Eisenstein polynomial property, we have

$$(x^{\wp^{N-2}})^{\wp} \equiv (x \cdot c_\wp^{N-2})^{\wp} \equiv c_\wp \cdot (x \cdot c_\wp^{N-2}) + (x \cdot c_\wp^{N-2})^{q^{\deg \wp}} \pmod{\mathfrak{P}^{N+1}}.$$

If $q \neq 2$ or $q = 2$ and $\wp$ is not a rational point on the curve X over $\mathbb{F}_2$ (i.e., $q^{\deg \wp} \geq 3$), then we have $(x \cdot c_\wp^{N-2})^{q^{\deg \wp}} \in \mathfrak{P}^{N+1}$. Hence

$$x^{\wp^{N-1}} \equiv x c_\wp^{N-1} \pmod{\mathfrak{P}^{N+1}}.$$

This completes the proof of (1). The proof of (2) is similar.

To prove (3), since $x \in \mathfrak{P}$ and $\deg_{\mathfrak{P}} c_\wp = 1$, $x^{\wp} = c_\wp \cdot x + x^2 = x(x + c_\wp) \in \mathfrak{P}^2$. The assertion $x^{\wp} \notin \mathfrak{P}^3$ follows from the facts that the characteristic of B is 2 and $x \not\equiv 0, c_\wp \pmod{\mathfrak{P}^2}$. $\square$

Lemma 2.3. *Suppose that $\mathfrak{P}$ and $\wp$ are as above. Then*:

(1) *If $N \geq 2$ is a positive integer and $x \in \mathfrak{P}, x \notin \mathfrak{P}^2$, then the submodule $\langle \overline{x} \rangle$ of $\psi(\mathrm{B}/\mathfrak{P}^N)$ generated by $\overline{x} = x \pmod{\mathfrak{P}^N} \in \psi(\mathrm{B}/\mathfrak{P}^N)$ is isomorphic to $\mathrm{A}/\wp^{N-1}$ except for the case when $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$.*

(2) *Suppose that $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$. If $N \geq 3$ is a positive integer and $x \in \mathfrak{P}^2, x \notin \mathfrak{P}^3$, then the submodule $\langle \overline{x} \rangle$ of $\psi(\mathrm{B}/\mathfrak{P}^N)$ generated by $\overline{x} = x \pmod{\mathfrak{P}^N} \in \psi(\mathrm{B}/\mathfrak{P}^N)$ is isomorphic to $\mathrm{A}/\wp^{N-2}$.*

(3) *Suppose that $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$ and $N \geq 2$. Then for all $x \in \mathfrak{P}, x \not\equiv 0, c_\wp \pmod{\mathfrak{P}^2}$, the submodule $\langle \overline{x} \rangle$ of $\psi(\mathrm{B}/\mathfrak{P}^N)$ generated by $\overline{x} = x \pmod{\mathfrak{P}^N} \in \psi(\mathrm{B}/\mathfrak{P}^N)$ is isomorphic to $\mathrm{A}/\wp^{N-1}$.*

Proof. By Lemma 2.2 (1), $x^{\wp^{N-1}} \equiv x \cdot c_\wp^{N-1} \pmod{\mathfrak{P}^{N+1}}$. Since $\deg_{\mathfrak{P}} c_\wp = 1$ and $x \in \mathfrak{P}$, we have

$$x^{\wp^{N-1}} \equiv 0 \pmod{\mathfrak{P}^N}.$$

Again by Lemma 2.2 (1), $\deg_{\mathfrak{P}} c_\wp = 1$ and $x \in \mathfrak{P}, x \notin \mathfrak{P}^2$,

$$x^{\wp^{N-2}} \equiv x \cdot c_\wp^{N-2} \not\equiv 0 \pmod{\mathfrak{P}^N}.$$

Since $\langle \overline{x} \rangle$ is a cyclic A-module, $\langle \overline{x} \rangle$ is isomorphic to $\mathrm{A}/\wp^{N-1}$. The proof of (2) is similar, and the proof of (3) follows from Lemma 2.2 (3), (2). □

Let $[\mathrm{H}:\mathrm{K}] = fr$ be the class number of A, where $f = [\mathrm{B}/\mathfrak{P} : \mathrm{A}/\wp]$. Then the main result is

Theorem 2.1. *Suppose that $\mathfrak{P}, \wp, \pi_\wp$ and f are as above. Then*

$$\psi(\mathrm{B}/\mathfrak{P}^N) \cong \begin{cases} \mathrm{A}/(\pi_\wp - 1) & \text{if } N = 1, \\ \mathrm{A}/(\pi_\wp - 1) \oplus \left(\mathrm{A}/\wp^{N-1}\right)^f & \text{if } N > 1, \end{cases}$$

except for the case when $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$.

Proof. The case $N = 1$ follows from the theory of Drinfeld modules over finite fields (cf. [3], Chapter 4). We suppose that $N \geq 2$. Given $x \in \psi(\mathrm{B})$. Since $\psi(\mathrm{B}/\mathfrak{P}) \cong \mathrm{A}/(\pi_\wp - 1)$, it follows that $x^{\pi_\wp - 1} \equiv 0 \pmod{\mathfrak{P}}$. By Lemma 2.2 (1), we have

$$(x^{\pi_\wp - 1})^{\wp^{N-1}} \equiv 0 \pmod{\mathfrak{P}^N}.$$

This implies that the Euler-Poincaré characteristic of any A-cyclic submodule of $\psi(\mathrm{B}/\mathfrak{P}^N)$ divides $(\pi_\wp - 1)\wp^{N-1}$.

Since $\psi(\mathrm{A}) \subset \mathrm{B}\{\tau\}$, $\psi(\mathfrak{P}/\mathfrak{P}^N)$ is a submodule of $\psi(\mathrm{B}/\mathfrak{P}^N)$. We have

$$\dim_{\mathbb{F}_q} \psi(\mathfrak{P}/\mathfrak{P}^N) = (N-1)\dim_{\mathbb{F}_q} \mathrm{B}/\mathfrak{P} = f(N-1)\dim_{\mathbb{F}_q} \mathrm{A}/\wp.$$

Since $x^{\wp^{N-1}} \equiv 0 \pmod{\mathfrak{P}^N}$ for all $x \in \mathfrak{P}$ (by Lemma2.2 (1)), as A-module

$$\psi(\mathfrak{P}/\mathfrak{P}^N) \cong \bigoplus_{i=1}^{l} \mathrm{A}/\wp^{n_i}$$

for suitable positive integers $1 \leq n_1 \leq n_2 \leq \cdots \leq n_l \leq N-1$ such that

$$n_1 + n_2 + \cdots + n_l = (N-1)f.$$

By Lemma 2.2 (1) and Lemma 2.3 (1), the subset of elements $\bar{x}$ in $\psi(\mathfrak{P}/\mathfrak{P}^N)$ such that $x^{\wp^{N-2}} \equiv 0 \pmod{\mathfrak{P}^N}$ is equal to $\psi(\mathfrak{P}^2/\mathfrak{P}^N)$. Counting cardinalities, we must have

$$l = f, \quad n_1 = n_2 = \cdots = n_f = N-1.$$

Thus we get

$$\psi(\mathfrak{P}/\mathfrak{P}^N) \cong (\mathrm{A}/\wp^{N-1})^f.$$

Next, we take $g \in \mathrm{B}$ such that $g \pmod{\mathfrak{P}}$ is a generator of $\psi(\mathrm{B}/\mathfrak{P})$. We let $\langle \bar{g} \rangle$ be the A-submodule of $\psi(\mathrm{B}/\mathfrak{P}^N)$ generated by $\bar{g} = g \pmod{\mathfrak{P}^N}$ in $\psi(\mathrm{B}/\mathfrak{P}^N)$. We define the A-module homomorphism $\chi : \langle \bar{g} \rangle \to \psi(\mathrm{B}/\mathfrak{P})$ by $\chi(x \pmod{\mathfrak{P}^N}) = x \pmod{\mathfrak{P}}$ for all $x \pmod{\mathfrak{P}^N}$ in $\langle \bar{g} \rangle$. Since $g \pmod{\mathfrak{P}}$ is a generator of $\psi(\mathrm{B}/\mathfrak{P})$ and $\chi(g \pmod{\mathfrak{P}^N}) = g \pmod{\mathfrak{P}}$, χ is a surjective homomorphism of $\langle \bar{g} \rangle$ onto $\psi(\mathrm{B}/\mathfrak{P})$. This implies that $(\pi_\wp - 1)$ divides the Euler-Poincaré characteristic of $\psi(\mathrm{B}/\mathfrak{P}^N)$, because $\langle \bar{g} \rangle$ is a submodule of $\psi(\mathrm{B}/\mathfrak{P}^N)$. Combining these, we obtain that $(\pi_\wp - 1)\wp^{f(N-1)}$ divides the Euler-Poincaré characteristic of $\psi(\mathrm{B}/\mathfrak{P}^N)$; this implies that the Euler-Poincaré characteristic of $\psi(\mathrm{B}/\mathfrak{P}^N)$ is equal to

$(\pi_\wp - 1)\wp^{f(N-1)}$; hence $\langle \bar{g} \rangle$ (or $\psi(\mathrm{B}/\mathfrak{P}^N)$) contains an A-submodule which is isomorphic to $\mathrm{A}/(\pi_\wp - 1)$. Therefore, we obtain that

$$\psi(\mathrm{B}/\mathfrak{P}^N) \cong \mathrm{A}/(\pi_\wp - 1) \oplus \left(\mathrm{A}/\wp^{N-1}\right)^f. \quad \square$$

Theorem 2.2. *Suppose that $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$. Then*

$$\psi(\mathrm{B}/\mathfrak{P}^N) \cong \begin{cases} \mathrm{A}/(\pi_\wp - 1), & \text{if } N = 1; \\ \mathrm{A}/(\pi_\wp - 1) \oplus (\mathrm{A}/\wp)^f, & \text{if } N = 2; \\ \mathrm{A}/(\pi_\wp - 1) \oplus \mathrm{A}/\wp \oplus (\mathrm{A}/\wp^{N-1})^{f-1} \oplus \mathrm{A}/\wp^{N-2}, & \text{if } N \geq 3. \end{cases}$$

Proof. The case $N = 1$ is standard. We suppose that $N \geq 2$. Using Lemmas 2.2 and 2.3, the proof is almost the same as the proof of Theorem 2.1. We obtain that the Euler-Poincaré characteristic of any A-cyclic submodule of $\psi(\mathrm{B}/\mathfrak{P}^N)$ divides $(\pi_\wp-1)\wp^{N-1}$, the finite A-module $\psi(\mathfrak{P}/\mathfrak{P}^N)$ is annihilated by $\wp^{N-1}$, and $\psi(\mathrm{B}/\mathfrak{P}^N)$ contains an A-submodule which is isomorphic to $\mathrm{A}/(\pi_\wp-1)$. From these, we deduce that the Euler-Poincaré characteristic of $\psi(\mathrm{B}/\mathfrak{P}^N)$ is equal to $(\pi_\wp-1)\wp^{f(N-1)}$ and

$$\psi(\mathrm{B}/\mathfrak{P}^N) \cong \mathrm{A}/(\pi_\wp - 1) \oplus \psi(\mathfrak{P}/\mathfrak{P}^N).$$

Next, we deal with the A-module structure of $\psi(\mathfrak{P}/\mathfrak{P}^N)$. For $N = 2$, since $\psi(\mathfrak{P}/\mathfrak{P}^2)$ is annihilated by $\wp$, counting the dimension of $\psi(\mathfrak{P}/\mathfrak{P}^2)$ over $\mathrm{A}/\wp$, we obtain that $\psi(\mathfrak{P}/\mathfrak{P}^2) \cong (\mathrm{A}/\wp)^f$. For $N \geq 3$, since $\wp$ is a rational point on the curve X defined over $\mathbb{F}_2$ and $[\mathrm{B}/\mathfrak{P} : \mathrm{A}/\wp] = f$, as abelian group $\mathfrak{P}/\mathfrak{P}^2 \cong (\mathrm{A}/\wp)^f \cong \mathbb{F}_2^f$. Let S be the A-submodule of $\psi(\mathfrak{P}/\mathfrak{P}^N)$ generated by elements $x \pmod{\mathfrak{P}^N}$ is such that $x \in \mathfrak{P}$ but $x \notin \mathfrak{P}^2$. We define the abelian group homomorphism $\chi : S \to \psi(\mathfrak{P}^2/\mathfrak{P}^3)$ by $\chi(x \pmod{\mathfrak{P}^N}) = x^\wp \pmod{\mathfrak{P}^3}$ for all $x \pmod{\mathfrak{P}^N} \in S$. From Lemma 2.2 (3), we know that if $x \pmod{\mathfrak{P}^N} \in S$ is such that $\chi(x \pmod{\mathfrak{P}^N}) = 0$, then $x \equiv 0, c_\wp \pmod{\mathfrak{P}^2}$. This implies that $\dim_{\mathbb{F}_2} \chi(S) = f - 1$. Combining this with Lemma 2.3 (3) and the fact that S is annihilated by $\wp^{N-1}$, we obtain that

$$S \cong \mathrm{A}/\wp \oplus (\mathrm{A}/\wp^{N-1})^{f-1}.$$

Since $\chi(c_\wp \pmod{\mathfrak{P}^N}) = 0$ and $c_\wp \pmod{\mathfrak{P}^N}) \in S$, there exists an element $x \in \mathfrak{P}^2, x \notin \mathfrak{P}^3$, such that $x \pmod{\mathfrak{P}^3} \notin \chi(S)$. By Lemma 2.2 (2), we know that $\langle x \pmod{\mathfrak{P}^N} \rangle$ is a submodule of $\psi(\mathfrak{P}/\mathfrak{P}^N)$ which is isomorphic to $\mathrm{A}/\wp^{N-2}$. Combining these and counting the dimension of $\psi(\mathfrak{P}/\mathfrak{P}^N)$ over $\mathrm{A}/\wp \cong \mathbb{F}_2$, we obtain that

$$\psi(\mathrm{B}/\mathfrak{P}^N) \cong \mathrm{A}/(\pi_\wp - 1) \oplus \mathrm{A}/\wp \oplus (\mathrm{A}/\wp^{N-1})^{f-1} \oplus \mathrm{A}/\wp^{N-2}.$$

This completes the proof. $\square$

As an application, we let $\mathrm{A} = \mathbb{F}_q[t]$ and let ϕ be the Carlitz A-module, i.e., $\phi : \mathrm{A} \to \mathbb{F}_2(t)\{\tau\}$ is given by

$$\phi_t(\tau) = t\tau^0 + \tau^1.$$

Then we have

Corollary 2.1. *If N is a positive integer and $\wp = (p)$ is a prime ideal in* A *generated by the monic polynomial p, then the finite* A*-module*

$$\phi(\mathrm{A}/\wp^N) \cong \mathrm{A}/(p^N - p^{N-1})$$

is cyclic except for the case when $\mathbb{F}_q$ equals $\mathbb{F}_2$ and $p \mid t(t+1)$.

Corollary 2.2. *If N is a positive integer, $\mathrm{A}=\mathbb{F}_2[t]$, $\wp=(p)$ with $p=t$ or $t+1\in\mathrm{A}$, then the finite* A*-module $\phi(\mathrm{A}/\wp^N)$ is isomorphic to*

$$\begin{cases}\mathrm{A}/(p-1), & \text{if } N=1;\\ \mathrm{A}/(t^2+t), & \text{if } N=2;\\ \mathrm{A}/(t^2+t)\oplus\mathrm{A}/(p^{N-2}) & \text{if } N\geq 3.\end{cases}$$

3. Passage to the limit

Let the notation $X,\mathbb{F}_q,\infty,\mathrm{K},\mathrm{A},\mathrm{H},\mathrm{B},f,\pi_\wp$ and sgn be as before. Let ψ be a sgn-normalized rank one Drinfeld A-module over H. Suppose that $\mathfrak{P}$ and $\wp$ are as in section 2 and $\wp$ does not correspond to a rational point on X if $q=2$. It is well-know that there exists a lattice $\mathfrak{A}\zeta$, $\zeta\in\mathrm{C}_\infty,\mathfrak{A}$ an ideal of A, of rank one such that ψ is determined by this lattice. The exponential function e_ψ associated to $\mathfrak{A}\zeta$ is defined to be

$$e_\psi(x)=z\prod_{a\in\mathfrak{A}}\left(1-\frac{x}{a\cdot\zeta}\right)\in\mathrm{H}\{\{\tau\}\}.$$

Let $\mathrm{H}_\mathfrak{P}$ (resp. $\mathrm{K}_\wp$) be the completion fields associated to $\mathfrak{P}$ (resp. $\wp$). Let $\mathrm{B}_\mathfrak{P}\subset\mathrm{H}_\mathfrak{P}$ and $\mathrm{A}_\wp\subset\mathrm{K}_\wp$ be the rings of integers.

It follows from theorem 2.1 that as A-module

$$\begin{aligned}\psi(\mathrm{B}_\mathfrak{P})&=\psi(\varprojlim\mathrm{B}/\mathfrak{P}^N)\\ &=\varprojlim\psi(\mathrm{B}/\mathfrak{P}^N)\\ &=\varprojlim\mathrm{A}/(\pi_\wp-1)\oplus\left(\mathrm{A}/\wp^{N-1}\right)^f\\ &=\mathrm{A}/(\pi_\wp-1)\oplus\mathrm{A}_\wp^f\\ &=\mathrm{A}/(\pi_\wp-1)\oplus\mathrm{B}_\mathfrak{P}\,.\end{aligned}$$

We know that the coefficients of e_ψ are in H and these coefficients are obtained by solving a recursion equation via any ψ_a, $a\in\mathrm{A},a\notin\mathbb{F}_q$ (cf. [3], Lemma 4.6.5). We can deduce from this recursion that e_ψ converges in a neighborhood of 0. Thus there exist element $\alpha\in\mathrm{H}_\mathfrak{P}$ such that $e(x)=e_\psi(\alpha\cdot x)$ is an analytic injective function of $\mathrm{B}_\mathfrak{P}$ into $\mathrm{B}_\mathfrak{P}$. By the property of the exponential function e_ψ, we obtain that $e(ax)=\psi_a(e(x))$ for all $a\in\mathrm{A}$. Combining these, we have

Theorem 3.1. *As* A*-module,*

$$\psi(\mathrm{B}_\mathfrak{P})\cong\begin{cases}\mathrm{A}/(\pi_\wp-1)\oplus\mathrm{A}/\wp\oplus\mathrm{B}_\mathfrak{P} & \text{if } q=2 \text{ and } \wp \text{ is a rational point};\\ \mathrm{A}/(\pi_\wp-1)\oplus\mathrm{B}_\mathfrak{P} & \text{otherwise.}\end{cases}$$

Moreover, one has an analytic map $e:\mathrm{B}_\mathfrak{P}\to\psi(\mathrm{B}_\mathfrak{P})$ satisfying the following commutative diagram:

$$\begin{array}{ccc}\mathrm{B}_\mathfrak{P} & \xrightarrow{\quad e\quad} & \psi(\mathrm{B}_\mathfrak{P})\\ {\scriptstyle a}\big\downarrow & & \big\downarrow{\scriptstyle\psi_a}\\ \mathrm{B}_\mathfrak{P} & \xrightarrow{\quad e\quad} & \psi(\mathrm{B}_\mathfrak{P})\end{array}\quad.$$

References

[1] E. -U. Gekeler 'Drinfeld Modular Curves', LNM 1231, Springer-Verlag (1986). MR **88b:**11077
[2] E. -U. Gekeler 'On finite Drinfeld Modules', J. Algebra 141 (1991), pp. 187–203. MR **92e:**11064
[3] David Goss 'Basic Structures of Function Field Arithmetic', Springer-Verlag (1996). CMP 97:05
[4] D. R. Hayes 'Explicit class field theory for ration function fields', Transations of the American Mathematical Society, vol 189 (1974), pp. 77 – 91. MR **48:**8444
[5] D. R. Hayes 'A Brief introduction to Drinfeld modules', in 'The Arithmetic of Function Fields' (edited by D. Goss, D. R. Hayes and M. I. Rosen), (1992), pp. 1–32. MR **93m:**11050
[6] K. Ireland and M. Rosen 'A Classical Introduction to Modern Number Theory', Springer-Verlag. MR **92e:**11001
[7] J. K. Yu 'Isogenies of Drinfeld modules over finite fields', J. Number Theory 54 (1995), pp. 161–171. MR **96i:**11060

Department of Mathematics, National Taiwan Normal University, 88 Sec. 4 Ting-Chou Road, Taipei, Taiwan

E-mail address: maco@math.ntnu.edu.tw