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 P be a prime ideal in B. We explicitly determine the finite A-module structure of ψ(B/PN). In particular, if K = Fq(t), q is an odd prime number and ψ is the Carlitz Fq[t]-module, then the finite Fq[t]-module ψ(Fq[t]/PN) is always cyclic.

1. Introduction

Recall that Gm(Z/pNZ) = (Z/pNZ)× is always cyclic except for the case that p = 2 and N ≥ 3; if N ≥ 3, then (Z/2NZ)× is the direct product of two cyclic groups, one of order 2, the other of order 2N−2. Let X be a smooth, projective, geometrically connected curve defined over the finite field Fq with q elements and let ∞ be a rational point on X. We set K to be the function field of X over Fq and A ⊂ 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 Gm 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 C∞{τ} = EndGq(Ga/C∞) be the twisted polynomial ring in the qth power Frobenius mapping τ. A rank one Drinfeld A-module ψ over C∞ is an injective ring homomorphism ψ : A → C∞{τ} such that the constant coefficient of ψa(τ) is equal to a and degψa(τ) = −Ord∞a for all a ∈ A. A sign-function (cf. [5] and [3]) sgn : K∞ → Fq× is a co-section of the inclusion map Fq× → K∞× such that sgn(α) = 1 for all α ∈ K∞× with α − 1 vanishing at ∞. A Drinfeld A-module ψ of rank one over C∞ is said to be sgn-normalized if the leading coefficient of ψa(τ) in τ is equal to sgn(a) for all 0 ≠ a ∈ 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.

©1998 American Mathematical Society

1955
Let B be the integral closure of A in H and let ψ be a rank one sgn-normalized Drinfeld A-module. Let M be an ideal in B. Via the action of ψ (mod M), B/M becomes a finite A-module. We denote this by ψ(B/M). This finite A-module plays the role of \( \mathbb{G}_m(\mathbb{Z}/p^N\mathbb{Z}) \). The purpose of this note is to determine the A-module structure of ψ(B/M). It is sufficient to consider the case ψ(B/P^N), where P is a prime ideal in B. The structure of ψ(B/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 ψ(B/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 \( B_\mathfrak{P} \) and \( \varprojlim \psi(B/P^N) \) via the exponential and logarithm functions of the sgn-normalized Drinfeld module ψ.

2. The structure of \( \psi(B/P^N) \)

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

\[
\psi(B/M) \cong \bigoplus_{i=1}^L (\psi(B/M_i^N)).
\]

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

\[
\psi(B/\mathfrak{P}) \cong A/(\pi_\varphi - 1).
\]

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

\[
f(x) = \psi_\varphi(\tau)(x)/x = x^\varphi/x
\]

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

Lemma 2.1. Suppose that \( N \) is a positive integer, \( \mathfrak{P} \) and \( \varphi \) are as above. Then for any \( b_1, b_2 \in \psi(B) \), if \( b_1 \equiv b_2 \) (mod \( \mathfrak{P}^N \)), then \( b_1^\varphi \equiv b_2^\varphi \) (mod \( \mathfrak{P}^{N+1} \)).
Proof. We may write $b_1 = b_2 + x$ for some $x \in \mathcal{P}^N$. Then, by the Eisenstein polynomial property,

$$\left(b_1^p = (b_2 + x)^p = b_2^p + x^p \equiv b_2^p \pmod{\mathcal{P}^{N+1}}\right).$$

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

1. If $N \geq 2$ is a positive integer, then $x^{\wp N-2} \equiv x \cdot c_\wp^{N-2} \pmod{\mathcal{P}^N}$ for all $x \in \mathcal{P}$ 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

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

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

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

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

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

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

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

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 $(x \cdot c_\wp^{N-2})q^{\deg \wp} \in \mathcal{P}^{N+1}$. Hence

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

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

To prove (3), since $x \in \mathcal{P}$ and $\deg \wp c_\wp = 1$, $x^p = c_\wp \cdot x + x^2 = x(x + c_\wp) \in \mathcal{P}^2$.

The assertion $x^p \not\in \mathcal{P}^3$ follows from the facts that the characteristic of $B$ is 2 and $x \not\equiv 0, c_\wp \pmod{\mathcal{P}^2}$.

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

1. If $N \geq 2$ is a positive integer and $x \in \mathcal{P}, x \not\in \mathcal{P}^2$, then the submodule $\langle x \rangle$ of $\psi(B/\mathcal{P}^N)$ generated by $\overline{x} = x \pmod{\mathcal{P}^N} \in \psi(B/\mathcal{P}^N)$ is isomorphic to $A/\wp^{N-1}$ 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 $x \in \mathcal{P}^2, x \not\in \mathcal{P}^3$, then the submodule $\langle x \rangle$ of $\psi(B/\mathcal{P}^N)$ generated by $\overline{x} = x \pmod{\mathcal{P}^N} \in \psi(B/\mathcal{P}^N)$ is isomorphic to $A/\wp^{N-2}$.

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

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

$$x^{\wp N-1} \equiv 0 \pmod{\mathcal{P}^N}.$$
Since $x$ is cyclic, $x$ is isomorphic to $\mathbb{Z}/p$. Thus $x$ is isomorphic to $\mathbb{Z}/p$. We consider $\mathbb{Z}/p$ as a $\mathbb{Z}$-module. Since $p$ is prime, $\mathbb{Z}/p$ is a field.

**Theorem 2.1.** Suppose that $\mathfrak{p}, \varphi, \pi, f$ are as above. Then

$$\psi(B/\mathfrak{p}) \cong \left\{ \begin{array}{ll}
A/(\pi \varphi - 1) & \text{if } N = 1, \\
A/(\pi \varphi - 1) \oplus (A/\varphi^{N-1})f & \text{if } N > 1,
\end{array} \right.$$  

except for the case when $\varphi$ 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 $x \in \psi(B)$. Since $\psi(B/\mathfrak{p}) \cong A/(\pi \varphi - 1)$, it follows that $x^{\varphi - 1} \equiv 0 \pmod{\mathfrak{p}}$. By Lemma 2.2 (1), we have

$$(x^{\varphi - 1})^{\varphi^{N-1}} \equiv 0 \pmod{\mathfrak{p}^N}.$$  

This implies that the Euler-Poincaré characteristic of any cyclic submodule of $\psi(B/\mathfrak{p})$ divides $(\varphi - 1)\varphi^{N-1}$.

Since $\psi(A) \subset B\{x\}$, $\psi(B/\mathfrak{p})$ is a submodule of $\psi(B/\mathfrak{p})$. We have

$$\dim_{\mathfrak{p}} \psi(B/\mathfrak{p}) = (N - 1)\dim_{\mathfrak{p}} B/\mathfrak{p} = f(N - 1)\dim_{\mathfrak{p}} A/\varphi.$$  

Since $x^{\varphi - 1} \equiv 0 \pmod{\mathfrak{p}^N}$ for all $x \in \mathfrak{p}$ (by Lemma 2.2 (1)), as $A$-module

$$\psi(B/\mathfrak{p}) \cong \bigoplus_{i=1}^{l} A/\varphi^{n_i}$$  

for suitable positive integers $1 \leq n_1 \leq n_2 \leq \cdots \leq n_l \leq (N - 1)f$. By Lemma 2.2 (1) and Lemma 2.3 (1), the subset of elements $x$ in $\psi(B/\mathfrak{p})$ such that $x^{\varphi - 1} \equiv 0 \pmod{\mathfrak{p}^N}$ is equal to $\psi(B/\mathfrak{p})$. Counting cardinalities, we must have

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

Thus we get

$$\psi(B/\mathfrak{p}) \cong (A/\varphi^{N-1})^f.$$  

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

$$ \psi(B/\mathcal{P}^N) \cong A/(\pi_\phi - 1) \oplus (A/\phi^{N-1})^f. \qed $$

**Theorem 2.2.** Suppose that $\phi$ is a rational point on the curve $X$ defined over $F_2$. Then

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

**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 $\psi(B/\mathcal{P}^N)$ divides $(\pi_\phi - 1)\phi^{N-1}$, the finite $A$-module $\psi(B/\mathcal{P}^N)$ is annihilated by $\phi^{N-1}$, and $\psi(B/\mathcal{P}^N)$ contains an $A$-submodule which is isomorphic to $A/(\pi_\phi - 1)$. From these, we deduce that the Euler-Poincaré characteristic of $\psi(B/\mathcal{P}^N)$ is equal to $(\pi_\phi - 1)\phi^{f(N-1)}$ and

$$ \psi(B/\mathcal{P}^N) \cong A/(\pi_\phi - 1) \oplus \psi(\mathcal{P}/\mathcal{P}^N). $$

Next, we deal with the $A$-module structure of $\psi(\mathcal{P}/\mathcal{P}^N)$. For $N = 2$, since $\psi(\mathcal{P}/\mathcal{P}^2)$ is annihilated by $\phi$, counting the dimension of $\psi(\mathcal{P}/\mathcal{P}^2)$ over $A/\phi$, we obtain that $\psi(\mathcal{P}/\mathcal{P}^2) \cong (A/\phi)^f$. For $N \geq 3$, since $\phi$ is a rational point on the curve $X$ defined over $F_2$ and $[B/\mathcal{P} : A/\phi] = f$, as abelian group $\mathcal{P}/\mathcal{P}^2 \cong (A/\phi)^f \cong \mathcal{P}_2^f$. Let $S$ be the $A$-submodule of $\psi(\mathcal{P}/\mathcal{P}^N)$ generated by elements $x \pmod{\mathcal{P}^N}$ such that $x \in \mathcal{P}$ but $x \not\in \mathcal{P}^2$. We define the abelian group homomorphism $\chi : S \to \psi(\mathcal{P}^2/\mathcal{P}^3)$ by $\chi(x \pmod{\mathcal{P}^N}) = x^\phi \pmod{\mathcal{P}^3}$ for all $x \pmod{\mathcal{P}^N} \in S$. From Lemma 2.2 (3), we know that if $x \pmod{\mathcal{P}^N} \in S$ is such that $\chi(x \pmod{\mathcal{P}^N}) = 0$, then $x \equiv 0, c_\phi \pmod{\mathcal{P}^2}$. This implies that $\dim F_2 \chi(S) = f - 1$. Combining this with Lemma 2.3 (3) and the fact that $S$ is annihilated by $\phi^{N-1}$, we obtain that

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

Since $\chi(c_\phi \pmod{\mathcal{P}^N}) = 0$ and $c_\phi \pmod{\mathcal{P}^N}) \in S$, there exists an element $x \in \mathcal{P}^2, x \not\in \mathcal{P}^3$, such that $x \pmod{\mathcal{P}^3} \not\in \chi(S)$. By Lemma 2.2 (2), we know that $\langle x \pmod{\mathcal{P}^N} \rangle$ is a submodule of $\psi(\mathcal{P}/\mathcal{P}^N)$ which is isomorphic to $A/\phi^{N-2}$. Combining these and counting the dimension of $\psi(\mathcal{P}/\mathcal{P}^N)$ over $A/\phi \cong \mathcal{P}_2$, we obtain that

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

This completes the proof. \qed

As an application, we let $A = F_q[t]$ and let $\phi$ be the Carlitz $A$-module, i.e., $\phi : A \to F_2(t)\{\tau\}$ is given by

$$ \phi(t) = t^{\tau^3} + \tau. $$

Then we have

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

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

is cyclic except for the case when $F_q$ equals $F_2$ and $p | t(t + 1)$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Corollary 2.2. If $N$ is a positive integer, $A = \mathbb{F}_2[t]$, $\varphi = (p)$ with $p = t$ or $t + 1 \in A$, then the finite $A$-module $\phi(A / \varphi^N)$ is isomorphic to

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

3. Passage to the limit

Let the notation $X, \mathbb{F}_q, \infty, K, A, H, f, \pi, \wp$, and $\sgn$ be as before. Let $\psi$ 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-known that there exists a lattice $\mathfrak{A}\zeta, \zeta \in \mathbb{C}\infty, \mathfrak{A}$ an ideal of $A$, of rank one such that $\psi$ is determined by this lattice. The exponential function $e_\psi$ associated to $\mathfrak{A}\zeta$ is defined to be

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

Let $H_\wp$ (resp. $K_\wp$) be the completion fields associated to $\wp$ (resp. $\wp$). Let $B_\wp \subset H_\wp$ and $A_\wp \subset K_\wp$ be the rings of integers.

It follows from theorem 2.1 that as $A$-module

$$
\psi(B_\wp) = \psi(\varprojlim B / \wp^N)
$$

$$
= \varprojlim \psi(B / \wp^N)
$$

$$
= \varprojlim A / (\pi_\wp - 1) \oplus (A / \varphi^N)^f
$$

$$
= A / (\pi_\wp - 1) \oplus A_{\wp}^f
$$

$$
= A / (\pi_\wp - 1) \oplus B_{\wp}.
$$

We know that the coefficients of $e_\psi$ are in $H$ and these coefficients are obtained by solving a recursion equation via any $\psi_a, a \in A, a \not\in \mathbb{F}_q$ (cf. [3], Lemma 4.6.5). We can deduce from this recursion that $e_\psi$ converges in a neighborhood of $0$. Thus there exist element $\alpha \in H_\wp$ such that $e(x) = e_\psi(\alpha \cdot x)$ is an analytic injective function of $B_\wp$ into $B_{\wp}$. By the property of the exponential function $e_\psi$, we obtain that $e(ax) = \psi_a(e(x))$ for all $a \in A$. Combining these, we have

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

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

Moreover, one has an analytic map $e : B_\wp \rightarrow \psi(B_\wp)$ satisfying the following commutative diagram:

$$
\begin{array}{ccc}
B_\wp & \xrightarrow{e} & \psi(B_\wp) \\
\downarrow a & & \downarrow \psi_a \\
B_{\wp} & \xrightarrow{e} & \psi(B_{\wp})
\end{array}
$$
REFERENCES


Department of Mathematics, National Taiwan Normal University, 88 Sec. 4 Ting-Chou Road, Taipei, Taiwan
E-mail address: maco@math.ntnu.edu.tw