Canad. Math. Bull. Vol. **38** (1), 1995 pp. 3–10

TORSION POINTS OF DRINFELD MODULES

SUNGHAN BAE AND JAKYUNG KOO

ABSTRACT. The finiteness of K-rational torsion points of a Drinfeld module of rank 2 over a locally compact complete field K with a discrete valuation is proved.

0. **Introduction.** In this note we show the finiteness of the K-rational torsion points of a Drinfeld module of rank 2 over K where K is a locally compact complete field with a discrete valuation. Then as an easy consequence, we get the finiteness of torsion points when K is a global function field, which is the analogue of the finiteness of the K-rational torsion points of an elliptic curve defined over a number field K.

Throughout the paper we fix the following notations unless otherwise stated;

$$A = \mathbb{F}_q[T],\ q \text{ a power of a prime } p.$$
$$K = \text{complete field with respect to a discrete valuation } v.$$
$$R = \text{the ring of integers of } K$$
$$\mathfrak{m} = \text{the maximal ideal of } R$$
$$\pi = \text{a uniformizer of } \mathfrak{m}.$$
$$k = R/\mathfrak{m}, \text{ the residue field.}$$

1. **Preliminary.** In this note we mean by a Drinfeld module over K a Drinfeld A-module of rank 2, unless otherwise stated. Thus a Drinfeld module ϕ is completely determined by

$$\phi_T = T + g\tau + \Delta\tau^2.$$

We call Δ the *discriminant* of ϕ and $j = g^{q+1}/\Delta$ the *j-invariant* of ϕ. We say that a Drinfeld module ϕ is *minimal* if $v(\Delta)$ is minimal among the Drinfeld modules which are K-isomorphic to ϕ with g and Δ integral. Then it can be easily verified that a Drinfeld module ϕ is minimal if and only if ϕ is defined over R and $v(\Delta) < q^2 - 1$ or $v(g) < q - 1$.

For a Drinfeld module ϕ over R, we denote by $\bar{\phi}$ the reduction of ϕ modulo $\mathfrak{m}$. We say that ϕ has *nondegenerate reduction* if $\bar{\phi}$ is a Drinfeld module of rank 2 over k. For a Drinfeld module ϕ over K, we say that ϕ has *stable* reduction if there exists a Drinfeld module ϕ' over R which is K-isomorphic to ϕ so that $\bar{\phi}'$ is a Drinfeld module of rank at least 1, ϕ has *good* reduction if, in addition, rank of $\bar{\phi}'$ is 2, and *bad* reduction otherwise.

The first author was partially supported by Non Directed Research Fund, Korea Research Foundation 1993.
The second author was partially supported by KOSEF Research Grant 91-08-00-07.
Received by the editors October 18, 1993.
AMS subject classification: 11G09.

We say that ϕ has *potential stable* (resp. *good*) reduction if there exists a finite extension L of K so that ϕ, as a Drinfeld module over L, has stable (resp. good) reduction. The followings are easy to verify.

PROPOSITION 1.1. *Let ϕ be a Drinfeld module over K.*

a) Let L be an unramified extension of K. Then the reduction type of ϕ over K is the same as the reduction type of ϕ over L.

b) ϕ always has potential stable reduction.

PROPOSITION 1.2. *A Drinfeld module ϕ over K has potential good reduction if and only if its j-invariant is integral.*

For a Drinfeld module ϕ we set

$$\begin{aligned} \mathrm{Tor}_\phi(K) &= \{x \in K : \phi_a(x) = 0 \text{ for some } a \in A\} \\ \mathrm{Tor}_\phi(R) &= \{x \in R : \phi_a(x) = 0 \text{ for some } a \in A\} \\ \mathrm{Tor}_\phi(\mathfrak{m}) &= \{x \in \mathfrak{m} : \phi_a(x) = 0 \text{ for some } a \in A\}. \end{aligned}$$

When ϕ is defined over R, then $\mathrm{Tor}_\phi(R)$ and $\mathrm{Tor}_\phi(\mathfrak{m})$ are also A-modules via ϕ. From now on we always assume that ϕ is defined over R unless otherwise stated. Put

$$\mathfrak{p} = \mathrm{Ker}(A \longrightarrow R \longrightarrow R/\mathfrak{m}).$$

We say that $\mathfrak{p}$ is the *divisorial characteristic* of k. Let $\bar{\phi}$ denote the reduction of ϕ with respect to $\mathfrak{m}$.

PROPOSITION 1.3. *Let ϕ be a Drinfeld module over R and $a \in A$ be relatively prime to $\mathfrak{p}$.*

(a) $\mathrm{Tor}_\phi(\mathfrak{m})$ *has no nontrivial points of order a.*

(b) The reduction map

$$\mathrm{Tor}_\phi(R)[a] \longrightarrow \mathrm{Tor}_{\bar{\phi}}(k)[a]$$

is an isomorphism, where $\mathrm{Tor}_\phi(R)[a] = \{x \in R : \phi_a(x) = 0\}$.

PROOF. Let $x \in \mathfrak{m}$ be nonzero. Then $v(x) > 0$. Since ϕ is defined over R,

$$v\big(\phi_a(x)\big) = v(ax) = v(x) > 0.$$

Therefore $\phi_a(x) \neq 0$ and this proves a), and b) follows from a) and Hensel's lemma.

REMARK 1.4. In view of Proposition 1.3 one might think $\mathrm{Tor}_\phi(K)$, $\mathrm{Tor}_\phi(R)$ and $\mathrm{Tor}_\phi(\mathfrak{m})$ as the analogues of $E(K)$, $E_0(K)$ and $E_1(K)$, respectively, of an elliptic curve E over K. For precise definitions of $E(K)$, $E_0(K)$ and $E_1(K)$, we refer to [S], Chapter VII. However, unlike the classical case the reduction map

$$\mathrm{Tor}_\phi(R) \longrightarrow \mathrm{Tor}_\phi(k)$$

is not surjective. For example, let $R = \mathbb{F}_q[T]$ and ϕ is defined by

$$\phi_T = T - \tau + \tau^2.$$

https://doi.org/10.4153/CMB-1995-001-4 Published online by Cambridge University Press

Then all the elements of $k = \mathbb{F}_q$ are the roots of $\overline{\phi_T} = 0$, but there exist no nonzero torsion points of ϕ in R.

If ϕ has nondegenerate reduction, then it is easy to see that $\mathrm{Tor}_\phi(K) = \mathrm{Tor}_\phi(R) \subset R$. Let Q be an irreducible polynomial in A. Define the Tate-module

$$T_Q(\phi) = \varprojlim \big(\mathrm{Tor}_\phi(K)[Q^n]\big).$$

Let $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ where K^{sep} is the separable closure of K, and let I be the inertia group. For a set Σ on which G acts, we say that Σ is *unramified* if the action of the inertia group I on Σ is trivial.

PROPOSITION 1.5. *Suppose that ϕ has good reduction.*

a) Let $a \in A$ be relatively prime to $\mathfrak{p}$. Then $\mathrm{Tor}_\phi(K^{\mathrm{sep}})[a]$ *is unramified.*

b) Let $Q \notin \mathfrak{p}$ be an irreducible polynomial. Then $T_Q(\phi)$ is unramified.

PROOF. Exactly the same method as in the classical case gives the result. (See [S] VII, §4).

REMARK 1.6. The converse of Proposition 1.5 is also true. For its proof we refer to [T].

2. **Finiteness of Torsion points.** In this section we will prove that $\mathrm{Tor}_\phi(K)$ is finite if K is locally compact. Let $p(T)$ be the monic generator of $\mathfrak{p}$ with $d = \deg\big(p(T)\big)$.

LEMMA 2.1. *For any A-algebra S, let ϕ be a Drinfeld module over S. Write*

$$\phi_{p(T)} = p(T) + a_1\tau + \cdots + a_{2d}\tau^{2d}.$$

Then $p(T)$ divides a_i in S for $1 \leq i \leq d-1$.

PROOF. Let $S = A[g, \Delta]$ with g and Δ two independent transcendental elements over A. Then we know from the general theory that $p(T)$ divides a_i in $S = \mathbb{F}_q[g, \Delta, T]$ for $1 \leq i < d$. Then by specializing g and Δ, we get the result.

LEMMA 2.2. *Let ϕ be a Drinfeld module over R. If a nonzero element x in* $\mathrm{Tor}_\phi(\mathfrak{m})$ *has the exact order $p(T)^n$, $n \geq 1$, then*

$$v(x) \leq \frac{v\big(p(T)\big)}{q^{dn} - q^{d(n-1)}}.$$

PROOF. We will use the induction on n. By Lemma 2.1

$$\phi_{p(T)}(X) = p(T)Xf(X) + X^{q^d} g(X),$$

with $\deg f(X) \leq q^{d-1} - 1$ and $f(0) = 1$. Suppose that $\phi_{p(T)}(x) = 0$ with $x \in \mathfrak{m} - \{0\}$. Then

$$0 = p(T)xf(x) + x^{q^d} g(x).$$

Thus

$$v\big(p(T)xf(x)\big) = v\big(x^{q^d} g(x)\big) \geq v(x^{q^d}).$$

Since $f(0) = 1$ and $v(x) > 0$, $v\big(p(T)xf(x)\big) = v\big(p(T)x\big)$. Therefore

$$v(x) \leq \frac{v\big(p(T)\big)}{q^d - 1}.$$

Now suppose that x has the exact order $p(T)^{n+1}$. Then

$$\begin{aligned} v\big(\phi_{p(T)}(x)\big) &= v\big(p(T)xf(x) + x^{q^d} g(x)\big) \\ &\geq \min\big\{v\big(p(T)x\big), v(x^{q^d})\big\} > 0. \end{aligned}$$

Thus $\phi_{p(T)}(x)$ lies in $\mathfrak{m}$ and has exact order $p(T)^n$. Hence by the induction hypothesis,

$$v\big(\phi_{p(T)}(x)\big) \leq \frac{v\big(p(T)\big)}{q^{dn} - q^{d(n-1)}}.$$

Therefore

$$\frac{v\big(p(T)\big)}{q^{dn} - q^{d(n-1)}} \geq \min\big\{v\big(p(T)x\big), v(x^{q^d})\big\}.$$

But we cannot have

$$\frac{v\big(p(T)\big)}{q^{dn} - q^{d(n-1)}} \geq v\big(p(T)x\big).$$

Hence

$$\frac{v\big(p(T)\big)}{q^{dn} - q^{d(n-1)}} \geq v(x^{q^d}) = q^d v(x).$$

So we get

$$v(x) \leq \frac{v\big(p(T)\big)}{q^{d(n+1)} - q^{dn}}.$$

EXAMPLE. Let ϕ be a Drinfeld module defined over A. Let x be a nonzero element in A of order a. If a is not a prime power, then x is a unit in $A_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of A by Proposition 1.3. If $a = p(T)^n$, then

$$\frac{v\big(p(T)\big)}{q^{dn} - q^{d(n-1)}} < 1$$

unless $\deg p(T) = 1$, $q = 2$ and $n = 1$. Thus, for $q \geq 3$,

$$\mathrm{Tor}_\phi(A) \subset (A^* = \mathbb{F}_q^*) \cup \{0\} = \mathbb{F}_q.$$

Let $a(T)$ be a polynomial in A with degree d. Then we can write

$$\phi_{a(T)}(X) = \sum_{\ell=0}^{2d} a_\ell X^{q^\ell}.$$

Then a_ℓ is a polynomial in g and Δ with coefficients in A.

PROPOSITION 2.3. *If ϕ has integral j-invariant, then for $x \in \mathrm{Tor}_\phi(K)$*

$$v(x) \geq -\frac{v(\Delta)}{q^2-1}.$$

In particular, if ϕ is minimal, then

$$\mathrm{Tor}_\phi(K) = \mathrm{Tor}_\phi(R).$$

PROOF. The case that $j = 0$ is easy, thus we assume that $j \neq 0$. Suppose that $x \neq 0$ is a root of $\phi_{a(T)}(x) = 0$ for some $a(T)$ in A. Then it is easy to see that

$$v(a_\ell) \geq \frac{q^\ell - 1}{q^2-1} v(\Delta) \quad \text{if } \ell \text{ is even}$$

and

$$v(a_\ell) \geq \frac{q^\ell - q}{q^2-1} v(\Delta) + v(g) \quad \text{if } \ell \text{ is odd}$$

because $0 \leq v(j) = v(\frac{g^{q+1}}{\Delta}) = (q+1)v(g) - v(\Delta)$. Also

$$v(a_{2d}) = \frac{q^{2d}-1}{q^2-1} v(\Delta).$$

Because $\sum a_\ell x^{q^\ell} = 0$, we must have

$$v(a_{2d}x^{q^d}) \geq v(a_\ell x^{q^\ell})$$

for some ℓ. Hence from the above discussion, if ℓ is even,

$$\frac{q^{2d}-1}{q^2-1} v(\Delta) + q^{2d} v(x) \geq \frac{q^\ell - 1}{q^2-1} v(\Delta) + q^\ell v(x)$$

and if ℓ is odd

$$\frac{q^{2d}-1}{q^2-1} v(\Delta) + q^{2d} v(x) \geq \frac{q^\ell - q}{q^2-1} v(\Delta) + v(g) + q^\ell v(x).$$

For ℓ even,

$$v(x) \geq -\frac{1}{q^2-1} v(\Delta).$$

For ℓ odd,

$$\begin{aligned} v(x) &\geq -\frac{1}{q^2-1} v(\Delta) + \frac{v(g)}{q^{2d}-q^\ell} - \frac{q-1}{(q^{2d}-q^\ell)(q^2-1)} v(\Delta) \\ &= -\frac{1}{q^2-1} v(\Delta) + \frac{1}{q^{2d}-q^\ell}\left(v(g) - \frac{v(\Delta)}{q+1}\right) \\ &\geq -\frac{1}{q^2-1} v(\Delta). \end{aligned}$$

If ϕ is minimal, then $v(\Delta) < q^2 - 1$, and so $v(x) \geq 0$.

PROPOSITION 2.4. *Suppose that ϕ has nonintegral j-invariant. If $x \in K$ is a torsion point of ϕ, then*

$$v(x) \geq -\frac{1}{q^2 - q} v(\Delta).$$

PROOF. Let $x \neq 0$ be a root of $\phi_{a(T)}(X) = 0$. As in the proof of Proposition 2.3, put

$$\phi_{a(T)}(X) = \sum_{\ell=0}^{2d} a_\ell X^{q^\ell}.$$

Since $v(\Delta) > (q+1)v(g) > 0$, we have

$$v(a_\ell) \geq \frac{q^\ell - 1}{q - 1} v(g) \geq 0 \quad \text{if } \ell \leq d$$

and

$$v(a_\ell) \geq \frac{q^{2i} - 1}{q^2 - 1} v(\Delta) + q^{2i} \frac{q^{d-i} - 1}{q - 1} v(g) \geq \frac{q^{2i} - 1}{q^2 - 1} v(\Delta) \quad \text{if } \ell = d + i,\ i < d.$$

But $v(a_{2d}) = \frac{q^{2d}-1}{q^2-1} v(\Delta)$. Hence

$$\frac{q^{2d} - 1}{q^2 - 1} v(\Delta) + q^{2d} v(x) \geq v(a_\ell) + q^\ell v(x).$$

for some $0 \leq \ell \leq 2d$. Thus

$$v(x) \geq -\frac{q^{2d} - 1}{(q^{2d} - q^\ell)(q^2 - 1)} v(\Delta) \quad \text{if } \ell \leq d,$$

and

$$v(x) \geq -\frac{q^{2d} - q^{2i}}{(q^{2d} - q^{d+i})(q^2 - 1)} v(\Delta) \quad \text{if } \ell = d + i,\ i < d.$$

However, it is not hard to see that

$$\frac{q^{2d} - 1}{q^{2d} - q^\ell} \leq \frac{q + 1}{q} \quad \text{and} \quad \frac{q^{2d} - q^{2i}}{q^{2d} - q^{d+i}} \leq \frac{q + 1}{q},$$

if $l \leq d$ and $i < d$. Therefore we get the result.

THEOREM 2.5. *Suppose that a Drinfeld module ϕ has a nonintegral torsion point. Let x be a torsion element with minimal $v(x)$. Then $q^2 - q$ divides $v(\Delta) - v(g)$ and*

$$v(x) = \frac{1}{q^2 - q}\big(v(g) - v(\Delta)\big).$$

PROOF. Assume first that ϕ is minimal. Note that $(q+1)v(g) < v(\Delta)$ by Proposition 2.3, and $v(g) < q-1$ since ϕ is minimal. Choose x in $\mathrm{Tor}_\phi(K)$ with minimal $v(x)$ so that

$$v(x) \leq v\big(\phi_T(x)\big) = v(x) + v(T + gx^{q-1} + \Delta x^{q^2-1}).$$

Assume first that $v(x) \geq \frac{-v(\Delta)}{q^2-1}$, then $v(\Delta x^{q^2-1}) \geq 0$. Thus

$$v(g) + (q-1)v(x) = v(gx^{q-1}) \geq 0,$$

since $v(x)$ is minimal. Then $v(x) \geq \frac{-v(g)}{q-1} > -1$. Hence $v(x) \geq 0$, which is a contradiction. Therefore we must have $v(\Delta x^{q^2-1}) < 0$. Since $v(x)$ is minimal, we must have

$$v(\Delta x^{q^2-1}) = v(gx^{q-1}).$$

Hence

$$v(x) = \frac{1}{q^2-q}\big(v(g) - v(\Delta)\big),$$

as desired. Now suppose that ϕ is not necessarily minimal. Pick $c \in K$ such that $\phi' = c\phi c^{-1}$ is minimal. Let g', Δ' correspond to ϕ'. Then

$$v(g') = v(g) + (1-q)v(c)$$

and

$$v(\Delta') = v(\Delta) + (1-q^2)v(c).$$

For a torsion element x of ϕ with minimal valuation cx is a torsion element of ϕ' with minimal valuation. Thus

$$\begin{aligned} v(cx) &= \frac{1}{q^2-q}\big(v(g') - v(\Delta')\big) \\ &= \frac{1}{q^2-q}\big(v(g) + (1-q)v(c) - v(\Delta) - (1-q^2)v(c)\big). \end{aligned}$$

Hence

$$v(x) = \frac{1}{q^2-q}\big(v(g) - v(\Delta)\big).$$

THEOREM 2.6. *Suppose that K is locally compact. Then for a Drinfeld module ϕ over K, $\mathrm{Tor}_\phi(K)$ is finite.*

PROOF. We may assume that ϕ is minimal. By Proposition 2.4 $\mathrm{Tor}_\phi(K)$ is a bounded set. Hence $\overline{\mathrm{Tor}_\phi(K)}$, the closure of $\mathrm{Tor}_\phi(K)$, is compact in K. Since $\mathfrak{m}$ is both open and closed in K, $\overline{\mathrm{Tor}_\phi(\mathfrak{m})} = \overline{\mathrm{Tor}_\phi(K)} \cap \mathfrak{m}$ is open in $\overline{\mathrm{Tor}_\phi(K)}$. But Proposition 1.3 and Lemma 2.2 imply that $\mathrm{Tor}_\phi(\mathfrak{m})$ is a finite set. Hence

$$\overline{\mathrm{Tor}_\phi(\mathfrak{m})} = \mathrm{Tor}_\phi(\mathfrak{m}).$$

Thus $\overline{\mathrm{Tor}_\phi(K)}/\,\mathrm{Tor}_\phi(\mathfrak{m}) = \overline{\mathrm{Tor}_\phi(K)}/\overline{\mathrm{Tor}_\phi(\mathfrak{m})}$ is a finite set. Hence $\mathrm{Tor}_\phi(K)$ is a finite set.

COROLLARY. *Let ϕ be a Drinfeld module defined over a global function field K. Then* $\mathrm{Tor}_\phi(K)$ *is finite.*

REMARK 2.7. In the proof of Theorem 2.6, we showed that $\mathrm{Tor}_\phi(K)/\,\mathrm{Tor}_\phi(\mathfrak{m})$ is finite, thus $\mathrm{Tor}_\phi(K)/\,\mathrm{Tor}_\phi(R)$ is finite. One can ask

'Is $\mathrm{Tor}_\phi(K)/\,\mathrm{Tor}_\phi(R)$ finite without the assumption that K is locally compact?'

This might be thought as an analogous statement of the theorem of Kodaira and Neron ([S], Chapter VII, Theorem 6.1) in view of Remark 1.4.

REFERENCES

[H] D. Hayes, *Explicit Class Field Theory in Global Functions Fields*, Studies in Algebra and Number Theory, (ed. G. C. Rota), Academic Press, New York, 1979.

[S] J. Silvermann, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, New York, Berlin, Heidelberg, 1986.

[T] T. Takahashi, *Good Reduction of Elliptic Modules*, J. Math. Soc. Japan **34**(1982), 475–487.

Department of Mathematics
KAIST
Taejon, 305-701
Korea