LOCAL ISOGENY THEOREM FOR DRINFELD MODULES WITH NONINTEGRAL INVARIANTS

SUNGHAN BAE AND PYUNG-LYUN KANG

(Communicated by William W. Adams)

Abstract. An isogeny theorem for the Drinfeld modules of rank 2 over a local field analogous to that of elliptic curves is proved.

0. Introduction

Let $k$ be a global function field over a finite constant field $F_q$. Drinfeld introduced the notion of elliptic modules, which are now known as Drinfeld modules, on $k$ in analogy with classical elliptic curves. Hayes also studied this independently to generate certain class fields of $k$.

Drinfeld modules of rank 2 have many interesting properties analogous to those of elliptic curves. We fix $k$ to be the rational function field $F_q(T)$. In [1] we introduced the Tate parametrization of Drinfeld modules of rank 2 with nonintegral invariants over a complete field. In this article we use the description of division points of Tate-Drinfeld modules and the methods in [6, 7] to get an isomorphism theorem for Drinfeld modules over a field with some restrictions on $t$ and $t'$. In other words, there exist $a$ and $b$ in $A = F_q[T]$ such that $\rho_a(t^{-1}) - \rho_b(t'^{-1})$ is integral. This restriction does not appear in the classical case because $\alpha/\beta$ is a unit if the valuations of $\alpha$ and $\beta$ are equal.

From now on Drinfeld modules always mean Drinfeld modules of rank 2 defined on $A = F_q[T]$.

1. Tate-Drinfeld modules

In this section we give a quick review of Tate-Drinfeld modules, which are the function field analogues of Tate elliptic curves [1]. Let $k = F_q(T)$ and $k_\infty = F_q((T))$, and let $C$ be the completion of the algebraic closure of $k_\infty$. Let $\pi$ be an element of $C$ associated to the Carlitz module

$$\rho_T = TX + X^q.$$

Any rank 2 Drinfeld module $\phi$ over $C$ on $A = F_q[T]$ is completely determined by

$$\phi_T = TX + \pi^{1-q} g X^q + \pi^{1-q^2} \Delta X^q.$$

Received by the editors April 29, 1991 and, in revised form, January 16, 1992.

1991 Mathematics Subject Classification. Primary 11G09, 11R58.

Partially supported by KOSEF Research Grant 91-08-00-07.
Then $g$ and $\Delta$ are modular forms on $\Omega = C - K_\infty$ for $\text{GL}_2(A)$ of weight $q - 1$ and $q^2 - 1$, respectively. Let

$$t = t(z) = e^{-1}(\pi z)$$

where

$$e(z) = z \prod_{a \in A} \left(1 - \frac{z}{a\pi}\right).$$

Then $g$ and $\Delta$ have $t$-expansions with coefficients in $A$ [3].

Now let $K$ be a complete field containing $k$ and $\delta > 0$ a real number so that $g(t)$ and $\Delta(t)$ converge for $|t| < \delta$. For $t \in K$ with $|t| < \delta$, we define the Tate-Drinfeld module associated to $t$ by

$$\phi_t^{(t)} = TX + g(t)X^q + \Delta(t)X^{q^2}.$$ 

The Tate-Drinfeld map $e_{(t)}$ is defined to be

$$e_{(t)}(u) = u \prod_{a \in A} \left(1 - \frac{u}{\rho_a(t)}\right).$$

Remark 1.1. If one views $K$ as an $A$-module via $\rho$ (i.e., $a \cdot x = \rho_a(x)$ for $a \in A$, $x \in K$), then $e_{(t)}$ has exactly the same form as the exponential map $e_{A}(z)$ associated to the lattice $A \cdot t^{-1}$.

The following is given in [1].

Proposition 1.2. (i) The set $D_t$ of zeros of $e_{(t)}$ is $D_t = \{\rho_a(t^{-1}) : a \in A\}$.

(ii) $e_{(t)}(u + v) = e_{(t)}(u) + e_{(t)}(v)$.

(iii) $\phi_a^{(t)}(e_{(t)}(u)) = e_{(t)}(\rho_a(u))$.

Remark 1.3. In the classical case, the Tate map is a homomorphism from the multiplicative group $K^*$ to the elliptic curve. Proposition 1.2 says that the Tate-Drinfeld map is an $A$-module homomorphism from $\overline{K}$ with $A$-module structure given by the Carlitz module to $\overline{K}$ with $A$-module structure given by the Tate-Drinfeld module $\phi_t^{(t)}$.

Proposition 1.4. For $a \in A$, let $t_a = 1/\rho_a(t)$. Then $\phi_t^{(t)}$ and $\phi_t^{(t_a)}$ are isogenous.

Proposition 1.5. Let

$$D_t^{1/a} = \{u \in \overline{K} : \rho_a(u) \in D_t\},$$

where $\overline{K}$ is the algebraic closure of $K$. Then $e_{(t)}$ induces a Galois isomorphism of $D_t^{1/a}/D_t$ with $\text{Ker} \phi_a^{(t)}$.

2. $p$-adic representation and Kummer theory

Let $p = (p(T))$ be a prime ideal of $A = \mathbb{F}_q[T]$, where $p(T)$ is a monic irreducible polynomial in $A$. Let $\phi$ be a Drinfeld module of rank 2. Then $\text{Ker} \phi_{p(T)n}$ has a natural structure of an $A/p^n$-module. Hence

$$T_p(\phi) = \lim \text{Ker} \phi_{p(T)n}$$

is an $A_p$-module, where

$$A_p = \lim A/p^n.$$
Let
\[ V_p(\phi) = T_p(\phi) \otimes A_p k_p. \]

Now let \( K \) be a finite extension of \( k_p \) and \( \phi^{(t)} \) be a Tate-Drinfeld module of rank 2 over \( K \) associated to \( t \) with \( |t| < 1 \). We use \( 1 \) instead of \( \delta \) because \( A \) is contained in the ring of integers of \( K \) and the coefficients of \( g \) and \( \Delta \) are in \( A \).

If \( z \in D_t^{1/p(T)^n} \), then \( \rho_{p(T)^n}(z) \) lies in \( D_t \). Hence there is an element \( a \in A \) such that \( \rho_{p(T)^n}(z) = \rho_a(t^{-1}) \). The association \( z \mapsto a \mod p^n \) defines a homomorphism of \( \Lambda_{p(T)^n} = \text{Ker } \phi^{(t)}_{p(T)^n} \) onto \( A/p^n \). Hence the Tate-Drinfeld map gives rise to an exact sequence

\[ 0 \rightarrow R_n \rightarrow \Lambda_{p(T)^n} \rightarrow A/p^n \rightarrow 0 \]

of \( A[G] \)-modules, where \( G = \text{Gal}(\overline{K}/K) \) and \( R_n \) is the set of \( p(T)^n \)th roots of \( \rho \) (i.e., \( \text{Ker } \rho_{p(T)^n} \)). By taking the limits, we obtain an exact sequence of \( A_p[G] \)-modules

\[ 0 \rightarrow T_p(R) \rightarrow T_p(\phi^{(t)}) \rightarrow A_p \rightarrow 0 \]

and tensoring with \( k_p \), we get an exact sequence

\[ 0 \rightarrow V_p(R) \rightarrow V_p(\phi^{(t)}) \rightarrow k_p \rightarrow 0 \]

where \( G \) acts on \( A_p \) and \( k_p \) trivially.

We will show that the sequence (3) does not split. To do this we introduce an invariant \( x \), which belongs to the \( A \)-module \( \lim H^1(G, R_n) \). Let \( d \) be the coboundary map

\[ d : H^0(G, A/p^n) \rightarrow H^1(G, R_n) \]

with respect to the sequence (1), and let \( x_n = d(1) \). Let \( x \) be an element of \( \lim H^1(G, R_n) \) defined by the family \( \{x_n\} \), \( n \geq 1 \).

From the exact sequence of \( A[G] \)-modules

\[ 0 \rightarrow R_n \rightarrow \overline{K}^{\rho_{p(T)^n}} \rightarrow \overline{K} \rightarrow 0, \]

we have an isomorphism \( \delta : K/\rho_{p(T)^n}(K) \rightarrow H^1(G, R_n) \), since \( H^1(G, \overline{K}) = 0 \) by Hilbert’s Theorem 90.

**Proposition 2.1.** (a) The isomorphism \( \delta : K/\rho_{p(T)^n}(K) \rightarrow H^1(G, R_n) \) transforms the class of \( t^{-1} \mod \rho_{p(T)^n}(K) \) into \( x_n \).

(b) The element \( x \) is \( A \)-torsion free.

**Proof.** (a) follows easily from the definition of \( x_n \) and \( \delta \). To prove (b), suppose that \( a \cdot x = \rho_a(x) = 0 \) for some \( a \in A \). Then

\[ a \cdot t^{-1} = \rho_a(t^{-1}) \in \rho_{p(T)^n}(K) \]

for every \( n \) by (a). Let \( v \) be the discrete valuation on \( K \). Then

\[ v(\rho_a(t^{-1})) = v(t^{-1})q^{\deg a}, \]

\[ v(\rho_{p(T)^n}(\alpha_n)) = v(\alpha_n)q^n \deg p(T). \]

But \( \rho_a(t^{-1}) = \rho_{p(T)^n}(\alpha_n) \) implies that

\[ v(\alpha_n) = v(t^{-1})q^{\deg a - n \deg p(T)}. \]
But for sufficiently large $n$, (4) implies that $v(\alpha_n)$ is not an integer, which is impossible.

**Corollary 2.2.** The exact sequence (3) does not split.

**Proof.** Exactly the same proof as in [6, 7], replacing $\mathbb{Z}_p$ by $A_p$ and $p$ by $p(T)$ would give the result.

### 3. Local isogeny theorem

In this section, we will prove the following local isogeny theorem.

**Theorem 3.1.** Let $K$ be a finite extension of $k_p$ and $\mathcal{O}$ the ring of integers in $K$. Let $v$ be the discrete valuation on $K$ and $t, t' \in K^*$ with $v(t)$ and $v(t') > 0$. Let $\phi = \phi(t)$ and $\phi' = \phi(t')$ be the corresponding Tate-Drinfeld modules over $K$. Suppose that there exist $a, b \in A - \{0\}$ such that $\rho_a(t^{-1}) - \rho_b(t')^{-1}$ lies in $\mathcal{O}$. Then $\phi$ and $\phi'$ are isogenous if and only if $V_p(\phi)$ and $V_p(\phi')$ are isomorphic as $k_p[G]$-modules.

**Proof.** The ‘only if’ part is trivial. To show the other direction, it suffices to show that there exist elements $\alpha, \beta \in A$ such that $\rho_\alpha(t) = \rho_\beta(t')$ by Proposition 1.2. Let $\varphi : V_p(\phi) \to V_p(\phi')$ be a $G$-isomorphism. By Corollary 2.2, $\varphi$ maps $V_p(R)$ into itself. After multiplying $\varphi$ by some element of $A_p$, we may assume that $\varphi$ maps $T_p(\phi)$ into $T_p(\phi')$. Then we have a commutative diagram

$$
\begin{array}{c}
0 \rightarrow T_p(R) \rightarrow T_p(\phi) \rightarrow A_p \rightarrow 0 \\
\downarrow r \quad \downarrow \varphi \quad \downarrow s \\
0 \rightarrow T_p(R) \rightarrow T_p(\phi') \rightarrow A_p \rightarrow 0
\end{array}
$$

where $r, s \in A_p$. Let $x$ and $x'$ be the invariants in $\lim H^1(G, R_n)$ associated to $\phi$ and $\phi'$, respectively, given in the previous section. Then the commutativity of (5) shows that $r \cdot x = s \cdot x'$, that is, writing $r = (r_n)$ and $s = (s_n)$, with $\deg r_n < \deg p(T)^n$ and $\deg s_n < \deg p(T)^n$,

$$
\rho_r(x_n) = \rho_s(x'_n)
$$

in $H^1(G, R_n)$. Therefore $\rho_r(t^{-1}) = \rho_s(t'^{-1})$ in $\lim K/\rho_p(T)^n(K)$ by Proposition 2.1. Let $z = \rho_a(t^{-1}) - \rho_b(t'^{-1}) \in \mathcal{O}$.

Then

$$
\rho_{sa - rb}(t^{-1}) = \rho_{sa}(t^{-1}) - \rho_{rb}(t^{-1}) = \rho_s(\rho_b(t'^{-1}) + z) - \rho_r(t^{-1})
$$

$$
= \rho_b(\rho_s(t'^{-1}) - \rho_r(t^{-1})) + \rho_s(z).
$$

Write $u = sa - rb = (u_n)$, with $\deg u_n < \deg p(T)^n$. Since $\rho_s(t'^{-1}) - \rho_r(t^{-1}) = 0$ in $\lim K/\rho_p(T)^n(K)$ and $\rho_a \rho_b = \rho_b \rho_a$, there exists $\alpha_n \in K$ such that

$$
\rho_{u_n}(t^{-1}) = \rho_p(T)^n(\alpha_n) + \rho_s(z), \quad v(\alpha_n) \leq 0.
$$

Suppose that $u = (u_n) \neq 0$. Then for all sufficiently large $n$,

$$
\gcd(u_n, p(T)^n) = p(T)^k
$$
for some fixed \( k < n \). Then there are \( c_n, d_n \in A \) such that
\[
c_n u_n + d_n p(T)^n = p(T)^k.
\]
Hence
\[
\rho_{p(T)^k}(t^{-1}) = \rho_{c_n u_n + d_n p(T)^n}(t^{-1})
\]
\[
= \rho_{p(T)^n}(\rho_{c_n}(\alpha_n) + \rho_{d_n}(t^{-1})) + \text{integral}
\]
\[
= \rho_{p(T)^n}(\beta_n) + \text{integral}, \quad \beta_n \in K.
\]

Then \( \rho_{p(T)^k}(t^{-1} - \rho_{p(T)^{n-k}}(\beta_n)) \) is integral, and so \( t^{-1} - \rho_{p(T)^{n-k}}(\beta_n) \) is integral for all large \( n \), which is impossible. Therefore \( u = 0 \). Hence \( sa = rb \) and \( \rho_s(z) = 0 \) in \( \lim K/p(T)^n(K) \).

Then
\[
(6) \quad \rho_{s_n}(z) = \rho_{p(T)^n}(\beta_n).
\]
Let \( k = v(s) \), the valuation of \( s \) in \( k_p \). Then \( \gcd(s_n, p(T)^n) = p(T)^k \) for \( n \geq k \). Hence there exist \( a_n \) and \( b_n \) in \( A \) such that \( a_n s_n + b_n p(T)^n = p(T)^k \).

From (6) we have
\[
\rho_{p(T)^k}(z) = \rho_{a_n s_n + b_n p(T)^n}(z) = \rho_{a_n}(\rho_{s_n}(z)) + \rho_{p(T)^n}(\rho_{b_n}(z))
\]
\[
= \rho_{a_n}(\rho_{p(T)^n}(\beta_n)) + \rho_{p(T)^n}(\rho_{b_n}(z))
\]
\[
= \rho_{p(T)^n}(\rho_{a_n}(\beta_n) + \rho_{b_n}(z)).
\]
Therefore \( u = \rho_{p(T)^n}(z) = 0 \) in \( \lim K/p(T)^n(K) \). The proof is complete if we show that \( u \) is a root of \( \rho_c \) for some \( c \in A \). Let \( \mathfrak{q} \) be the maximal ideal of \( \mathcal{O} \) and the residual class degree of \( \mathcal{O}/\mathfrak{q} \) be \( m \). Since \( p(T) \in \mathfrak{q} \) and
\[
\rho_{p(T)^n}(X) \equiv X^{n \deg p(T)} \pmod{p(T)}
\]
we have
\[
\rho_{p(T)^{m-1}}(u) \equiv 0 \pmod{\mathfrak{q}}.
\]
Let \( u' = \rho_{p(T)^{m-1}}(u) \). Then \( v(u') > 0 \). Since \( u' = 0 \) in \( \lim K/p(T)^n(K) \), there is a sequence \( \{\delta_n\} \) in \( K \) with \( u' = \rho_{p(T)^n}(\delta_n) \). Since \( v(u') > 0 \), we have \( v(\delta_n) > 0 \). In this case it is easy to see that
\[
v(\rho_{p(T)^n}(\delta_n)) \to \infty \quad \text{as} \quad n \to \infty.
\]
Hence \( u' = \lim \rho_{p(T)^n}(\delta_n) = 0 \), and we are done.

**Remark 3.2.** The \( j \)-invariant \( j_t \) of \( \phi(t) \) is defined to be \( j_t = g(t)^{q+1}/\Delta(t) \). It is shown in [3] that
\[
j_t = \frac{1}{t^{q-1}} + \text{power series in } t^{q-1}.
\]
Hence \( j_t \) is nonintegral iff \( v(t) > 0 \).

**Remark 3.3.** (a) The proof of Theorem 3.1 is quite similar to that of the classical case except the use of the assumption that \( \rho_a(t^{-1}) - \rho_b(t'^{-1}) \) lies in \( \mathcal{O} \). The comparison is shown in the following table:
<table>
<thead>
<tr>
<th>Elliptic curve case</th>
<th>Drinfeld module case</th>
</tr>
</thead>
<tbody>
<tr>
<td>( q, q' )</td>
<td>( t^{-1}, t'^{-1} )</td>
</tr>
<tr>
<td>( v(q), v(q') \in \mathbb{Z} )</td>
<td>( a, b \in A )</td>
</tr>
<tr>
<td>( \alpha = q^{v(q')}/q'^{v(q)} )</td>
<td>( z = \rho_a(t^{-1}) - \rho_b(t'^{-1}) )</td>
</tr>
<tr>
<td>root of unity</td>
<td>torsion points of ( \rho )</td>
</tr>
</tbody>
</table>

In the elliptic curve case, for each element \( q \in K^* \), there is a naturally associated integer \( v(q) \), the valuation of \( q \). The fact that \( \alpha = q^{v(q')}/q'^{v(q)} \) is a unit in \( \mathcal{O} \) is used in the proof. In our case, there is no natural element of \( A \) associated to an element \( t \in K \), however, we need some elements \( a \) and \( b \) in \( A \), which make \( z = \rho_a(t^{-1}) - \rho_b(t'^{-1}) \) to be integral in order to prove that

(i) \( sa = rb \),

(ii) \( z \) is a torsion point of \( \rho \).

(b) The condition that \( \rho_a(t^{-1}) - \rho_b(t'^{-1}) \) lies in \( \mathcal{O} \) is not necessary if \( 0 < v(t), v(t') < q \). Indeed, in the proof we showed that

\[
\rho_{s_n}(t^{-1}) - \rho_{s_n}(t'^{-1}) = \rho_{p(T)^n}(\alpha_n)
\]

for some \( \alpha_n \in K \) with \( \deg r_n, \deg s_n < \deg p(T)^n \). Then

\[
v(\rho_{r_n}(t^{-1})) = v(t^{-1}) \cdot q^{\deg r_n} > -q^{1+\deg r_n} \geq -q^{n \deg p(T)'}
\]

and

\[
v(\rho_{s_n}(t'^{-1})) = v(t'^{-1}) \cdot q^{\deg s_n} > -q^{1+\deg s_n} \geq -q^{n \deg p(T)}.
\]

Thus

\[
v(\alpha_n)q^n \deg p(T) = v(\rho_{r_n}(t^{-1}) - \rho_{s_n}(t'^{-1})) > -q^n \deg p(T)
\]

since \( v(\alpha_n) \) is an integer, \( v(\alpha_n) \geq 0 \). Then \( \rho_{p(T)^n}(\alpha_n) \) lies in \( \mathcal{O} \), as does \( \rho_{r_n}(t^{-1}) - \rho_{s_n}(t'^{-1}) \). Hence one may take \( a = r_n \), \( b = s_n \) for any \( n \).

(c) The existence of the condition prevents one from getting the global isogeny theorem. Thus one may ask: “Do there exist \( a \) and \( b \) so that \( \rho_a(t^{-1}) - \rho_b(t'^{-1}) \) lies in \( \mathcal{O} \) only assuming that \( v(t), v(t') > 0 \) and \( V_p(\phi) \) and \( V_p(\phi') \) are \( G \)-isomorphic?”

Remark 3.4. One might be able to replace \( A \) by a more general function ring \( B \) to get the similar result. But there are some problems to be resolved primarily because \( B \) is not a principal ideal domain. For example,

(i) One should consider a family of Tate-Drinfeld modules \( \phi(b) \) for each ideal class (b) of \( B \).

(ii) To each \( \phi(b) \) one must replace the Carlitz module by the sign normalized rank 1 Drinfeld module \( \rho^{(b)} \), which is defined over the Hilbert class field of \( B \). Hence we need more restrictions on the complete field \( K \) to make \( \rho^{(b)} \) Galois invariant.

(iii) One must define invariants of Drinfeld modules of rank 2 on \( B \) to get the analogue of Proposition 1.4.
References


Department of Mathematics, Korea Advanced Institute of Science and Technology, Taejon, 305-701, Korea

Hongik University, Jochiwon, Chungchungnamdo, 339-800, Korea