BULL. AUSTRAL. MATH. SOC.
VOL. 64 (2001) [15–20]

11G09, 11G15

A NOTE ON KUMMER THEORY OF DIVISION POINTS OVER SINGULAR DRINFELD MODULES

ANLY LI

In this paper, we shall establish a Kummer theory of division points over singular Drinfeld modules which is in complete analogy with the classical one in number fields.

1. INTRODUCTION

The analogy between number fields and function fields has been an attractive subject in number theory. In 1972, Drinfeld introduced the notion of elliptic modules, now called Drinfeld modules. Since then, Drinfeld modules have played a central role in the study of arithmetic properties of function fields. In particular, using Drinfeld modules have been used to investigate many arithmetic properties of function fields, which are analogous to those of number fields (see [**1, 5, 7, 8**]).

Let $k = \mathbb{F}_q(T)$ be the rational function field over a finite field $\mathbb{F}_q$, where $q = p^n$ for some prime number p. Let $A = \mathbb{F}_q[T]$ and let τ be the q^{th} power mapping on $\overline{k}$. Let ϕ be a Drinfeld A-module of rank m defined over a finite extension L of k in a fixed algebraic closure $\overline{k}$, where L is viewed as an A-field of generic characteristic (see [**6**, Section 4.4], for general definition of Drinfeld modules). Via ϕ, L becomes an A-module. We denote this module by $\phi(L)$. Denote by $\overline{k}\{\tau\}$ the subspace of $\overline{k}[X]$ spanned by the linear combinations of $\{\tau^i,\ i = 0, 1, 2, \ldots\}$; this forms a ring under composition. Let $\mathrm{End}(\phi) \subset \overline{k}\{\tau\}$ be the ring of endomorphisms of ϕ which contain A. A Drinfeld module ϕ is said to be singular (or of complex multiplication) if $\mathrm{End}(\phi)$ strictly contains A and $\mathrm{End}(\phi) \otimes_A k$ is a field extension E of k with degree m. For a monic irreducible polynomial l in A, let Λ_l^ϕ be the set of l-torsion points of the Drinfeld module ϕ. Explicitly, $\Lambda_l^\phi = \{\alpha \in \overline{k} \mid \phi_l(\alpha) = 0\}$, where $\phi_l(\alpha)$ denotes the action of l on α.

In [**3**] we considered Drinfeld modules of rank one and established the Kummer theory of division points over Drinfeld modules of rank one, which is in complete analogy with the classical case for multiplicative algebraic groups over number fields. In this case, there are some well-known results which are necessary in the problem. For

Received 12th July, 2000
This research was partially supported by the National Science Council of the Republic of China.
The author wishes to thank Professor Wen-Chen Chi and Professor Jing Yu for their helpful discussions and invaluable suggestions.

example, for rank one Drinfeld modules ϕ the Galois group of the cyclotomic extension $L(\Lambda_l^\phi)/L$ is isomorphic to $(A/lA)^*$ for almost all monic irreducible polynomials l in A. Using this fact, we can directly construct an A-module structure of the Galois group $\mathrm{Gal}\Big(L\big(\Lambda_L^\phi,(a/l)\big)/L(\Lambda_l^\phi)\Big)$ via the natural conjugate action of $\mathrm{Gal}\big(L(\Lambda_l^\phi)/L\big)$, where $a \in \phi(L)$ and $a/l = \big\{\alpha \in \overline{k} \mid \phi_l(\alpha) = a\big\}$.

In this article, we shall establish the Kummer theory of division points over singular Drinfeld modules. The result is in complete analogy with the results for CM-elliptic curves (see [**9**, Chapter V, Theorem 5.2]) and for Abelian varieties of CM-type (see [**11**]). The main idea here follows the same line as in [**3, 9, 11**] together with some results developed in [**4, 12**].

Since for higher rank case, there is no such well-known result as in the rank one case, this Galois group $G(l) = \mathrm{Gal}(L(\Lambda_l^\phi)/L)$ is not completely understood. So, for this case we can not directly follow the same path as in the previous paper. For the rest of this paper, we assume that ϕ is a singular Drinfeld A-module of rank m defined over L. More precisely, $\mathrm{End}(\phi) \otimes_A k$ is a field extension E of k with degree m, and $\mathrm{End}(\phi) = \mathcal{O}$ which is an A-order of E. Furthermore, replacing L by a finite extension in $\overline{k}$, we assume that $\mathrm{End}(\phi) = \mathrm{End}_L(\phi)$ and $E \subseteq L$. Here we use the determinant module of ϕ which is of rank one to construct an A/lA-module structure of the group $\mathrm{Gal}\Big(L\big(\Lambda_l^\phi,(a/l)\big)/L(\Lambda_l^\phi)\Big)$ and hence it is an $A/lA\big[G(l)\big]$-module. Therefore, we also give a reduction theorem for endomorphism rings (see Proposition 2) which is similar to the classical one in number fields and hence prove that $A/lA\big[G(l)\big] = \mathcal{O}_E/l\mathcal{O}_E$ for almost all l where $\mathcal{O}_E$ is the ring of integers of E (see Proposition 3). Thus we can give the Galois group $\mathrm{Gal}\Big(L\big(\Lambda_l^\phi,(a/l)\big)/L(\Lambda_l^\phi)\Big)$ an $\mathcal{O}_E/l\mathcal{O}_E$-module structure and hence a discussion similar to that in [**3**] can then be followed.

Furthermore, let $\Gamma = \{a_1,\dots,a_r\}$ be a given finite set of elements of the A-module $\phi(L)$. Let $\mathbb{L}_l = L(\Lambda_l^\phi,\Gamma/l)$ be the extension of $L(\Lambda_l^\phi)$ obtained by adjoining to $L(\Lambda_l^\phi)$ all l^{th} roots of these elements a_i in $\overline{k}$. Then $\mathbb{L}_l$ is a Galois extension of L and we have the tower of Kummer extensions $L \subseteq L(\Lambda_l^\phi) \subseteq \mathbb{L}_l \subseteq L^{\mathrm{sep}}$, where L^{sep} is the separable closure of L in $\overline{k}$.

Let $H_\Gamma(l) = \mathrm{Gal}\big(\mathbb{L}_l/L(\Lambda_l^\phi)\big)$, $G(l) = \mathrm{Gal}\big(L(\Lambda_l^\phi)/L\big)$, and $G_\Gamma(l) = \mathrm{Gal}(\mathbb{L}_l/L)$. Analogous to the classical case, we have the following result:

Main Theorem 1. *Assume that $a_1,\dots,a_r \in L$ are linearly independent over $\mathcal{O}$. Then, for almost all monic irreducible polynomials l in A, $H_\Gamma(l)$ is isomorphic to $\Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ (r-copies).*

2. The Proof of Main Theorem

Let $\langle\Gamma\rangle$ be the A-submodule of $\phi(L)$ generated by $a_1,\dots,a_r$. Observe that for each $b \in A$, $L\Big(\Lambda_l^\phi,\big(\phi_b(a_i)\big)/l\Big) \subseteq L\big(\Lambda_l^\phi,\phi_b(a_i)/l\big) = L(\Lambda_l^\phi,a_i/l)$. So, it is easy to see that

https://doi.org/10.1017/S0004972700019638 Published online by Cambridge University Press

$L(\Lambda_l^\phi, (\Gamma/l) = L(\Lambda_l^\phi, 1/l\langle\Gamma\rangle))$.

For each $a \in \langle\Gamma\rangle$, let ψ_a be the map $H_\Gamma(l) \to \Lambda_l^\phi$ defined by $\psi_a(\sigma) = \sigma(\alpha) - \alpha$, where α is any l-division point of a (that is, $\phi_l(\alpha) = a$). It is easy to see that the difference $\sigma(\alpha) - \alpha$ is independent of the choice of α and is an l-torsion point of ϕ. Moreover, the map $\psi : H_\Gamma(l) \to \Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ (r-copies) defined by $\sigma \longmapsto \big(\psi_{a_1}(\sigma), \ldots, \psi_{a_r}(\sigma)\big)$ is an injective group homomorphism.

Notice that $G(l)$ acts on $H_\Gamma(l)$ by conjugation and acts naturally on $\Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ (r-copies).

PROPOSITION 1. *The map $\psi : H_\Gamma(l) \to \Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ is an injective $G(l)$-module homomorphism.*

PROOF: Let $H_{a_i}(l) = \mathrm{Gal}\Big(L\big(\Lambda_l^\phi, (a_i/l)\big)/L(\Lambda_l^\phi)\Big)$. For any $\varphi \in H_\Gamma(l)$, $\varphi|_{L\left(\Lambda_l^\phi, (a_i/l)\right)} \in H_{a_i}(l)$ is of the form: $\varphi_{\lambda_i}(\alpha_i) = \alpha_i + \lambda_i$ for some $\lambda_i \in \Lambda_l^\phi$ and $\phi_l(\alpha_i) = a_i$. For $\overline{\sigma} \in G_\Gamma(l)$ with $\overline{\sigma}|_{L(\Lambda_l^\phi)} = \sigma \in G(l)$, we have

$$\begin{aligned}
\sigma \cdot \varphi_{\lambda_i}(\alpha_i) &= \overline{\sigma} \circ \varphi_{\lambda_i} \circ \overline{\sigma}^{-1}(\alpha_i) \\
&= \overline{\sigma} \circ \varphi_{\lambda_i}(\alpha_i + \lambda_i') \quad (\text{assume that } \overline{\sigma}^{-1}(\alpha_i) = \alpha_i + \lambda_i') \\
&= \overline{\sigma}(\alpha_i + \lambda_i' + \lambda_i) \\
&= \alpha_i + \sigma(\lambda_i) \\
&= \varphi_{\sigma(\lambda_i)}(\alpha_i).
\end{aligned}$$

Hence ψ is an injective $G(l)$-module homomorphism. □

In particular, $H_\Gamma(l)$ can be viewed as a $G(l)$-submodule of $\Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ (r-copies).

Let $\mathcal{O}_E$ be the ring of A-integers in E. Note that if l is prime to the conductor of $\mathcal{O}$, then $\mathcal{O}/l\mathcal{O} = \mathcal{O}_E/l\mathcal{O}_E$. Also, we may identify A with $\phi(A) = \{\phi_a | a \in A\}$ in $\mathrm{End}(\phi)$.

For the rest of this section, we shall assume that our monic irreducible polynomials l are unramified in E and prime to the conductor of $\mathcal{O}$. Note that under the assumption that $\mathrm{End}(\phi) = \mathrm{End}_L(\phi)$, we are free to develop a theory of Drinfeld modules over $\mathcal{O}$ exactly as in the complex multiplication of elliptic curves, see [7]. The natural injection of $\mathcal{O}$ into $L\{\tau\}$ gives a rank one Drinfeld $\mathcal{O}$-module over L, denoted by ϕ'. By definition it is easy to see that ϕ and ϕ' have the same l-torsion points, and hence we have that Λ_l^ϕ is a free rank one $\mathcal{O}_E/l\mathcal{O}_E$-module. Note that, under these assumptions, we also have that $G(l) \subseteq \mathrm{Aut}_{\mathcal{O}/l\mathcal{O}}(\Lambda_l^\phi) \cong (\mathcal{O}_E/l\mathcal{O}_E)^*$.

PROPOSITION 2. *Let ϕ have good reduction at $\mathcal{B}$, say $\overline{\phi}$; and $\mathcal{B} \cap k = \wp$. If $\wp$ does not divide the conductor of $\mathcal{O}$ and splits completely in E, then $\mathrm{End}(\phi) \cong \mathrm{End}(\overline{\phi})$ via the natural reduction map.*

PROOF: The proof is exactly the same as in the classical case using a normalised pair (see [**10**, Chapter 13, Theorem 12] and [**1**, Theorem 3.1]). □

https://doi.org/10.1017/S0004972700019638 Published online by Cambridge University Press

PROPOSITION 3. *For almost all monic irreducible polynomials l in A, the subring $(A/lA)[G(l)]$ of $\mathcal{O}_E/l\mathcal{O}_E$ generated by all elements of $G(l)$ is all of $\mathcal{O}_E/l\mathcal{O}_E$.*

PROOF: Suppose that ϕ has good reduction at a prime ideal $\mathcal{B}$ of $\mathcal{O}_L$. Let $\wp = \mathcal{B} \cap k$ and let $\mathcal{F}$ be the residue field of $\mathcal{B}$.

Let c be the conductor of the A-order $\mathcal{O}$. By Proposition 2, under the conditions $c \notin \wp$ and $\wp$ splits completely in E, the natural reduction map from $\mathrm{End}(\phi)$ to $\mathrm{End}(\overline{\phi})$ is an isomorphism. For such a reduction $\overline{\phi}$, let $D = \mathrm{End}(\overline{\phi}) \otimes_A k$ and let π be the Frobenius automorphism of $\overline{\phi}$. We have the isomorphism $E \cong D$. On the other hand, it is known that the centraliser of D in $\mathcal{F}(\tau)$ is equal to $k(\pi)$ (see [**12**, Theorem 1]). Hence $D = k(\pi)$. In particular, if we view π as an element in $\mathcal{O}_E$, then $A[\pi]$ is an order in $\mathcal{O}_E$.

It is easy to see that if l is prime to the conductor of $A[\pi]$ in $\mathcal{O}_E$, then $\mathcal{O}_E/l\mathcal{O}_E = (A/lA)[\pi]$. If $(l) \neq \wp$, then $\mathcal{B}$ is unramified in $L(\Lambda_l^\phi)/L$. So, π is the image in $G(l)$ of any Frobenius element for $\mathcal{B}$ in $\mathrm{Gal}(\overline{L}/L)$ and hence π (or rather its image in $\mathcal{O}_E/l\mathcal{O}_E$) belongs to $G(l)$. We have then $\mathcal{O}_E/l\mathcal{O}_E = (A/lA)[\pi] \subseteq (A/lA)[G(l)] \subseteq \mathcal{O}_E/l\mathcal{O}_E$ for all $(l) \neq \wp$ and prime to the conductor of $A[\pi]$. This completes the proof. □

PROPOSITION 4. *For almost all monic irreducible polynomials l in A, $H^1\big(G(l), \Lambda_l^\phi\big) = 0$.*

PROOF: Let l be prime to the conductor of the A-order $\mathcal{O}$ and the discriminant of E over k. Under the assumption that $\mathrm{End}(\phi) = \mathrm{End}_L(\phi)$, we have that $G(l) \subseteq \mathrm{Aut}_{\mathcal{O}/l\mathcal{O}}(\Lambda_l^\phi) \cong (\mathcal{O}_E/l\mathcal{O}_E)^*$. Since l is unramified in E, it is clear that the order of $G(l)$ is relatively prime to p. The result follows from a well-known result in group cohomology (see [**2**, Corollary 10.2]). □

Let $H_l = \mathrm{Gal}\big(L^{\mathrm{sep}}/L(\Lambda_l^\phi)\big)$. Consider the map $\psi' : L \to \mathrm{Hom}(H_l, \Lambda_l^\phi)$ given by $x \mapsto \psi'_x$, where $\psi'_x(\sigma) = \sigma(\alpha) - \alpha$ for $\sigma \in H_l$ and some α with $\phi_l(\alpha) = x$. It is easy to see that the map ψ' is $\mathrm{End}(\phi)$-linear. Consider the map $\delta : L \to H^1\big(\mathrm{Gal}(L^{\mathrm{sep}}/L), \Lambda_l^\phi\big)$, which is obtained by taking cohomology in the short exact sequence $0 \to \Lambda_l^\phi \to L^{\mathrm{sep}} \xrightarrow{l} L^{\mathrm{sep}} \to 0$. By definition, it is easy to see that ψ' is the composition of δ with the restriction homomorphism $\mathrm{Res} : H^1\big(\mathrm{Gal}(L^{\mathrm{sep}}/L), \Lambda_l^\phi\big) \to H^1(H_l, \Lambda_l^\phi) = \mathrm{Hom}(H_l, \Lambda_l^\phi)$. By the restriction-inflation sequence together with the vanishing of $H^1(G(l), \Lambda_l^\phi)$ (given in Proposition 4), we have that ψ' induces an $(\mathcal{O}_E/l\mathcal{O}_E)$-linear injection $L/\phi_l(L) \to \mathrm{Hom}(H_l, \Lambda_l^\phi)$. Notice that if we restrict ψ' to $\langle\Gamma\rangle/\phi_l\big(\langle\Gamma\rangle\big)$, then each ψ'_x in $\psi'\Big(\langle\Gamma\rangle/\phi_l\big(\langle\Gamma\rangle\big)\Big)$ factors through $H_\Gamma(l)$. So, we may view the map $\psi'|_{\langle\Gamma\rangle/\phi_l\left(\langle\Gamma\rangle\right)}$ as the natural map $\langle\Gamma\rangle/\phi_l\big(\langle\Gamma\rangle\big) \to \mathrm{Hom}\big(H_\Gamma(l), \Lambda_l^\phi\big)$ given by $a \mapsto \psi_a$ as defined above Proposition 1. By the same arguments as in [4] (see [**4**, Theorem 5]), we have that for almost all monic irreducible polynomials l in A, these images of $a_1, \ldots, a_r$ in $\Gamma/\phi_l(\Gamma)$ are also linearly independent over $\mathcal{O}_E/l\mathcal{O}_E$. Then, via the $\mathcal{O}_E/l\mathcal{O}_E$-injection ψ, we have the following proposition:

PROPOSITION 5. *For almost all monic irreducible polynomials l in A, $\psi_{a_1}, \ldots, \psi_{a_r}$ are linearly independent over $\mathcal{O}_E/l\mathcal{O}_E$.*

https://doi.org/10.1017/S0004972700019638 Published online by Cambridge University Press

Let ϕ be a rank m Drinfeld module over L given by $\phi_T = T\tau^0 + g_1\tau + \ldots + g_m\tau^m$, $g_m \neq 0$. Let $\Lambda\phi$ be the determinant module of ϕ which is defined by $(\Lambda\phi)_T = T\tau^0 + (-1)^{m-1}g_m\tau$. It is well-known that $\Lambda\phi$ is a rank one Drinfeld module over L and $L(\Lambda_l^\phi) \supseteq L(\Lambda_l^{\Lambda\phi})$ (see [**6**, Section 2.6, p.344]). Further, $\mathrm{Gal}\big(L(\Lambda_l^{\Lambda\phi})/L\big) \cong (A/lA)^*$ for almost all monic irreducible polynomials l which are unramified in the maximal separable subextension L_s/k in L/k and such that $\Lambda\phi$ has good reduction at the primes above l in L (see [**7**, Theorem 7.7]). If ϕ is singular, then $G(l) \subset (\mathcal{O}_E/l\mathcal{O}_E)^*$ is a finite Abelian group. So, for almost all l, there is a subgroup H of $G(l)$ which is isomorphic to $(A/lA)^*$. Under the conjugation action of $G(l)$ on $H_\Gamma(l)$, $(A/lA)^*$ acts on $H_\Gamma(l)$ naturally and hence $H_\Gamma(l)$ can be viewed as an A/lA-vector space.

Recall the following well-known result (see [**11**, p.71, Lemma]):

LEMMA. *Let R be a product of fields, and let V be a free rank 1 module over R. Suppose that C is an R-submodule of $B = V \times \cdots \times V$ (n times) which is strictly smaller than B. Then there are elements $t_1, \ldots, t_n$ of R, not all 0, such that $\sum t_i v_i = 0$ for all $(v_1, \ldots, v_n) \in C$.*

In addition, suppose that l is unramified in the maxmial separable subextension L_s/k in L/k and such that $\Lambda\phi$ has good reduction at the primes above l in L. Then we have the following result:

PROPOSITION 6. *$H_\Gamma(l) \cong \Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ (r-copies), whenever the following two conditions are satisfied:*

(1) *The subring $(A/lA)\big[G(l)\big]$ of $\mathcal{O}_E/l\mathcal{O}_E$ generated by all elements of $G(l)$ is in fact all of $\mathcal{O}_E/l\mathcal{O}_E$,*

(2) *The homomorphisms $\psi_{a_1}, \ldots, \psi_{a_r}$ are linearly independent over $\mathcal{O}_E/l\mathcal{O}_E$.*

PROOF: By the observation preceding the above Lemma, it has been shown that $H_\Gamma(l)$ is an $(A/lA)\big[G(l)\big]$-module. Under condition (1), we see that $H_\Gamma(l)$ is an $\mathcal{O}_E/l\mathcal{O}_E$-module.

Applying the above Lemma by taking $R = \mathcal{O}_E/l\mathcal{O}_E$, $V = \Lambda_l^\phi \cong \mathcal{O}_E/l\mathcal{O}_E$, $B = \Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ (r-copies), and $C =$ the image $\psi\big(H_\Gamma(l)\big)$ of ψ in $\Lambda_l^\phi \times \cdots \times \Lambda_l^\phi$ (r-copies), the result follows immediately from condition (2). □

Therefore, by Propositions 3 and 5, we complete the proof of the main theorem.

REMARKS.

(i) Since for almost all l, the orders of Λ_l^ϕ and $G(l)$ are relatively prime, so we have that $H^2(G(l), \Lambda_l^\phi) = 0$. On the other hand, the orders of $H_\Gamma(l)$ and $G(l)$ are also relatively prime, so $H^2\big(G(l), H_\Gamma(l)\big) = 1$, where $G(l)$ acts on $H_\Gamma(l)$ by conjugation. In particular, the exact sequence $1 \to H_\Gamma(l) \to G_\Gamma(l) \to G(l) \to 1$ is split and $G_\Gamma(l)$ is a semidirect product of $H_\Gamma(l)$ by $G(l)$.

(ii) The assumption that the field of definition L of ϕ is large enough is indeed

necessary. For example, let ϕ be the Drinfeld module of rank 2 defined over $k = \mathbb{F}_q(T)$ given by $\phi_T(X) = TX + X^{q^2}$. It is easy to check that $\alpha \in \mathbb{F}_{q^2} - \mathbb{F}_q$ is an element of $\mathrm{End}(\phi)$ which is not in A. So ϕ is a singular Drinfeld module of rank 2. Moreover, α lies in $\mathrm{End}(\phi)$, but not in $\mathrm{End}_k(\phi)$. As an exercise, one can show that the order of $G(l) = \mathrm{Gal}\big(k(\Lambda_l^\phi)/k\big)$ is equal to $2(q^d-1)^2$ if $\deg(l) = d$ is even; and is equal to $2(q^{2d}-1)$ if d is odd. In this case, $G(l) \not\subseteq (\mathcal{O}_E/l\mathcal{O}_E)^*$ even if l is unramified in E.

References

[1] S. Bae and J.K. Koo, 'On the singular Drinfeld modules of rank 2', *Math. Z.* **210** (1992), 267–276.

[2] K.S. Brown, *Cohomology of groups* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

[3] W.-C. Chi and A. Li, 'Kummer theory of division points over Drinfeld modules of rank one', *J. Pure Appl. Algebra* **156** (2001), 171–185.

[4] L. Denis, 'Géométrie diophantienne sur les modules de Drinfeld', in *Proceedings "The Arithemetic of Function Fields"*, (D.Goss, D. Hayes and M.Rosen, Editors) (Walter de Gruyter, Berlin, 1997), **pp.** 285–302.

[5] E. Gekeler, 'Zur arithmetik von Drinfeld moduln', *Math. Ann.* **262** (1983), 167–182.

[6] D. Goss, 'Drinfeld modules: cohomology and special functions', in *Proceedings of Symposia in Pure Mathematics, Part 2,* **55** (Amer. Math. Soc., Providence, R.I., 1994), **pp.** 309–362.

[7] D. Goss, *Basic structures of function field arithmetic* (Springer-Verlag, Berlin, Heidelberg, New York, 1996).

[8] D. Hayes, 'Explicit class field theory in global function fields', in *Studies in Algebra and Number Theory*, Advances in Math. **16** (Academic Press, New York, London, 1980), **pp.** 173–217.

[9] S. Lang, *Elliptic curves: Diophantine analysis* (Springer-Verlag, Berlin, Heidelberg, New York, 1987).

[10] S. Lang, *Elliptic functions* (Springer-Verlag, Berlin, Heidelberg, New York, 1973).

[11] K.A. Ribet, 'Dividing rational points on abelian varieties of CM-type', *Compositio Math.* **33** (1976), 69–74.

[12] J-K. Yu, 'Isogenies of Drinfeld modules over finite fields', *J. Number Theory* **54** (1995), 161–171.

Department of Mathematics
Fu-Jen University
Taipei
Taiwan
Republic of China
e-mail: anlyli@math.fju.edu.tw