International Journal of Algebra, Vol. 7, 2013, no. 4, 157 - 166
HIKARI Ltd, www.m-hikari.com

Kummer Type Extensions in Function Fields

Marco Sánchez-Mirafuentes

Universidad Autónoma Metropolitana
Unidad Iztapalapa
División de Ciencias Básicas e Ingeniería
Departamento de Matemáticas
Av. San Rafael Atlixco 186, Col Vicentina
Del. Iztapalapa, C.P. 09240 México, D.F.

Gabriel Villa Salvador

CINVESTAV IPN
Departamento de Control Automático
Apartado Postal 14-740
México, D.F. C.P 07000

Abstract

We present a generalization of Kummer extensions in algebraic function fields with finite field of constants $\mathbb{F}_q$, using the action of Carlitz-Hayes. This generalization of Kummer type extensions is due to Wen-Chen Chi and Anly Li and due also to Fred Schultheis. The main results of this article are Proposition 3.2 and Theorem 3.4. They provide a partial analogue of a theorem of Kummer, which establishes a bijection between Kummer extensions L/K of exponent n and subgroups of K^* containing $(K^*)^n$.

Mathematics Subject Classification: 11R60, 11R99, 12F05, 14H05

Keywords: Carlitz Module, Kummer extensions, Dual module, Bilinear map

1 Introduction

An *n-Kummer* extension, is a field extension L/K such that n is relatively prime to char(K), the characteristic of K, $\mu_n \subseteq K$, where μ_n is the group of n-th roots of unity, and

$$L = K(\sqrt[n]{\Delta}),$$

where Δ is a subgroup of K^* containing the group K^{*n} of n-th powers, and $K(\sqrt[n]{\Delta})$ is the field generated by all the roots $\sqrt[n]{a}$, with $a \in \Delta$. This is the origin of *the theory of Kummer* which is of significance in class field theory, for example see [5] Chapter 1. In this setting we have the followings facts.

Let K be any field containing the group μ_n of n-th roots of unity, where n is a natural number prime to the characteristic of K. Then

(1) An n-Kummer extension L/K is a Galois extension and Gal(L/K) is an abelian group of exponent n.

(2) If L/K is an abelian extension of exponent n, then $L = K(\sqrt[n]{\Delta})$, where $\Delta \subseteq K^*$ and $(K^*)^n \subseteq \Delta$.

We will present a generalization of Kummer extensions via the Carlitz-Hayes action. In what follows, p denotes a prime number, $q = p^s$, $s \in \mathbb{N}$, R_T denotes the ring $\mathbb{F}_q[T]$, k denotes the field of rational functions $\mathbb{F}_q(T)$ and $\overline{k}$ denotes an algebraic closure of k.

In Section 2 we present some facts over R_T-modules that are used in Section 3. The main part of this work is precisely Section 3. We will discuss extensions L/K such that $k \subseteq K \subseteq L \subseteq \overline{k}$. Next we give a brief outline of the Carlitz Hayes action. For details see [2] and [7].

Let φ be the Frobenius automorphism $\varphi : \overline{k} \to \overline{k}$, $\varphi(u) = u^q$, and let μ_T be the homomorphism $\mu_T : \overline{k} \to \overline{k}$, $\mu_T(u) = Tu$. We have an action of R_T in $\overline{k}$ given as follows: if $M \in R_T$ and $u \in \overline{k}$, then $u^M := M(\varphi + \mu_T)(u)$. It can be shown that with this definition, $\overline{k}$ becomes an R_T-module, see [7] Chapter 12. We have that z^M is a separable polynomial in z of degree $d = \deg(M)$. Moreover, the polynomial z^M can be written as $z^M = \sum_{i=0}^{d} (M, i) z^{q^i}$, where $(M, i) \in R_T$, $(M, 0) = M$ and (M, d) is the leader coefficient of M, see [7] Chapter 12.

On the other hand, assuming that $M \in R_T \setminus \{0\}$, the M-torsion set of $\overline{k}$, denoted by Λ_M, is $\Lambda_M := \{u \in \overline{k} \mid u^M = 0\}$. We also call Λ_M to be the set of *M-roots* of Carlitz. Note that if $a \in \overline{k}$ then set of all roots of the polynomial $z^M - a$ is $\{\alpha + \lambda \mid \lambda \in \Lambda_M\}$, where α is any fixed root of $z^M - a$ in $\overline{k}$.

Proposition 3.2 and Theorem 3.4 are analogous to facts (1) and (2) listed above, except that we only consider *finite* extensions.

2 Module theory

In this section, unless otherwise indicated, all modules and homomorphisms considered are R_T-modules and R_T-homomorphisms, respectively.

Let A be a module, and $a \in A$. Let $\varphi_a : R_T \to A$ be the homomorphism defined by $\varphi_a(M) = Ma$.

Definition 2.1. We say that A is a *cyclic module*, if there exists $a \in A$, such that φ_a is a surjective homomorphism.

Note that the above definition is equivalent to say that there exists $a \in A$ such that $A = (a)$.

Let $a \in A$ and consider the kernel of the homomorphism φ_a, $\ker(\varphi_a)$. If $\ker(\varphi_a) \neq \{0\}$ there exists a nonzero polynomial M that we may assume to be monic, such that $\ker(\varphi_a) = (M)$.

Definition 2.2. Let $a \in A$. We say that a has *infinite order* if the kernel of φ_a is zero. We say that a has *finite order* M, where M is a monic polynomial, if $\ker(\varphi_a)$ is nonzero and $\ker(\varphi_a) = (M)$. Now if A is a module, an *exponent* of A is a nonzero $M \in R_T$, such that $Ma = 0$ for each $a \in A$.

Remark 2.3. If A is a finite cyclic module, there exists $a \in A$ such that φ_a is a surjective homomorphism. Therefore there exists $M \in R_T \setminus \{0\}$ such that

(i) $\ker(\varphi_a) = (M)$ and

(ii) $R_T/(M) \cong A$.

As before, we may replace M by a monic polynomial and we say that A has *order* M.

The proof of the following lemma is straightforward.

Lemma 2.4. *Let A be a cyclic module of order N, with $N \neq 0$. Let N_1 be a monic divisor of N. Then there exists a submodule of A, of order N_1.* □

Remark 2.5. With the conditions of Lemma 2.4, by Remark 2.3 we have $Na = 0$.

On the other hand, if B is a cyclic submodule of A of order N_1 then, again by Remark 2.3, there exists $b \in B$, such that φ_b is surjective and $\ker(\varphi_b) = (N_1)$. Since $b \in A$, there exists $N_2 \in R_T$, such that $b = N_2 a$.

Now, because $Nb = N(N_2 a) = N_2(Na) = 0$ we have $N \in \ker(\varphi_b) = (N_1)$. Therefore N_1 is a divisor of N. Since all cyclic modules of order M are isomorphic to $R_T/(M)$ we have there is only one cyclic module of order M, it follows that for each monic divisor M of N, there is a unique cyclic submodule of A of order N.

Analogously to the case of cyclic groups C_m, we denote by C_M the module $R_T/(M)$ which is cyclic of order M.

Definition 2.6. Let A be a module. We denote by $\widehat{A}$ or by $\operatorname{Hom}_{R_T}(A, C_M)$, the group of homomorphisms from A into C_M, $\widehat{A}$ is the *dual module* of A.

Let $f : A \to B$ be a homomorphism, such that A and B have exponent M. Then we have a homomorphism $\widehat{f} : \widehat{B} \to \widehat{A}$ defined by $\widehat{f}(\psi) = \psi \circ f$. Note that this is a contravariant functor, namely

$$\widehat{()} : R_T\text{-modules of exponent } M \to R_T\text{-modules}$$

such that if $f : A \to B$ and $g : B \to C$ are homomorphisms, then

(1) $\widehat{g \circ f} = \widehat{f} \circ \widehat{g}$ and
(2) $\widehat{1} = 1$.

Lemma 2.7. *If A is a finite module, with exponent M such that $A = B \times D$, then $\widehat{A}$ is isomorphic to $\widehat{B} \times \widehat{D}$.*

Proof. The natural projections $\pi_1 : B \times D \to B$ and $\pi_2 : B \times D \to D$ induce homomorphisms $\widehat{\pi_1} : \widehat{B} \to \widehat{B \times D}$ and $\widehat{\pi_2} : \widehat{D} \to \widehat{B \times D}$. Therefore we may define $\theta : \widehat{B} \times \widehat{D} \to \widehat{B \times D}$ given by $\theta(\psi_1, \psi_2) = \widehat{\pi_1}(\psi_1) + \widehat{\pi_2}(\psi_2)$, where $(\psi_1, \psi_2) \in \widehat{B} \times \widehat{D}$.

We have θ is a homomorphism. Moreover if $\psi \in \widehat{B \times D}$, since ψ is a homomorphism, we get $\psi(x, y) = \psi(x, 0) + \psi(0, y)$ for all $(x, y) \in B \times D$. Now, if we define $\psi_1 : B \to C_M$ by $\psi_1(x) = \psi(x, 0)$ and $\psi_2 : D \to C_M$ by $\psi_2(y) = \psi(0, y)$ then ψ_1 and ψ_2 are homomorphisms. Thus, we obtain the induced map

$$\delta : \widehat{B \times D} \to \widehat{B} \times \widehat{D}$$

given by $\delta(\psi) = (\psi_1, \psi_2)$ which is a module homomorphism whose inverse is θ. This completes the proof. □

Proposition 2.8. *A finite module A with exponent M is isomorphic to its dual. In other words*

$$A \cong \widehat{A}$$

Proof. By Theorem 4.7, Chapter 5 of [3], we can write $A \cong \bigoplus_P A_P$. The above sum is over all irreducible polynomials P and A_P denotes the set of elements of A having order a power of P.

Now by Theorem 4.9 of Chapter 5 of [3], each A_P can be written as $A_P \cong C_{P^{\alpha_1}} \oplus \ldots \oplus C_{P^{\alpha_k}}$, where $\alpha_1 \geq \ldots \geq \alpha_k \geq 1$, and each $C_{P^{\alpha_i}}$ is a cyclic module whose generator has order P^{α_i}, so each $C_{P^{\alpha_i}}$ has order P^{α_i}. Note that each A_P and each $C_{P^{\alpha_i}}$ have exponent M.

By the above observation and by Lemma 2.7, we may assume that A is cyclic generated by a of order P^α, where $\alpha \in \mathbb{N}$ and P is irreducible. Hence the function φ_a is an epimorphism and $(P^\alpha) = \ker(\varphi_a)$.

Since M is an exponent of A, we have $P^\alpha \mid M$. Now from Lemma 2.4 and Remark 2.3, C_M has a unique cyclic submodule of order P^α. We denote such module by C_{P^α}. The homomorphism $\varphi_a : R_T \to A$ induces an isomorphism, denoted again by $\varphi_a : R_T/(P^\alpha) \to A$.

The inverse of the isomorphism φ_a will be denoted by ψ. Let $y = \psi(a)$. Then y is a generator of C_{P^α}. The composition ψ with the natural inclusion $C_{P^\alpha} \hookrightarrow C_M$, gives an element of $\widehat{A}$, also denoted by ψ.

Let $\varphi \in \widehat{A}$. Note that $\mathrm{Im}(\varphi) \subseteq C_M$ is a cyclic submodule of order N. Thus, there exists $w \in \mathrm{Im}(\varphi)$ such that $w = \varphi(a_w)$ where $a_w \in A$ generates $\mathrm{Im}(\varphi)$ and its order is N.

On the other hand $P^\alpha \in (N)$. Therefore $P^\alpha = ND$, for some $D \in R_T$. Consequently $N = P^\gamma$ for some $\gamma \leq \alpha$, i.e., w has order P^γ and as a_w generates $\mathrm{Im}(\varphi)$, we have $\mathrm{Im}(\varphi) \subseteq C_{P^\alpha}$.

Now φ is determined by its action on a, where $a \in A$ is a generator of A. Therefore $\varphi(a) = Ny$. Now if $\psi_N = N\psi$ then $\psi_N(a) = N\psi(a) = Ny = \varphi(a)$, that is, $\varphi = \psi_N \in (\psi)$.

So $\widehat{A} = (\psi)$ and the order of $\widehat{A}$ is $q^{\deg(P^\alpha)}$. Therefore $A \cong \widehat{A}$. □

Definition 2.9. Let A and B be modules. A *bilinear* map of $A \times B$ into a module C, denoted by $(a, b) \mapsto < a, b >$, is a function $A \times B \to C$ that has the following property: for each $a \in A$, the function $b \mapsto < a, b >$ is a homomorphism and, for each $b \in B$, the function $a \mapsto < a, b >$ is a homomorphism. An element $a \in A$ is said *orthogonal* to $S \subseteq B$, if $< a, b >= 0$, for each $b \in S$.

Analogously, we say that $b \in B$ is orthogonal to $S \subseteq A$ if $< a, b >= 0$ for all $a \in A$. The *left kernel* of the bilinear function is the submodule of A that is orthogonal to B. The *right kernel* of the bilinear function is the submodule of B that is orthogonal to A.

Let A' and B' be the left and right kernels of the bilinear map respectively. An element $b \in B$ gives an element in $\mathrm{Hom}_{R_T}(A, C)$ given by $a \mapsto < a, b >$, which we denote by ψ_b. Then ψ_b vanishes in A', i.e., $\psi_b(a) = 0$ for each $a \in A$. Therefore, ψ_b induces a homomorphism $A/A' \to C$ given by $a + A' \mapsto \psi_b(a)$.

On the other hand, if $b \equiv b' \mod B'$ then $\psi_b = \psi_{b'}$. Therefore we obtain firstly a homomorphism $\psi : B/B' \to \mathrm{Hom}_{R_T}(A/A', C)$ given by $\psi(b+B') = \psi_b$ and secondly, an exact sequence of modules

$$0 \to B/B' \to \mathrm{Hom}_{R_T}(A/A', C). \tag{1}$$

Similarly we obtain the exact sequence

$$0 \to A/A' \to \mathrm{Hom}_{R_T}(B/B', C). \tag{2}$$

Proposition 2.10. *Let $A \times A' \to C_M$ be a bilinear map of modules into a cyclic module C_M of finite order M. Let B, B' be their respective left and right kernels. Suppose that A'/B' is finite with exponent M and that A/B have exponent M. Then A/B is finite and A'/B' is isomorphic to the dual module of A/B.*

Proof. From the exact sequences (1) and (2) it follows that the following sequences are exact

$$0 \to A'/B' \to \mathrm{Hom}_{R_T}(A/B, C_M) \tag{3}$$

and

$$0 \to A/B \to \mathrm{Hom}_{R_T}(A'/B', C_M). \tag{4}$$

From (4) we obtain that A/B can be viewed as a submodule of $\widehat{A'/B'}$. From this follows the finiteness of A/B. On the other hand we obtain from the exact sequences (3) and (4) and Proposition 2.8

$$\mathrm{card}(A/B) \leq \mathrm{card}(\widehat{(A'/B')}) = \mathrm{card}(A'/B'). \tag{5}$$

and

$$\mathrm{card}(A'/B') \leq \mathrm{card}(\widehat{(A/B)}) = \mathrm{card}(A/B). \tag{6}$$

the second equality follows from Proposition 2.8. Now from (3) we have obtain injective map $\phi : A'/B' \to \widehat{A/B}$. Then by (5) and (6), ϕ is surjective, and this finishes the proof. □

3 Kummer theory

In this section we give a generalization of Kummer extensions, a little different from those given by Chi and Li [1] and Schultheis [6]. In what follows we will assume that the extensions considered are subextensions of $\overline{k}/k$. Let $M \in R_T$ be a non-constant polynomial and $\varphi : K \to K$ defined by $\varphi(u) = u^M$, where $K = k(\Lambda_M)$. Then φ is a homomorphism. Moreover consider a submodule B of K under the action of Carlitz-Hayes containing $K^M = \varphi(K)$.

Let $b \in K$ we shall use the symbol $\sqrt[M]{b}$ to denote any such element β, which will be called an *M-root of b*. Since the M-roots of Carlitz are in K, we observe that field $K(\beta)$ is the same no matter which M-root β of b we select. We denote this field by $K(\sqrt[M]{b})$.

For our next proposition we need the definition give in [1].

Definition 3.1. An abelian extension L/K with Galois group G, is said to be an R_T-*abelian extension* if its Galois group has an R_T-module structure. An R_T-abelian extension L/K is said to be of *exponent* M if G is an M-torsion R_T-module, i.e., $M \cdot \sigma = 1$ for all $\sigma \in G$.

Proposition 3.2. *(1) Let B be an R_T-submodule of K containing K^M and let K_B be the composite of all fields $K(\sqrt[M]{b})$ with $b \in B$. Then K_B/K is a Galois abelian extension.*

(2) Assume that K_B/K is an R_T-abelian extension of exponent M with Galois group G. Then there is a bilinear map

$$G \times B \to \Lambda_M \text{ given by } (\sigma, a) \mapsto <\sigma, a>$$

where $<\sigma, a> = \sigma(\alpha) - \alpha$ and $\alpha^M = a$. The left kernel is 1 and the right kernel is K^M.

The extension K_B/K es finite if only if $(B : K^M)$ is finite. In this case we have

$$B/K^M \cong \widehat{G}$$

In particular we have the equality

$$[K_B : K] = (B : K^M).$$

Proof. (1) Let $b \in B$ and let β be an M-root of b. The polynomial $z^M - b$ splits into linear factors in K_B for all $b \in B$. Thus K_B/K is a Galois extension.

Now let $G = \mathrm{Gal}(K_B/K)$, $\sigma \in G$, $b \in B$ and β a root of the polynomial $z^M - b$. Then $\sigma(\beta) = \beta + \lambda^{M_\sigma}$ for some $M_\sigma \in R_T$, where λ is a generator of Λ_M. Therefore the map $\sigma \mapsto M_\sigma$ is a injective homomorphism of G into Λ_M.

(2) We define $G \times B \to \Lambda_M$ by $(\sigma, b) \mapsto <\sigma, b>$, where $<\sigma, b> = \sigma(\beta) - \beta$ and $\beta^M = b$. This definition is independent of the choice of the M-root of b. We have $<\sigma, a + b> = <\sigma, a> + <\sigma, b>$ for all $a, b \in B$ and since the definition of $<\sigma, b>$ is independent of the choice of the M-root of b, it follows $<\sigma \cdot \tau, b> = <\sigma, b> + <\tau, b>$.

Let $\sigma \in G$. Suppose $<\sigma, a> = 0$ for all $a \in B$. Then for every α of K_B such that $\alpha^M = a \in B$ we have $\sigma(\alpha) = \alpha$. Hence σ induces the identity on K_B and the left kernel is 1. On the other hand, let $a \in B$ and suppose $<\sigma, a> = 0$ for all $\sigma \in G$. Then $\sigma(\alpha) = \alpha$ for all $\sigma \in G$. Therefore $\alpha \in K$ and $a = \alpha^M \in K^M$. So the right kernel is K^M.

Now suppose that B/K^M is finite. Since the right kernel is K^M, from Proposition 2.10 we obtain that $G = G/1$ is finite. In particular K_B/K is finite. On the other hand if K_B/K is finite then, from Proposition 2.10, we have that the sequence

$$0 \to B/K^M \to \operatorname{Hom}_{R_T}(G/1, \Lambda_M)$$

is exact. Since $\operatorname{Hom}_{R_T}(G/1, \Lambda_M)$ is finite, it follows that B/K^M is finite.

Finally, since by Proposition 2.10 B/K^M is isomorphic to the dual module of G, we have that $B/K^M \cong \widehat{G}$, so $[K_B : K] = (B : K^M)$. □

For our next result we need definition given in [1]

Definition 3.3. An R_T-abelian extension L/K is said to be *R_T-cyclic* if its Galois group is a cyclic R_T-module. In this case, if $\mathrm{Gal}(L/K) \cong R_T/(M)$, where M is a monic polynomial, we say that the R_T-cyclic extension L/K is of order M.

In the following theorem let $\mathfrak{M}$ denote the set of R_T-submodules which contain K^M and let $\mathfrak{F}$ denote the set of R_T-abelian extensions of K with exponent M.

Theorem 3.4. *With the notation of Proposition 3.2, the function $\varphi : \mathfrak{M} \to \mathfrak{F}$ given by $\varphi(B) = K_B$ is injective. Also if L/K is a finite R_T-abelian extension finite of exponent M, then there is a submodule B of K containing K^M, such that $L = K_B$.*

Proof. To show that the function φ is injective, it is enough to prove that if $K_{B_1} \subseteq K_{B_2}$ then $B_1 \subseteq B_2$, since from the equality $\varphi(B_1) = \varphi(B_2)$, it follows that $K_{B_1} \subseteq K_{B_2}$ and that $K_{B_2} \subseteq K_{B_1}$. Let $b \in B_1$. Then $K(\sqrt[M]{b}) \subseteq K_{B_2}$ and $K(\sqrt[M]{b})$ is contained in a finitely generated subextension of K_{B_2}. Thus we may assume, without loss of generality, that B_2/K^M is finitely generated, hence finite.

Now let β be such that $\beta^M = b$. Let B_3 be the submodule of K generated by B_2 and b. We will show that $K_{B_2} = K_{B_3}$. We have $K_{B_2} \subseteq K_{B_3}$. To show $K_{B_2} \supseteq K_{B_3}$, let α be any M-root of $c \in B_3$. Therefore c is of the form $b^N + \sum_{i=1}^{s} b_i^{N_i}$, with $b_i \in B_2$. Then $\alpha^M = b^N + \sum_{i=1}^{s} b_i^{N_i} = \beta^{MN} + \sum_{i=1}^{s} \beta_i^{MN_i}$ with $\beta_i^M = b_i$, $i = 1, \ldots, s$, i.e., $\alpha = \beta^N + \sum_{i=1}^{s} \beta_i^{N_i} + \lambda^A$, where λ is a generator of Λ_M. Therefore $K(\alpha) \subseteq K_{B_2}$. It follows that $K_{B_3} \subseteq K_{B_2}$.

Thus by Proposition 3.2 (2) $(B_2 : K^M) = (B_3 : K^M)$. Hence $b \in B_2$, so that $B_1 \subseteq B_2$.

On the other hand, let K' be a finite R_T-abelian extension of K of exponent M. Let $G = \mathrm{Gal}(K'/K)$. Then, by Theorem 4.7 and Theorem 4.9 Chapter 4 of [3], G is a finite direct sum of R_T-submodules of exponent M. By Galois theory we may assume that the extension K'/K is cyclic of exponent M. Now, by Proposition 2.6 of [1], we have that every R_T-cyclic extension of exponent M is obtained by attaching an M-root of an element of K.

Therefore there exits sets $\{b_j\} \subseteq K$, $\{\alpha_j\} \subseteq K'$ such that $\alpha_j^M = b_j$ and $K' = K(\{\alpha_j\})$. Let B be the submodule of K generated by $\{b_j\}$ and K^M. Then $K' \subseteq K_B$. On the other hand, consider an M-root of $c \in B$, say α. So, $\alpha^M = c$. Other hand $c = \sum_{j=1}^{s} b_j^{N_j} + a^M$, $a \in K$. Then, we have $\alpha = \sum_{j=1}^{s} \alpha_j^{N_j} + a$ therefore $K(\alpha) \subseteq K'$. It follows that $K_B \subseteq K'$ and $\varphi(B) = K'$. This completes the proof. □

Proposition 3.5. *Let L/K be a finite R_T-abelian extension. Assume $\Lambda_N \subseteq K$, with $N \in R_T$. Let*

$$W = \{\overline{a} = a + K^N \in K/K^N \mid \sqrt[N]{a} \in L\}.$$

Then $W \cong \mathrm{Hom}(G, \Lambda_N)$, where $G = \mathrm{Gal}(L/K)$.

Proof. Let $\overline{a} \in W$. We define a function $\varphi_{\overline{a}} : G \to \Lambda_N$, given by $\varphi_{\overline{a}}(\sigma) = \sigma(\alpha) - \alpha$, where α is an N-root of a, i.e., $\alpha^N = a$. The definition of $\varphi_{\overline{a}}$ is independent of the root used. Note that

$$\begin{aligned}
\varphi_{\overline{a}}(\sigma \circ \tau) &= \sigma(\tau(\alpha)) - \alpha \\
&= \sigma(\tau(\alpha) - \alpha + \alpha) - \alpha \\
&= \sigma(\tau(\alpha) - \alpha) + \sigma(\alpha) - \alpha \\
&= \tau(\alpha) - \alpha + \sigma(\alpha) - \alpha.
\end{aligned}$$

Thus $\varphi_{\overline{a}}$ is a homomorphism of abelian groups. Therefore it is possible to define $f : W \to \mathrm{Hom}(G, \Lambda_N)$ given by $f(\overline{\alpha}) = \varphi_{\overline{\alpha}}$.

We have that f is a homomorphism of abelian groups. Now if $f(\overline{a}) = \varphi_{\overline{a}} = 0$ then $\sigma(\alpha) - \alpha = 0$, for all $\sigma \in G$. In this way we obtain that $\alpha \in K$. Since $a = \alpha^N$ then $a \in K^N$. In this way $\overline{a} = 0$, so f is injective.

Now let $\varphi : G \to \Lambda_N$ be a homomorphism of abelian groups. Then

$$\varphi(\sigma \circ \tau) = \varphi(\sigma) + \varphi(\tau) = \varphi(\sigma) + \sigma(\varphi(\tau)),$$

that is, φ is a crossed homomorphism. By the additive Hilbert Theorem 90, there exists $\alpha \in L$ such that $\varphi(\sigma) = \sigma(\alpha) - \alpha$. Therefore $(\sigma(\alpha) - \alpha)^N = \sigma(\alpha^N) - \alpha^N = 0$. Thus $a = \alpha^N \in K$, and this shows that the function f is surjective. □

References

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

[2] D.R. Hayes. Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc,* **189** (1974), 77-91.

[3] P. Hilton, Y. Wu. *A course in modern algebra*, Wiley Interscience Publication John Wiley and Sons. New York, 1974.

[4] S. Lang. *Algebra* 3rd ed, Addison-Wesley Co. Reading, Mass, 1993.

[5] J. Neukirch. *Class field theory,* Springer-Verlag, Berlin Heidelberg, 1986.

[6] F. Schultheis. Carlitz-Kummer Function Fields, *J. Number Theory,* **36** (1990), 133-144.

[7] G. D. Villa Salvador. *Topics in the Theory of Algebraic Function Fields*, Birkhäuser, Boston, 2006.

Received: January, 2013