Korean J. Math. **20** (2012), No. 4, pp. 477–483
http://dx.doi.org/10.11568/kjm.2012.20.4.477

HILBERT ℓ-CLASS FIELD TOWERS OF IMAGINARY ℓ-CYCLIC FUNCTION FIELDS

Hwanyup Jung

Abstract. In this paper we study the infiniteness of the Hilbert ℓ-class field tower of imaginary ℓ-cyclic function fields when $\ell \geq 5$.

1. Introduction

Let $k = \mathbb{F}_q(T), \mathbb{A} = \mathbb{F}_q[T]$ and $\infty = (1/T)$. For a finite extension F of k, write $\mathcal{O}_F$ for the integral closure of $\mathbb{A}$ in F and H_F for the Hilbert class field of F with respect to $\mathcal{O}_F$ ([4]). Let ℓ be a prime number. Let $F_1^{(\ell)}$ be the Hilbert ℓ-class field of $F_0^{(\ell)} = F$, i.e., $F_1^{(\ell)}$ is the maximal ℓ-extension of F inside H_F, and inductively, $F_{n+1}^{(\ell)}$ be the Hilbert ℓ-class field of $F_n^{(\ell)}$ for $n \geq 1$. We obtain a sequence of fields

$$F_0^{(\ell)} = F \subset F_1^{(\ell)} \subset \cdots \subset F_n^{(\ell)} \subset \cdots ,$$

which is called the *Hilbert ℓ-class field tower of F*. We say that the Hilbert ℓ-class field tower of F is *infinite* if $F_n^{(\ell)} \neq F_{n+1}^{(\ell)}$ for each $n \geq 0$. For any multiplicative abelian group A, let $r_\ell(A) = \dim_{\mathbb{F}_\ell}(A/A^\ell)$ be the ℓ-rank of A. Let $\mathcal{C}l_F$ and $\mathcal{O}_F^*$ be the ideal class group and the group of

---

Received November 2, 2012. Revised December 10, 2012. Accepted December 15, 2012.

2010 Mathematics Subject Classification: 11R58, 11R60, 11R18.

Key words and phrases: Hilbert ℓ-class field tower, imaginary ℓ-cyclic function field.

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST)(No.2010-0008139).

units of $\mathcal{O}_F$, respectively. In [6], Schoof proved that the Hilbert ℓ-class field tower of F is infinite if

$$r_\ell(\mathcal{C}l_F) \geq 2 + 2\sqrt{r_\ell(\mathcal{O}_F^*) + 1}.$$

Assume that q is odd, and let ℓ be a prime divisor of $q-1$. By an *imaginary ℓ-cyclic function field*, we always mean a finite (geometric) cyclic extension F of degree ℓ over k in which ∞ is ramified. In [2, 3], we studied the infiniteness of the Hilbert 2-class field tower of imaginary quadratic function fields and of the Hilbert 3-class field tower of imaginary cubic function fields. The aim of this paper is to study the infiniteness of the Hilbert ℓ-class field tower of imaginary ℓ-cyclic function fields when $\ell \geq 5$. We give a several criterions for imaginary ℓ-cyclic function fields to have infinite Hilbert ℓ-class field tower with some examples.

2. Preliminaries

2.1. Rédei matrix and the invariant λ_2. Assume that q is odd, and let ℓ be an odd prime divisor of $q-1$. Write $\mathcal{P}$ for the set of all monic irreducible polynomials in $\mathbb{A}$. Fix a generator γ of $\mathbb{F}_q^*$. Any ℓ-cyclic function field F can be written as $F = k(\sqrt[\ell]{D})$, where $D = aP_1^{r_1} \cdots P_t^{r_t}$ with $a \in \{1, \gamma\}$ and $P_i \in \mathcal{P}$, $1 \leq r_i \leq \ell - 1$ for $1 \leq i \leq t$. Then $F = k(\sqrt[\ell]{D})$ is imaginary if and only if $\ell \nmid \deg D$. Let σ be a generator of $G = Gal(F/k)$. Then we have

$$r_\ell(\mathcal{C}l_F) = \sum_{i=1}^{\ell-1} \lambda_i(F), \tag{2.1}$$

where $\lambda_i(F) = \dim_{\mathbb{F}_\ell}(\mathcal{C}l_F^{(1-\sigma)^{i-1}}/\mathcal{C}l_F^{(1-\sigma)^i})$. By genus theory, $\lambda_1(F) = t-1$. Let $\eta = \gamma^{\frac{q-1}{\ell}}$. For $1 \leq i \neq j \leq t$, let $e_{ij} \in \mathbb{F}_\ell$ be defined by $\eta^{e_{ij}} = (\frac{P_i}{P_j})_\ell$. Let $d_i \in \mathbb{F}_\ell$ be defined by $\deg P_i \equiv d_i \bmod \ell$ for $1 \leq i \leq t$. Let $R'_F = (e_{ij})_{1 \leq i,j \leq t}$ be the $t \times t$ matrix over $\mathbb{F}_\ell$, where the diagonal entries e_{ii} are defined by the relation $\sum_{i=1}^t r_j e_{ij} = 0$ or $d_i + \sum_{i=1}^t r_j e_{ij} = 0$ according as $a = 1$ or $a = \gamma$. Then we have

Proposition 2.1. *For an imaginary ℓ-cyclic function field F over k, we have*

$$\lambda_2(F) = \begin{cases} t - 1 - \operatorname{rank} R'_F & \text{if } a = 1, \\ t - \operatorname{rank} R'_F & \text{if } a = \gamma. \end{cases} \tag{2.2}$$

Proof. Let R_F be the $(t+1)\times t$ matrix over $\mathbb{F}_\ell$ obtained from R'_F by adding $(d_1\cdots d_t)$ in the last row. By [1, Corollary 3.8], we have $\lambda_2(F) = t - \operatorname{rank} R_F$. Using the relation $\sum_{i=1}^t r_j e_{ij} = 0$ or $d_i + \sum_{i=1}^t r_j e_{ij} = 0$ according as $a = 1$ or $a = \gamma$, it can be shown that $\operatorname{rank} R_F = 1 + \operatorname{rank} R'_F$ if $a = 1$ and $\operatorname{rank} R_F = \operatorname{rank} R'_F$ if $a = \gamma$. Hence we get the result. □

2.2. Some lemmas. Let E and K be finite (geometric) separable extensions of k such that E/K is a cyclic extension of degree ℓ, where ℓ is a prime number not dividing q. Write $S_\infty(F)$ for the set of all primes of F lying above ∞. Let $\gamma_{E/K}$ be the number of prime ideals of $\mathcal{O}_K$ that ramify in E and $\rho_{E/K}$ be the number of places $\mathfrak{p}_\infty$ in $S_\infty(K)$ that ramify or inert in E. It is known ([2, Proposition 2.1]) that the Hilbert ℓ-class field tower of E is infinite if

$$(2.3)\quad \gamma_{E/K} \geq |S_\infty(K)| - \rho_{E/K} + 3 + 2\sqrt{\ell|S_\infty(K)| + (1-\ell)\rho_{E/K} + 1}.$$

For $D \in \mathbb{A}$, write $\pi(D)$ for the set of all monic irreducible divisors of D.

LEMMA 2.2. *Assume that $\ell \geq 5$ is a prime divisor of $q-1$. Let $r = 2$ if $\ell = 5$ or 7 and $r = 1$ if $\ell \geq 11$. Let $F = k(\sqrt[\ell]{D})$ be an imaginary ℓ-cyclic function field over k. If there is a nonconstant monic polynomial D' such that $\ell \mid \deg D'$, $\pi(D') \subset \pi(D)$ and $(\frac{D'}{P_1})_\ell = \cdots = (\frac{D'}{P_r})_\ell = 1$ for some $P_1,\ldots,P_r \in \pi(D)\setminus\pi(D')$, then F has infinite Hilbert ℓ-class field tower.*

Proof. Put $K = k(\sqrt[\ell]{D'})$. Then K is an ℓ-cyclic extension of k in which $\infty, P_1,\ldots,P_r$ split completely. Let $E = KF$. Applying (2.3) on E/K with $\gamma_{E/K} \geq r\ell$ and $|S_\infty(K)| = \rho_{E/K} = \ell$, we see that E has infinite Hilbert ℓ-class field tower. Since $E \subset F_1^{(\ell)}$, F also has infinite Hilbert ℓ-class field tower. □

LEMMA 2.3. *Assume that $\ell \geq 5$ is a prime divisor of $q-1$. Let $F = k(\sqrt[\ell]{D})$ be an imaginary ℓ-cyclic function field over k. If there are two distinct nonconstant monic polynomials D_1, D_2 such that $\ell \mid \deg D_i$, $\pi(D_i) \subset \pi(D)$ for $i = 1,2$ and $(\frac{D_1}{P})_\ell = (\frac{D_2}{P})_\ell = 1$ for some $P \in \pi(D)\setminus(\pi(D_1)\cup\pi(D_2))$, then F has infinite Hilbert ℓ-class field tower.*

Proof. Put $K = k(\sqrt[\ell]{D_1}, \sqrt[\ell]{D_2})$. Then K is a bicyclic ℓ^2-extension of k in which ∞, P split completely. Let $E = KF$. By applying (2.3) on E/K with $\gamma_{E/K} \geq \ell^2$ and $|S_\infty(K)| = \rho_{E/K} = \ell^2$, we see that E has infinite Hilbert ℓ-class field tower. Since $E \subset F_1^{(\ell)}$, F also has infinite Hilbert ℓ-class field tower. $\square$

3. Hilbert ℓ-class field tower of imaginary ℓ-cyclic function field

Let $\ell \geq 5$ be a prime divisor of $q-1$. Let $F = k(\sqrt[\ell]{D})$ be an imaginary ℓ-cyclic extension of k, where $D = aP_1^{r_1} \cdots P_t^{r_t}$ with $a \in \{1, \gamma\}$, $P_i \in \mathcal{P}$ and $1 \leq r_i \leq \ell - 1$ for $1 \leq i \leq t$ and $\ell \nmid \deg D$. Since $\mathcal{O}_F^* = \mathbb{F}_q^*$, i.e., $r_\ell(\mathcal{O}_F^*) = 1$, by Schoof's theorem, the Hilbert 3-class field tower of F is infinite if $r_\ell(\mathcal{C}l_F) \geq 5$. Since $\lambda_1(F) = t-1$, F has infinite Hilbert ℓ-class field tower if $t \geq 6$. Let ϑ_F be 0 or 1 according as $a = 1$ or $a = \gamma$. Then, by (2.2), we have $\lambda_1(F) + \lambda_2(F) = 2t - 2 + \vartheta_F - \operatorname{rank} R'_F$. Hence, for the case $t = 4$ or $t = 5$, we have the following theorem.

THEOREM 3.1. *Let ℓ be an odd prime divisor of $q-1$. Let $F = k(\sqrt[\ell]{D})$ be an imaginary ℓ-cyclic function field with $D = aP_1^{r_1} \cdots P_t^{r_t}$. Assume that $t = 4$ or 5. If $\operatorname{rank} R'_F \leq 2t - 7 + \vartheta_F$, then F has infinite Hilbert ℓ-class field tower.*

EXAMPLE 3.2. *Consider $k = \mathbb{F}_{11}(T)$ and $\ell = 5$. Then $\gamma = 2$ is a generator of $\mathbb{F}_{11}^*$ and $\eta = 4$. Let $P_1 = T, P_2 = T+1, P_3 = T+\eta$ and $P_4 = T + \eta^{-1}$. We have $e_{12} = e_{34} = 0, e_{13} = e_{24} = 2, e_{14} = e_{23} = 3$. Let $F = k(\sqrt[5]{D})$ with $D = \gamma P_1 P_2 P_3 P_4$. Then F is an imaginary 5-cyclic function field over k and the matrix R'_F is*

$$\begin{pmatrix} 0 & 0 & 2 & 3 \\ 0 & 0 & 3 & 2 \\ 2 & 3 & 0 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix}$$

whose rank is 2. Then F has infinite Hilbert 5-class field tower by Theorem 3.1.

In the following we will give more simple criterions for the infiniteness of Hilbert ℓ-class field tower of F by using Lemma 2.2 and Lemma 2.3.

THEOREM 3.3. *Assume that $\ell = 5$ or 7. Let $F = k(\sqrt[\ell]{D})$ be an imaginary ℓ-cyclic extension of k with $D = aP_1^{r_1} \cdots P_t^{r_t}$. Then F has infinite Hilbert ℓ-class field tower if one of following conditions holds:*

(1) *$t \geq 4$ and $\ell | \deg P_i$ for $1 \leq i \leq 3$,*

(2) $t \geq 3$ *and* $\ell | \deg P_i, (\frac{P_i}{P_3})_\ell = 1$ *for* $i = 1, 2$.

Proof. For (1), choose $x, y, z, w \in \mathbb{F}_\ell$ such that $(x, y) \neq (0, 0), xe_{14} + ye_{24} = 0$ and $(z, w) \neq (0, 0), ze_{14} + we_{34} = 0$. Let $D_1 = P_1^x P_2^y$ and $D_2 = P_1^z P_3^w$. We have $\ell | \deg D_1, \ell | \deg D_2$ and $(\frac{D_1}{P_4})_\ell = (\frac{D_2}{P_4})_\ell = 1$. Hence, by Lemma 2.3, the Hilbert ℓ-class field tower of F is infinite. (2) is an immediate consequence of Lemma 2.3. □

Let $N(n, q)$ be the number of monic irreducible polynomials of degree n in $\mathbb{A} = \mathbb{F}_q[T]$. Then it satisfies the following one ([5, Corollary of Proposition 2.1]):

$$N(n, q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}. \tag{3.1}$$

For $\alpha \in \mathbb{F}_q^*$, let $N(n, \alpha, q)$ be the number of monic irreducible polynomials of degree n with constant term α in $\mathbb{A} = \mathbb{F}_q[T]$. Let $D_n = \{r : r|(q^n - 1), r \nmid (q^m - 1) \text{ for } m < n\}$. For each $r \in D_n$, let $r = m_r d_r$, where $d_r = \gcd(r, \frac{q^n-1}{q-1})$. In [7], Yucas proved that $N(n, \alpha, q)$ satisfies the following formula:

$$N(n, \alpha, q) = \frac{1}{n\phi(f)} \sum_{\substack{r \in D_n \\ m_r = f}} \phi(r), \tag{3.2}$$

where f is the order of α in $\mathbb{F}_q^*$.

Example 3.4. *Consider* $k = \mathbb{F}_{11}(T)$ *and* $\ell = 5$. *By using* (3.1), *we can see that there are* 32208 *monic irreducible polynomials of degree* 5 *in* $\mathbb{A} = \mathbb{F}_{11}[T]$. *Choose three distinct monic irreducible polynomials* P_1, P_2, P_3 *of degree* 5. *Then* $F = k(\sqrt[5]{TP_1P_2P_3})$ *is an imaginary* 5*-cyclic function field over* k *whose Hilbert* 5*-class field tower of* F *is infinite by Theorem 3.3, (1).*

Example 3.5. *Consider* $k = \mathbb{F}_{29}(T)$ *and* $\ell = 7$. *For any* $\alpha \in \mathbb{F}_{29}^*$, *we have* $(\frac{\alpha}{T})_7 = \alpha^4$. *Using* (3.2), *it can be easily shown that* $N(7, 1, 29) = N(7, -1, 29) = 88009572$. *Let* P_1 *and* P_2 *be monic irreducible polynomials of degree* 7 *in* $\mathbb{A} = \mathbb{F}_{11}[T]$ *with* $P_1(0) = 1$ *and* $P_2(0) = -1$. *Then* $(\frac{P_1}{T})_7 = (\frac{1}{T})_7 = 1$ *and* $(\frac{P_2}{T})_7 = (\frac{-1}{T})_7 = 1$. *Hence* $F = k(\sqrt[7]{TP_1P_2})$ *is an imaginary* 7*-cyclic function field over* k *whose Hilbert* 7*-class field tower of* F *is infinite by Theorem 3.3, (2).*

THEOREM 3.6. *Assume that $\ell \geq 11$. Let $F = k(\sqrt[\ell]{D})$ be an imaginary ℓ-cyclic extension of k with $D = aP_1^{r_1} \cdots P_t^{r_t}$. Then F has infinite Hilbert ℓ-class field tower if one of following conditions holds:*

(1) *$t \geq 3$ and $\ell | \deg P_i$ for $i = 1, 2$,*
(2) *$t \geq 2$ and $\ell | \deg P_1, (\frac{P_1}{P_2})_\ell = 1$.*

Proof. For (1), choose $x, y \in \mathbb{F}_\ell$ such that $(x, y) \neq (0, 0), xe_{13} + ye_{23} = 0$. Let $D = P_1^x P_2^y$. Then D is a monic nonconstant polynomial with $\ell | \deg D$ and $(\frac{D}{P_3})_\ell = \eta^{xe_{13}+ye_{23}} = 1$. Hence, by Lemma 2.2, the Hilbert ℓ-class field tower of F is infinite. (2) is an immediate consequence of Lemma 2.2. □

EXAMPLE 3.7. *Consider $k = \mathbb{F}_{23}(T)$ and $\ell = 11$. By using (3.1), we can see that there are* 86619068901264 *monic irreducible polynomials of degree* 11 *in $\mathbb{A} = \mathbb{F}_{23}[T]$. Choose two distinct monic irreducible polynomials P_1, P_2 of degree* 11. *Then $F = k(\sqrt[11]{TP_1P_2})$ is an imaginary* 11*-cyclic function field over k whose Hilbert* 11*-class field tower of F is infinite by Theorem 3.6, (1).*

EXAMPLE 3.8. *Consider $k = \mathbb{F}_{53}(T)$ and $\ell = 13$. Using (3.2), it can be easily shown that $N(13, 1, 53) = 38515860836695985496$. Let P be a monic irreducible polynomial of degree* 13 *in $\mathbb{A} = \mathbb{F}_{53}[T]$ with $P(0) = 1$. Then $(\frac{P}{T})_{13} = (\frac{1}{T})_{13} = 1$. Hence $F = k(\sqrt[13]{TP})$ is an imaginary* 13*-cyclic function field over k whose Hilbert* 13*-class field tower of F is infinite by Theorem 3.6, (2).*

References

[1] S. Bae, S. Hu and H. Jung, *The generalized Rédei matrix for function fields*, Finite Fields Appl. **18** (2012), no. 4, 760–780.

[2] H. Jung, *Hilbert* 2*-class field towers of imaginary quadratic function fields* submitted.

[3] ———, *Hilbert* 3*-class field towers of imaginary cubic function fields*, submitted.

[4] M. Rosen, *The Hilbert class field in function fields*, Expo. Math. **5** (1987), no. 4, 365–378.

[5] ———, Number theory in function fields, Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002.

[6] R. Schoof, *Algebraic curves over $\mathbb{F}_2$ with many rational points*, J. Number Theory **41** (1992), no. 1, 6–14.

[7] J.L. Yucas, *Irreducible polynomials over finite fields with prescribed trace/prescribed constant term*, Finite Fields Appl. **12** (2006), 211–221.

Department of Mathematics Education
Chungbuk National University
Cheongju 361-763, Korea
E-mail: hyjung@chungbuk.ac.kr