JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **26**, No. 3, August 2013

HILBERT 3-CLASS FIELD TOWERS OF REAL CUBIC FUNCTION FIELDS

Hwanyup Jung*

Abstract. In this paper we study the infiniteness of Hilbert 3-class field tower of real cubic function fields over $\mathbb{F}_q(T)$, where $q \equiv 1 \bmod 3$. We also give various examples of real cubic function fields whose Hilbert 3-class field tower is infinite.

1. Introduction

Let $k = \mathbb{F}_q(T)$ be a rational function field over the finite field $\mathbb{F}_q$ of q and $\mathbb{A} = \mathbb{F}_q[T]$. For a finite separable extension F of k, write $\mathcal{O}_F$ for the integral closure of $\mathbb{A}$ in F. Let ∞ be the infinite place of k and $S_\infty(F)$ be the set of places of F lying over ∞. Let ℓ be a prime number. The *Hilbert ℓ-class field of F* is the maximal unramified abelian ℓ-extension of F in which every places $\nu_\infty \in S_\infty(F)$ splits completely. Let $F_0^{(\ell)} = F$ and inductively, $F_{n+1}^{(\ell)}$ be the Hilbert ℓ-class field of $F_n^{(\ell)}$ for $n \geq 0$ (cf. [4]). Then the sequence of fields

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

is called the *Hilbert ℓ-class field tower of F* and 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 a multiplicative abelian group A, let $r_\ell(A) = \dim_{\mathbb{F}_\ell}(A/A^\ell)$ be the the ℓ-rank of A. Let $\mathcal{C}l_F$ and $\mathcal{O}_F^*$ be the ideal class group and the group of units of $\mathcal{O}_F$, respectively. Schoof [6] proved that the Hilbert ℓ-class field tower of F is infinite if

$$r_\ell(\mathcal{C}l_F) \geq 2 + 2\sqrt{r_\ell(\mathcal{O}_F^*) + 1}. \tag{1.1}$$

Received March 18, 2013; Accepted July 08, 2013.
2010 Mathematics Subject Classification: 11R58, 11R60, 11R18.
Key words and phrases: Hilbert 3-class field tower, real cubic function field.
This work was conducted during the research year of the Chungbuk National University in 2012 .

In [1], Ahn and Jung studied the infiniteness of the Hilbert 2-class field tower of imaginary quadratic function fields. Assume that q is odd with $q \equiv 1 \bmod 3$. In [3], we studied the infiniteness of the Hilbert 3-class field tower of imaginary cubic function fields. By a *real cubic function field*, we always mean a finite (geometric) cyclic extension F over k of degree 3 in which ∞ splits completely. The aim of this paper is to study the infiniteness of the Hilbert 3-class field tower of real cubic function fields and give a various examples of real cubic function fields which have infinite Hilbert 3-class field tower.

2. Preliminaries

2.1. Rédei matrix and the invariant λ_2

Assume that q is odd with $q \equiv 1 \bmod 3$. Fix a generator γ of $\mathbb{F}_q^*$. Let $\mathcal{P}(\mathbb{A})$ be the set of all monic irreducible polynomials in $\mathbb{A}$. Assume that we have given a total ordering "$<$" on the set $\mathcal{P}(\mathbb{A})$ such that $P < Q$ for any $P, Q \in \mathcal{P}(\mathbb{A})$ with $\deg P < \deg Q$. Then any real cubic function field F can be written as $F = k(\sqrt[3]{D})$, where $D = P_1^{r_1} \cdots P_t^{r_t}$ with $P_i \in \mathcal{P}(\mathbb{A})$, $r_i \in \{1, 2\}$ for $2 \le i \le t$ and $3 | \deg D$. If we assume that $P_1 < \cdots < P_t$ and $r_1 = 1$, then D is uniquely determined by F, and we denote $D_F = D$. We say that D_F is *special* if $3 | \deg P_i$ for all $1 \le i \le t$. Let σ be a generator of $G = Gal(F/k)$. We have

$$r_3(\mathcal{C}l_F) = \dim_{\mathbb{F}_3}\left(\mathcal{C}l_F/\mathcal{C}l_F^{(1-\sigma)}\right) + \dim_{\mathbb{F}_3}\left(\mathcal{C}l_F^{(1-\sigma)}/\mathcal{C}l_F^{(1-\sigma)^2}\right). \tag{2.1}$$

Put

$$\lambda_i(F) = \dim_{\mathbb{F}_3}\left(\mathcal{C}l_F^{(1-\sigma)^{i-1}}/\mathcal{C}l_F^{(1-\sigma)^i}\right) \quad (i = 1, 2).$$

For $0 \ne N \in \mathbb{A}$, write $\omega(N)$ for the number of distinct monic irreducible divisors of N. Then, by the Genus theory (see [2, Corollary 3.5]), we have

$$\lambda_1(F) = \begin{cases} \omega(D_F) - 1, & \text{if } D_F \text{ is special,} \\ \omega(D_F) - 2, & \text{otherwise.} \end{cases} \tag{2.2}$$

Let $\eta = \gamma^{\frac{q-1}{3}}$. Let M_F be the $t \times t$ matrix $(e_{ij})_{1 \le i,j \le t}$ over $\mathbb{F}_3$, where, for $1 \le i \ne j \le t$, $e_{ij} \in \mathbb{F}_3$ is defined by $\eta^{e_{ij}} = (\frac{P_i}{P_j})_3$, and the diagonal entries e_{ii} are defined to satisfy the relation $\sum_{i=1}^t r_j e_{ij} = 0$. Let $d_i \in \mathbb{F}_3$ be defined by $d_i \equiv \deg P_i \bmod 3$ for $1 \le i \le t$. We associate a $(t+1) \times t$ matrix R_F over $\mathbb{F}_3$ to F as follows:

- If D_F is non-special or D_F is special with $\gamma \in N_{F/k}(\mathcal{O}_F^*)$, then R_F is the $(t+1)\times t$ matrix obtained from M_F by adjoining $(d_1, \dots, d_t)$ in last row.
- If D_F is special with $\gamma \notin N_{F/k}(\mathcal{O}_F^*)$, then R_F is the $(t+1)\times t$ matrix obtained from M_F by adjoining $(e_{B1}, \dots, e_{Bt})$ in last row, where $B \in \mathbb{A}$ is a monic polynomial such that $B = \mathcal{N}(\mathfrak{B})$, $\mathfrak{B}^{\sigma-1} = x\mathcal{O}_F$, $N_{F/k}(x) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*3}$ and $e_{Bi} \in \mathbb{F}_3$ is defined by $\eta^{e_{iB}} = (\frac{P_i}{B})$.

Then we have (see [2, Corollary 3.8])

$$\lambda_2(F) = \omega(D_F) - 1 - \operatorname{rank} R_F. \tag{2.3}$$

Hence, by inserting (2.2) and (2.3) into (2.1), we have

$$r_3(\mathcal{C}l_F) = \begin{cases} 2\omega(D_F) - 2 - \operatorname{rank} R_F, & \text{if } D_F \text{ is special,} \\ 2\omega(D_F) - 3 - \operatorname{rank} R_F, & \text{otherwise.} \end{cases} \tag{2.4}$$

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. 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. If

$$\gamma_{E/K} \geq |S_\infty(K)| - \rho_{E/K} + 3 + 2\sqrt{\ell|S_\infty(K)| + (1-\ell)\rho_{E/K} + 1}, \tag{2.5}$$

then E has infinite Hilbert ℓ-class field tower (see [1, Proposition 2.1]). By using this criterion, we give some sufficient conditions for a real cubic function field to have infinite Hilbert 3-class field tower. For $D \in \mathbb{A}$, write $\pi(D)$ for the set of all monic irreducible divisors of D.

LEMMA 2.1. *Assume that q is odd with $q \equiv 1 \bmod 3$. Let F be a real cubic function field over k. If there is a nonconstant monic polynomial D' such that $3|\deg D'$, $\pi(D') \subset \pi(D_F)$ and $(\frac{D'}{P_i})_3 = 1$ for $P_i \in \pi(D) \setminus \pi(D')$ $(1 \leq i \leq 5)$, then F has infinite Hilbert 3-class field tower.*

Proof. Put $K = k(\sqrt[3]{D'})$ and $E = FK$. Since $\gamma_{E/K} \geq 15$, $|S_\infty(K)| = 3$ and $\rho_{E/K} = 0$, the inequality (2.5) is satisfied, so E has infinite Hilbert 3-class field tower. By hypothesis, P_1, P_2, P_3, P_4, P_5 and ∞ split completely in K, so E is contained in $F_1^{(3)}$. Hence F also has infinite Hilbert 3-class field tower. ☐

LEMMA 2.2. *Assume that q is odd with $q \equiv 1 \bmod 3$. Let F be a real cubic function field over k. If there are two distinct nonconstant monic polynomials D_1, D_2 such that $3|\deg D_i$, $\pi(D_i) \subset \pi(D_F)$ for $i = 1, 2$ and*

$(\frac{D_1}{P_j})_3 = (\frac{D_2}{P_j})_3 = 1$ for some $P_j \in \pi(D_F) \setminus (\pi(D_1) \cup \pi(D_2))$ $(1 \leq j \leq 3)$, then F has infinite Hilbert 3-class field tower.

Proof. Put $K = k(\sqrt[3]{D_1}, \sqrt[3]{D_2})$ and $E = FK$. Since $\gamma_{E/K} \geq 27$, $|S_\infty(K)| = 9$ and $\rho_{E/K} = 0$, the inequality (2.5) is satisfied, so E has infinite Hilbert 3-class field tower. By hypothesis, P_1, P_2, P_3 and ∞ split completely in K, so E is contained in $F_1^{(3)}$. Hence F also has infinite Hilbert 3-class field tower. □

3. Hilbert 3-class field tower of real cubic function field

Assume that q is odd with $q \equiv 1 \bmod 3$. In this section we give several sufficient conditions for real cubic function fields to have infinite Hilbert 3-class field tower and examples.

Let F be a real cubic function field. Since $r_3(\mathcal{O}_F^*) = 2$, by Schoof's theorem, the Hilbert 3-class field tower of F is infinite if $r_3(\mathcal{C}l_F) \geq 6$. By (2.2), F has infinite Hilbert 3-class field tower if $\omega(D_F) \geq 7$ or $\omega(D_F) \geq 8$ according as D_F is special or not. We will consider the cases that $\omega(D_F) \leq 6$ if D_F is special and $\omega(D_F) \leq 7$ if D_F is non-special.

THEOREM 3.1. *Assume that q is odd with $q \equiv 1 \bmod 3$. Let F be a real cubic function field.*

(i) *Assume that D_F is special. If $\omega(D_F) = 6$ with $\operatorname{rank} R_F \leq 4$, $\omega(D_F) = 5$ with $\operatorname{rank} R_F \leq 2$ or $\omega(D_F) = 4$ with $\operatorname{rank} R_F = 0$, then F has infinite Hilbert 3-class field tower.*

(ii) *Assume that D_F is non-special. If $\omega(D_F) = 7$ with $\operatorname{rank} R_F \leq 5$, $\omega(D_F) = 6$ with $\operatorname{rank} R_F \leq 3$ or $\omega(D_F) = 5$ with $\operatorname{rank} R_F \leq 1$, then F has infinite Hilbert 3-class field tower.*

Proof. By using the Schoof's theorem with (2.4), we see that F has infinite Hilbert 3-class field tower if

$$\operatorname{rank} R_F \leq \begin{cases} 2\omega(D_F) - 8, & \text{if } D_F \text{ is special,} \\ 2\omega(D_F) - 9, & \text{if } D_F \text{ is non-special.} \end{cases}$$

Hence the result follows immediately. □

THEOREM 3.2. *Assume that q is odd with $q \equiv 1 \bmod 3$. Let F be a real cubic function field with $\omega(D_F) \geq 6$. If there exists $Q \in \pi(D_F)$ with $3 | \deg Q$ and $P_i \in \pi(D_F) \setminus \{Q\}$ such that $(\frac{Q}{P_i})_3 = 1$ $(1 \leq i \leq 5)$, then F has infinite Hilbert 3-class field tower.*

Proof. By applying Lemma 2.1 with $D' = Q$, we see that F has infinite Hilbert 3-class field tower. $\square$

EXAMPLE 3.3. *Let* $k = \mathbb{F}_7(T)$ *and* $\mathbb{A} = \mathbb{F}_7[T]$. *Take* $Q = T^3+2T^2+1$, $P_1 = T$, $P_2 = T+2$, $P_3 = T+3$, $P_4 = T^2+2$ *and* $P_5 = T^3+T+1$. *By simple computations, we see that* $(\frac{Q}{P_i})_3 = 1$ *for* $1 \le i \le 5$. *Then, for any* $D = Q^e P_1^{e_1} P_2^{e_2} P_3^{e_3} P_4^{e_4} P_5^{e_5}$ *with* $e, e_i \in \{1,2\}$ *and* $e_1+e_2+e_3+2e_4 \equiv 0 \bmod 3$, $k(\sqrt[3]{D})$ *is a real cubic function field whose Hilbert* 3*-class field tower is infinite by Theorem 3.2.*

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]):

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

For $\alpha \in \mathbb{F}_q^*$, let $\mathcal{N}(n,\alpha,q)$ be the set of monic irreducible polynomials of degree n with constant term α in $\mathbb{A} = \mathbb{F}_q[T]$ and $N(n,\alpha,q) = |\mathcal{N}(n,\alpha,q)|$. Define

$$D_n = \{r : r|(q^n-1), r \nmid (q^m-1) \text{ for } m < n\}.$$

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:

$$N(n,\alpha,q) = \frac{1}{n\phi(f)} \sum_{\substack{r\in D_n \\ m_r = f}} \phi(r), \tag{3.1}$$

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

EXAMPLE 3.4. *Let* $k = \mathbb{F}_7(T)$ *and* $\mathbb{A} = \mathbb{F}_7[T]$. *We will find the number* $N(3,1,7)$. *We have*

$$D_3 = \{r : r|(7^3-1), r\nmid(7^2-1), r\nmid(7-1)\} = \{9,18,19,38,57,114,171,342\}$$

and $m_9 = 1$, $m_{18} = 6$, $m_{19} = 1$, $m_{38} = 2$, $m_{57} = 1$, $m_{114} = 2$, $m_{171} = 3$, $m_{342} = 6$. *Since the order of* 1 *in* $\mathbb{F}_7^*$ *is* 1, *by* (3.1), *we have*

$$N(3,1,7) = \frac{1}{3\phi(1)}(\phi(9)+\phi(19)+\phi(57)) = 20.$$

Hence, $\mathcal{N}(3,1,7)$ *consists of exactly* 20 *distinct monic irreducible polynomials. Take* $Q = T$, $P_1 = T^2+\alpha T+1$ *with* $\alpha \in \{0,3,4\}$ *and* $P_2, P_3, P_4, P_5 \in \mathcal{N}(3,1,7)$. *Then, for any* $D = Q^e P_1^{e_1} P_2^{e_2} P_3^{e_3} P_4^{e_4} P_5^{e_5}$ *with* $e, e_i \in \{1,2\}$ *and* $e_1+e_2+e_3+2e_4 \equiv 0 \bmod 3$, *we have* $(\frac{Q}{P_i})_3 = 1$

for $1 \le i \le 5$, *so* $k(\sqrt[3]{D})$ *is a real cubic function field whose Hilbert 3-class field tower is infinite by Theorem 3.2.*

THEOREM 3.5. *Assume that q is odd with $q \equiv 1 \bmod 3$. Let F be a real cubic function field with $\omega(D_F) \ge 5$. If there exist $Q_1, Q_2 \in \pi(D_F)$ whose degrees are divisible by 3 and $P_i \in \pi(D_F) \setminus \{Q_1, Q_2\}$ such that $(\frac{Q_1}{P_i})_3 = (\frac{Q_2}{P_i})_3 = 1$ $(1 \le i \le 3)$, then F has infinite Hilbert 3-class field tower.*

Proof. By applying Lemma 2.2 with $D_1 = Q_1$ and $D_2 = Q_2$, we see that F has infinite Hilbert 3-class field tower. □

EXAMPLE 3.6. *Let $k = \mathbb{F}_7(T)$ and $\mathbb{A} = \mathbb{F}_7[T]$. Take $P_1 = T$, $P_2 = T+1$, $P_3 = T^2+1$, $Q_1 = T^3+T^2+1$ and $Q_2 = T^3+T+1$. By simple computations, we see that $(\frac{Q_1}{P_i})_3 = (\frac{Q_2}{P_i})_3 = 1$ for $1 \le i \le 3$. Then, for any $D = P_1^{e_1}P_2^{e_2}P_3^{e_3}Q_1^{f_1}Q_2^{f_2}$ with $e_i, f_j \in \{1,2\}$ and $e_1 + e_2 + 2e_3 \equiv 0 \bmod 3$, $k(\sqrt[3]{D})$ is a real cubic function field whose Hilbert 3-class field tower is infinite by Theorem 3.5.*

THEOREM 3.7. *Assume that q is odd with $q \equiv 1 \bmod 3$. Let F be a real cubic function field with non-special D_F. Assume that $\omega(D_F) = 6$ or $\omega(D_F) = 7$. If there exist $Q_1, Q_2, Q_3 \in \pi(D_F)$ whose degrees are divisible by 3 and $P_i \in \pi(D_F) \setminus \{Q_1, Q_2, Q_3\}$ such that $(\frac{Q_1Q_2}{P_i})_3 = (\frac{Q_1Q_3}{P_i})_3 = 1$ $(1 \le i \le 3)$, then F has infinite Hilbert 3-class field tower.*

Proof. By applying Lemma 2.2 with $D_1 = Q_1Q_2$ and $D_2 = Q_1Q_3$, we see that F has infinite Hilbert 3-class field tower. □

EXAMPLE 3.8. *Let $k = \mathbb{F}_7(T)$ and $\mathbb{A} = \mathbb{F}_7[T]$. Take $P_1 = T$, $P_2 = T+2$, $P_3 = T^2+1$, $Q_1 = T^3+T+1$, $Q_2 = T^3+T^2+1$ and $Q_3 = T^3+T-1$. By simple computations, we see that*

$$\left(\frac{Q_i}{P_1}\right)_3 = \left(\frac{Q_i}{P_3}\right)_3 = 1\,(1 \le i \le 3),\ \left(\frac{Q_1}{P_2}\right)_3 = \eta^2,\ \left(\frac{Q_2}{P_2}\right)_3 = \left(\frac{Q_3}{P_2}\right)_3 = \eta.$$

Hence, we have

$$\left(\frac{Q_1Q_2}{P_i}\right)_3 = \left(\frac{Q_1Q_3}{P_i}\right)_3 = 1\ (1 \le i \le 3).$$

Then, for any $D = P_1^{e_1}P_2^{e_2}P_3^{e_3}Q_1^{f_1}Q_2^{f_2}$ with $e_i, f_j \in \{1,2\}$ and $e_1 + e_2 + 2e_3 \equiv 0 \bmod 3$, $k(\sqrt[3]{D})$ is a real cubic function field whose Hilbert 3-class field tower is infinite by Theorem 3.7.

References

[1] J. Ahn and H. Jung, *Hilbert* 2*-class field towers of imaginary quadratic function fields.* J. Chungcheong Math. Soc. **23** (2010), no. 4, 699–704.

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

[3] H. Jung, *Hilbert* 3*-class field towers of imaginary cubic function fields.* J. Chungcheong Math. Soc. **26** (2013), no. 1, 161–166.

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

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

[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), no. 2, 211–221.

*

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