JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **24**, No. 3, September 2011

NOTE ON CLASS NUMBER OF REAL CYCLOTOMIC FUNCTION FIELD

Hwanyup Jung*

Abstract. We prove that for any positive integer $g \geq 3$, there are $\gg q^{\frac{l}{2g}}$ real cyclotomic function fields whose conductor has degree $\leq l$ and ideal class number is divisible by $\frac{g}{\gcd(2,g)}$.

1. Introduction

For an integer $m > 2$, the divisibility of class number h_m^+ of the maximal real subfield $\mathbb{Q}(\zeta_m + \zeta_m^+)$ of m-th cyclotomic field $\mathbb{Q}(\zeta_m)$ has been studied by many authors ([1, 5, 6, 7, 9, 10]). Many results are obtained by studying the class number of quadratic, cubic, or cyclic subfield of $\mathbb{Q}(\zeta_m + \zeta_m^+)$. In this paper, we study the class number of maximal real subfield of cyclotomic function field by adapting Osada's methods in [7].

Let q be a power of an prime number p. Let $k = \mathbb{F}_q(T)$ be a rational function field over the finite field $\mathbb{F}_q$ and $\mathbb{A} = \mathbb{F}_q[T]$. For any monic polynomial $N \in \mathbb{A}$, we denote by K_N the N-th cyclotomic function field and K_N^+ be its maximal real subfield, which is also called the *N-th real cyclotomic function field*. Let $\mathcal{O}_N^+$ be the integral closure of $\mathbb{A}$ in K_N^+ and h_N^+ be the ideal class number of $\mathcal{O}_N^+$. For more details on the theory of cyclotomic function field, we refer Rosen's book ([8, chapter 12]).

In this paper, we shall prove the following theorem.

Theorem 1.1. *For any positive integer $g \geq 3$, there are $\gg q^{\frac{l}{2g}}$ real cyclotomic function fields K_N^+ such that $\deg N \leq l$ and h_N^+ is divisible by $\frac{g}{\gcd(2,g)}$.*

Received July 07, 2011; Accepted August 25, 2011.
2010 Mathematics Subject Classification: Primary 11R58, 11R60, 11R29.
Key words and phrases: real cyclotomic function field, class number.
The author was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2011-0005138).

2. Genus theory in function field

In this section we recall genus theory in function field ([2]) and prove a proposition which will play an important role in the proof of Theorem 1.1. Let ∞ be the place of k associated to $1/T$ and k_∞ the completion of k at ∞. Put $\widetilde{C} := k_\infty(\sqrt[q-1]{-1/T})$. In the following we mean by an *extension* of k, a separable extension of k for which any of its embedding into k_∞^{ac} lies in $\widetilde{C}$ viewing as a subfield of k_∞^{ac}. In particular, any finite abelian extension F of k is contained in some cyclotomic function field. In this case the monic polynomial N of minimal degree such that K_N contains F is called the the conductor N. We say that an extension F of k is *real* if ∞ splits completely in F. Let $\mathcal{O}_F$ be the integral closure of $\mathbb{A}$ in F and $\mathcal{C}l(F)$ be the ideal class group of $\mathcal{O}_F$, $h(F) = |\mathcal{C}l(F)|$, which is called the ideal class number of F.

Let ℓ be a prime number and F be a real cyclic extension of degree ℓ of k. The ordinary Hilbert class field H_F of F is the maximal abelian extension of F in which every infinite primes of F split completely. Then ordinary genus field $G(F/k)$ of F/k is defined as the maximal abelian extension of k inside H_F. The narrow Hilbert class field H_F^+ of F is the maximal abelian extension of F inside $\widetilde{C}$ and the narrow genus field $G^+(F/k)$ is defined as the maximal abelian extension of k inside H_F^+. The Galois groups $\mathfrak{G}(F/k) = \mathrm{Gal}(G(F/k)/F)$ and $\mathfrak{G}^+(F/k) = \mathrm{Gal}(G^+(F/k)/F)$ are called the genus group and narrow genus group of F/k, respectively. In the case $\ell|(q-1)$, any real cyclic extension F of degree ℓ of k is a Kummer extension, so it can be written as $F = k(\sqrt[\ell]{N})$, where $N \in \mathbb{A}$ is an ℓ-th power free monic polynomial and $\deg N$ divisible by ℓ.

The following lemmas will be used to prove proposition 2.4.

LEMMA 2.1. *Assume that ℓ is a prime divisor of $q-1$. Let $F = k(\sqrt[\ell]{N})$ be a real cyclic extension of degree ℓ of k, where $N \in \mathbb{A}$ is an ℓ-th power free monic polynomial with monic irreducible factorization $N = P_t^{r_t} \cdots P_t^{r_t}$. Set $P_i^* = (-1)^{\deg P_i} P_i$. Then the narrow genus field $G^+(F/k)$ is given as*

$$G^+(F/k) = k\big(\sqrt[\ell]{P_1^*}, \ldots, \sqrt[\ell]{P_t^*}\big).$$

Proof. See [2, §1]. □

LEMMA 2.2. *If $\ell \nmid (q-1)$, then we have $G(F/k) = G^+(F/k)$.*

Proof. See [2, Proposition 2.3]. □

LEMMA 2.3. *The narrow genus group $\mathfrak{G}^+(F/k)$ is an elementary abelian ℓ-group of rank $t-1$, where t is the number of finite places of k ramifying in F.*

Proof. See [2, Theorem 3.10]. □

PROPOSITION 2.4. *Let ℓ be a prime number and F be a real cyclic extension of degree ℓ of k. If N_0 is the conductor of F, then the ideal class group $\mathcal{C}l(K_{N_0}^+)$ has a subgroup which is isomorphic to $\mathcal{C}l(F)^\ell$.*

Proof. We first assume that ℓ is a prime divisor of $q-1$. Then $F = k(\sqrt[\ell]{N})$ for some ℓ-th power free monic polynomial $N \in \mathbb{A}$ of degree $\deg N$ divisible by ℓ. Let $N = P_1^{r_1} \cdots P_t^{r_t}$ be the monic irreducible factorization of N and write $N_0 = P_1 \cdots P_t$. Then N_0 is the conductor of F and $G^+(F/k) = k(\sqrt[\ell]{P_1^*}, \ldots, \sqrt[\ell]{P_t^*})$ (see Lemma 2.1). Hence, we can see that $\mathrm{Gal}(G^+(F/k)/F)$ is an elementary abelian ℓ-group of rank $t-1$. Let $M = G^+(F/k) \cap H_F$. Let $\mathcal{H}$ be the subgroup of $\mathcal{C}l(F)$ which is isomorphic to $\mathrm{Gal}(H_F/M)$ under the Artin isomorphism $\mathcal{C}l(F) \cong \mathrm{Gal}(H_F/F)$. Since $\mathrm{Gal}(G^+(F/k)/F)$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^{t-1}$, $\mathcal{C}l(F)/\mathcal{H}$ is an elementary ableian ℓ-group. Hence, $\mathcal{C}l(F)^\ell$ is contained in $\mathcal{H}$. Since $G^+(F/k)$ is contained in K_{N_0}, M is contained in $K_{N_0}^+$. Since $G^+(F/k)$ is the narrow genus field of F/k, we have $K_{N_0}^+ \cap H_F = M$. Hence the compositum $K_{N_0}^+ H_F$ of $K_{N_0}^+$ and H_F is an unramified abelian extension of $K_{N_0}^+$ in which all infinite primes of K_N^+ splits completely, and $\mathrm{Gal}(K_{N_0}^+ H_F/K_{N_0}^+)$ is isomorphic to $\mathrm{Gal}(H_F/M)$. Since $\mathrm{Gal}(H_F/M)$ is isomorphic to $\mathcal{H}$ which is a subgroup $\mathcal{C}l(F)^\ell$, $\mathrm{Gal}(K_{N_0}^+ H_F/K_{N_0}^+)$ has a subgroup which is isomorphic to $\mathcal{C}l(F)^\ell$. Hence $\mathcal{C}l(K_{N_0}^+)$ has a subgroup which is isomorphic to $\mathcal{C}l(F)^\ell$.

Next, we prove the assertion in the case when $\ell \nmid (q-1)$. In this case $G^+(F/k)$ is equal to the genus field $G(F/k)$, so $G^+(F/k)$ is a subfield of Hilbert class field H_F. Let $\mathcal{H}$ be the subgroup of $\mathcal{C}l(F)$ which is isomorphic to $\mathrm{Gal}(H_F/G^+(F/k))$ under the Artin isomorphism $\mathcal{C}l(F) \cong \mathrm{Gal}(H_F/F)$. By Lemma 2.3, $\mathrm{Gal}(G^+(F/k)/F)$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^{t-1}$, where t is the number of finite places of k ramifying in F. Hence $\mathcal{C}l(F)/\mathcal{H}$ is also an elementary ableian ℓ-group, so $\mathcal{C}l(F)^\ell$ is contained in $\mathcal{H}$. Since $G^+(F/k)$ is contained in the cyclotomic function field K_{N_0}, $G^+(F/k)$ is contained in $K_{N_0}^+$ and $K_{N_0}^+ \cap H_F = G^+(F/k)$. In the same way as in the proof of this proposition for the case $\ell | (q-1)$, we can show that $\mathcal{C}l(K_{N_0}^+)$ has a subgroup which is isomorphic to $\mathcal{C}l(F)^\ell$. □

3. Proof of Theorem 1.1

In this section we give a proof of Theorem 1.1. First, we consider the case when q is odd. Note that any real quadratic extension F of k is of the form $F = k(\sqrt{N})$, where N is a monic square-free polynomial of even degree, and F is always contained in the real cyclotomic function field K_N^+, that is, N is the conductor of $F = k(\sqrt{N})$. In [4], Chakraborty and Mukhopadhyay has shown that for any positive integer $g \geq 3$, there are $\gg q^{l/2g}$ real quadratic extensions $k(\sqrt{N})$ such that $\deg N \leq l$ and the ideal class group $\mathcal{C}l(\mathcal{O}_{k(\sqrt{N})})$ of $\mathcal{O}_{k(\sqrt{N})}$ has an element of order g. By applying Proposition 2.4 to such N's with $\ell = 2$, we can see that the ideal class group $\mathcal{C}l(K_N^+)$ has a subgroup which is isomorphic to $\mathcal{C}l(\mathcal{O}_{k(\sqrt{N})})^2$. Then, by the result of Chakraborty and Mukhopadhyay, $\mathcal{C}l(K_N^+)$ has an element of order $\frac{g}{\gcd(2,g)}$. Hence, h_N^+ is divisible by $\frac{g}{\gcd(2,g)}$. This competes the proof of Theorem 1.1 when q is odd.

Now, we consider the case when q is even. Any separable quadratic extension F of k can be written as $F = k(\alpha)$, where α is a zero of $\mathbf{x}^2 + A\mathbf{x} + B = 0$ with $A, B \in \mathbb{A}$. Here, we can always assume that A is monic and (A, B) satisfies the property that for any irreducible polynomial P dividing A, the congruence

$$\mathbf{x}^2 + A\mathbf{x} + B \equiv 0 \bmod P^2$$

is not solvable in $\mathbb{A}$. Then we have $\mathcal{O}_F = \mathbb{A}[\alpha]$ and A is uniquely determined since the discriminant of $\mathcal{O}_F$ is A^2. Write $d(F) = \deg A$. Recently, Bae and Jung [3] has shown that for any positive integer $g \geq 2$, there are $\gg q^{\nu(g,\ell)}$ real quadratic extensions F of k such that $d(F) \leq \ell$ and the ideal class group of $\mathcal{O}_F$ contains an element of order g, where $\nu(g, \ell)$ is $\frac{\ell}{2g}$ or $\frac{\ell}{g+1}$ according as g is odd or even. It is easy to see that the conductor of $F = k(\alpha)$ is A^2, i.e., F is contained in the real cyclotomic function field $K_{A^2}^+$. By Proposition 2.4, we can see that the ideal class group $\mathcal{C}l(K_{A^2}^+)$ has a subgroup which is isomorphic to $\mathcal{C}l(\mathcal{O}_F)^2$. Then, by the result of Bae and Jung, $\mathcal{C}l(K_{A^2}^+)$ has an element of order $\frac{g}{\gcd(2,g)}$. Hence, $h_{A^2}^+$ is divisible by $\frac{g}{\gcd(2,g)}$. This competes the proof of Theorem 1.1 when q is even.

References

[1] N. C. Ankeny, S. Chowla and H. Hasse, *On the class-number of the maximal real subfield of a cyclotomic field.* J. reine angew. Math. **217** (1965), 217–220.

[2] S. Bae and J. Koo, *Genus theory for function fields.* J. Austral. Math. Soc. Ser. A **60** (1996), no. 3, 301–310.
[3] S. Bae and H. Jung, *Class number divisibility of quadratic function fields in even characteristic.* submitted.
[4] K. Chakraborty and A. Mukhopadhyay, *Exponents of class groups of real quadratic function fields.* Proc. Amer. Math. Soc. **132** (2004), 1951–1955.
[5] S. D. Lang, *Note on the class-number of the maximal real subfield of a cyclotomic field.* J. reine angew. Math. **290** (1977), 70–72.
[6] H. Osada, *Note on the class-number of the maximal real subfield of a cyclotomic field.* Manuscripta Math. **58** (1987), 215–227.
[7] ———, *Note on the class-number of the maximal real subfield of a cyclotomic field, II.* Nagoya Math. J. **113** (1989), 147–151.
[8] M. Rosen, Number Theory in Function Fields. Springer-Verlag, New York, 2002.
[9] H. Takeuchi, *On the class-number of the maximal real subfield of a cyclotomic field.* Canadian J. Math. **33** (1981), 55–58.
[10] I. Yamaguchi, *On the class-number of the maximal real subfield of a cyclotomic field.* J. reine angew. Math. **272** (1975), 217–220.

*

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