CYCLOTOTOMIC UNITS AND DIVISIBILITY OF
THE CLASS NUMBER OF FUNCTION FIELDS

JAEHYUN AHN AND HWANYUP JUNG

ABSTRACT. Let $k = \mathbb{F}_q(T)$ be a rational function field. Let $\ell$ be a
prime number with $(\ell, q-1) = 1$. Let $K/k$ be an elementary abelian
$\ell$-extension which is contained in some cyclotomic function field. In
this paper, we study the $\ell$-divisibility of ideal class number $h_K$ of
$K$ by using cyclotomic units.

1. Introduction

Let $K$ be a finite abelian number field. When $K$ is a real extension,
the class number $h_K$ of $K$ is difficult to calculate. If the conductor of
$K$ is divisible by many primes $q_1, \ldots, q_s$, where each $q_i$ is congruent to
1 modulo a prime $\ell$, then $h_K$ has a tendency to be divisible by a higher
power of $\ell$. There are several ways to show results of this type. Cornell
and Rosen([3], [4]) showed this result using unramified $\ell$-extensions and
central extensions of $K$. There is another way to show similar results
using the group of cyclotomic units and its index in the full unit group
$\mathcal{O}_K^\times$ of $K$. It is carried out by Kučera ([9]) for $p = 2$ and compositum $K$
of quadratic fields and by Greither, Hacham and Kučera ([5]) for odd
prime $p$. In function field case, Bae and Jung ([1]) obtained some results
of $\ell$-rank of ideal class groups of real cyclotomic function fields following
Cornell and Rosen. In this paper, we show similar results following the
idea in [5] and compare our results with those in ([1]). Now we state our
result precisely.

Let $A = \mathbb{F}_q[T]$ be the ring of polynomials over a finite field $\mathbb{F}_q$ with
$q$ elements and $k = \mathbb{F}_q(T)$. Let $q = p^f$ with $p = \text{char}(k)$ and $f > 0$.
For each $M \in A$, one uses the Carlitz module to construct a field
extension $k_M^+$, called the $M$-th cyclotomic function field and its maximal
real subfield $k_M^+$. For a finite abelian extension $F$ of $k$ which is contained

Received December 7, 2001. Revised March 14, 2002.
2000 Mathematics Subject Classification: 11R58, 11R60.
Key words and phrases: function field, class number, cyclotomic unit.
in some cyclotomic function field, we call $M$ the conductor of $F$ if $k_M$ is the smallest cyclotomic function field which contains $F$. Also we call $F$ real if $F$ is contained in $k_M^+$ where $M$ is the conductor of $F$.

Let $\ell$ be a prime rational number with $(\ell, q - 1) = 1$. For $s \in \mathbb{Z}$, $s > 0$, we write $S = \{1, \ldots, s\}$. Let $Q_1, \ldots, Q_s$ be distinct monic irreducible polynomials in $A$. In addition, if $\ell \neq p$, we require that each $Q_i$ satisfies $q^{\deg(Q_i)} \equiv 1 \mod \ell$. We choose $e_1, \ldots, e_s \in \mathbb{Z}$ so that $e_i = 1$ (resp. $e_i \geq 2$) for $\ell \neq p$ (resp. $\ell = p$) for each $i \in S$. Let $K_i$ be any elementary abelian $\ell$-extension of $k$ in $k_{Q_i^{e_i}}$, for each $i \in S$ and $\delta_i$ be the $\ell$-rank of $G_i = \text{Gal}(K_i/k)$. Since $(\ell, q - 1) = 1$, each $K_i$ is real, i.e., $K_i \subseteq k_{Q_i^{e_i}}^+$. It is known ([1, Section 5]) that $\delta_i = 1$ if $\ell \neq p$ and $\delta_i \leq f \times \deg(Q_i) \times (e_i - 1 - [(e_i - 1)/p])$ if $\ell = p$.

Let $K$ be the compositum of all $K_i$, $i \in S$ and $G = \text{Gal}(K/k)$. Since $G \simeq \prod_{i=1}^s G_i$, $G$ is an elementary abelian $\ell$-group of rank $\delta = \sum_{i=1}^s \delta_i$. Let $\mathcal{O}_K$ be the integral closure of $A$ in $K$. Let $h_K$ be the ideal class number of $\mathcal{O}_K$. Our main result is the following theorem.

**Main Theorem.** With notations as above, the ideal class number $h_K$ is divisible by $\ell \prod_{i=1}^s (1 + \delta_i)^s \delta s - 1$.

Now we assume that $K_i$ is the maximal elementary abelian $\ell$-extension of $k$ in $k_{Q_i^{e_i}}$. Then $\delta_i$ equals to $f \times \deg(Q_i) \times (e_i - 1 - [(e_i - 1)/p])$ for $\ell = p$. In [1], Bae and Jung showed that $h_K$ is divisible by $\ell^{s(s-3)/2}$ (resp. $\ell^{s\sum_i \delta_i - s\sum_i \delta_i}$) for $\ell \neq p$ (resp. for $\ell = p$). For $\ell \neq p$, our **Main Theorem** says that $h_K$ is divisible by $\ell^{s^2 - s^3 - 1}$. Note that $2^s - s^3 - 1 > s(s - 3)/2$ for $s > 4$. For $\ell = p$, elementary calculations show that

$$
\prod_{i=1}^s (1 + \delta_i) \geq 1 + \sum_i \delta_i + \sum_{i<j} \delta_i \delta_j + \left( \sum_{i=3}^s \binom{s}{i}/s \right) \sum_i \delta_i,
$$

and so $\prod_{i=1}^s (1 + \delta_i) - s\delta - 1$ is greater than $\sum_{i<j} \delta_i \delta_j - \sum_i \delta_i$ for $s > 4$. Thus our result gives larger $\ell$-factor of $h_K$ than the result in [1] for $s > 4$. In [1], authors also give results for the case that $\ell$ divides $q - 1$. These cases corresponds to the case $p = 2$ in the number field case. Thus it will be interesting to consider the function field analogue of Kučera’s result ([9]).

2. **Cyclotomic units**

We keep all the notations of the preceding section. In this section, we give some basic facts of the cyclotomic function fields and cyclotomic
units which are needed in the proof of Main Theorem. Let \( k^{ac} \) be an algebraic closure of \( k \). Then \( k^{ac} \) becomes an \( \mathbb{A} \)-module (called Carlitz module) under the following action: For \( u \in k^{ac} \) and \( M \in \mathbb{A} \), define

\[
u^M = M(\varphi + \mu_T)(u),
\]

where the map \( \varphi \) is defined as \( \varphi(u) = u^q \) and \( \mu_T \) is defined as \( \mu_T(u) = Tu \). It is known that the set \( \Lambda_M \) of roots of \( u^M = 0 \) generates an abelian extension \( k(\Lambda_M) \) of \( k \), called the \( M \)-th cyclotomic function field and we denote it by \( k_M \) for simplicity. By a primitive \( M \)-th torsion point, we mean a generator of \( \Lambda_M \) as an \( \mathbb{A} \)-module. The following facts are basic in the cyclotomic function field theory.

**Proposition 2.1** ([8]).

(i) \( \text{Gal}(k_M/k) \cong (\mathbb{A}/M)^* \).

(ii) \( k_M^+ \) is the fixed field of \( F_q^* \) in \( k_M \), and it is the maximal subfield of \( k_M \), where \( \infty = (1/T) \) splits completely.

(iii) If \( (M, N) = 1 \), then \( k_M \) and \( k_N \) are linearly disjoint over \( k \).

(iv) If \( M = P^n \), a power of monic irreducible \( P \), then \( N_{k_M/k}(\lambda_M) = P \).

Here \( \lambda_M \) is a primitive \( M \)-torsion point.

Recall that the group \( D \) of cyclotomic numbers of \( K \) is defined as the subgroup of \( K^* \) generated by \( F_q^* \) and all elements \( N_{k_N/K}(\lambda_N^\sigma) \) with \( N, A \in \mathbb{A} \) where \( K_N = k_N \cap K \). Let \( C = D \cap \mathcal{O}_K^* \), called the group of cyclotomic units of \( K \) (cf. [7, Section 3]). For \( \emptyset \neq I \subset S \), we set \( M_I = \prod_{i \in I} Q_i^{e_i} \), \( \delta_I = \sum_{i \in I} \delta_i \), \( K_I \) the compositum of \( K_i, i \in I \) and \( x_I = N_{k_M/K}(\lambda_I) \), where \( \lambda_I \) is a fixed primitive \( M_I \)-th torsion point. It is known that \( D \) is generated by \( \mathbb{F}_q^* \cup \{ x_\sigma^\sigma : \sigma \in G, \emptyset \neq I \subset S \} \), and \( D \) (resp. \( C \)) has rank \( \ell^\delta + s - 1 \) (resp. \( \ell^\delta - 1 \)). The index of \( C \) in the full unit group \( \mathcal{O}_K^* \) is related to the ideal class number \( h_K \).

**Proposition 2.2** ([2], Corollary 3.11).

\[ [\mathcal{O}_K^* : C] = (q - 1)^{\ell^\delta - 1}h_K. \]

As the classical case, we have the following.

**Lemma 2.3.** Let \( N, P, Q \in \mathbb{A} \) with \( P \) monic irreducible, \( N = PQ \). If \( P \nmid Q \), we let \( \sigma = (P, k_Q/k)^{-1} \in \text{Gal}(k_Q/k) \). Then we have

\[
N_{k_N/k_Q}(\lambda_N) = \begin{cases} 
\lambda_N^P & \text{if } P \nmid Q , \\
(\lambda_N^P)^{(1-\sigma)} & \text{if } P \nmid Q, Q \notin \mathbb{F}_q^* .
\end{cases}
\]

Note that \( \lambda_N^P \) is also primitive \( Q \)-torsion point and so \( \lambda_N^P = \lambda_Q^\tau \) for some \( \tau \in \text{Gal}(k_Q/k) \).
Proof. First we note that

\[ (k_N : k_Q) = \begin{cases} \deg(P) & \text{if } P|Q, \\ \deg(P) - 1 & \text{if } P \nmid Q. \end{cases} \]

Let \( \mathcal{W} = \mathcal{W}(QA/NA) \) be a complete set of representatives of \( QA/NA \) consisting of monic polynomials. If \( P|Q \), then

\[ \text{Gal}(k_N/k_Q) \cong \{(1 + X) + NA \in (A/NA)^* : X \in \mathcal{W}\} \]

and so we have

\[ N_{k_N/k_Q}(\lambda_N) = \prod_{X \in \mathcal{W}} \lambda_N^{1+X} = \prod_{X \in \mathcal{W}} (\lambda_N + \lambda_N^X). \]

We claim that \( \Lambda_P = \{\lambda_N^X : X \in \mathcal{W}\} \). Clearly \( \lambda_N^X \neq \lambda_N^Y \) for any distinct \( X, Y \in \mathcal{W} \) and \( (\lambda_N^X)^P = 0 \). Since \( |\mathcal{W}| = |QA/NA| = |\mathcal{W}|/|P| = |\Lambda_P| \), we get the claim. Since

\[ u^P = \prod_{\lambda \in \Lambda_P} (u + \lambda) = \prod_{X \in \mathcal{W}} (u + \lambda_N^X), \]

we have

\[ \lambda_N^P = \prod_{X \in \mathcal{W}} (\lambda_N + \lambda_N^X) = N_{k_N/k_Q}(\lambda_N). \]

Now, suppose that \( P \nmid Q \). There exists \( X_0 \in QA \) such that \( X_0 \equiv -1 \) mod \( P \). Without loss of generality, we may assume that \( X_0 \in \mathcal{W} \). Then \( P|(X_0 + 1) \); so \( X_0 + 1 \) is not prime to \( N \). Hence we have

\[ \text{Gal}(k_N/k_Q) \cong \{(1 + X) + NA \in (A/NA)^* : X \in \mathcal{W}, X \neq X_0\} \]

and

\[ N_{k_N/k_Q}(\lambda_N) = \prod_{X \in \mathcal{W}} \frac{(\lambda_N + \lambda_N^X)}{\lambda_N + \lambda_N^{X_0}}. \]

Let \( 1 + X_0 = PB \). Since \( X_0 \in QA \), \( (P, k_Q/k)^{-1} = (B, k_Q/k) = \sigma \) and so

\[ \lambda_N + \lambda_N^{X_0} = \lambda_N^{PB} = (\lambda_N^P)^B = (\lambda_N^P)^{(B, k_Q/k)} = (\lambda_N^P)^\sigma. \]

Therefore, we get \( N_{k_N/k_Q}(\lambda_N) = (\lambda_N^P)^{1-\sigma}. \) \( \square \)

Let \( \sigma_1, \ldots, \sigma_{\delta_i} \) be the generators of \( \text{Gal}(K_S/K_{S-\{i\}}) \). For \( i \in S, 1 \leq j \leq \delta_i \), define \( N_{i,j} = 1 + \sigma_{ij} + \cdots + \sigma_{ij}^{\delta_i-1} \), the norm corresponding to the group \( \langle \sigma_{ij} \rangle \). For \( \emptyset \neq I \subset S \), let \( \bar{I} = \{i \in I, 1 \leq j \leq \delta_i\} \). For \( J \subset I \), we define

\[ x_{I,J} = x_J \prod_{(i,j) \in J} N_{i,j}. \]
For any subset $J$ of $I$, we say that $J$ satisfies the condition $(\ast)$ for $I$ if $|\{j : (i, j) \in J\}| < \delta_i$ for each $i \in I$. Note that, if $\ell \neq p$, then $J = \emptyset$ is the only one which satisfies $(\ast)$ and so $x_{I, J}$ is just $x_I$. For $\emptyset \neq I \subset S$, $J \subset \tilde{I}$, define
\[
S_{I, J} = \prod_{i \in I, 1 \leq j \leq \delta_i, (i, j) \in J} \sigma_{ij}^{a_{ij}} : 0 \leq a_{ij} \leq \ell - 2.
\]
Let $B = \{x_{\{i\}, \tilde{I}}^{a_{ij} - 1} : 1 \leq i \leq s\} \cup \{x_{I, J}^\sigma : \emptyset \neq I \subset S, J \subset \tilde{I}, J \text{satisfies}(\ast), \sigma \in S_{I, J}\}$.

**Proposition 2.4.** $B$ is a $\mathbb{Z}$-basis of $D/\mathbb{F}_q^\ast$.

**Proof.** First we calculate the cardinality of $B$. We have
\[
|B| = \sum_{\emptyset \neq I \subset S} \sum_{J \subset \tilde{I}, J \text{satisfies } (\ast)} (\ell - 1)^{|J|} + s.
\]
Then,
\[
\sum_{J \text{satisfies } (\ast)} (\ell - 1)^{|J|} = \sum_{J \subset \tilde{I}} (\ell - 1)^{|J|} - \sum_{i \in I} \sum_{J \subset \tilde{I}, (i) \subset J} (\ell - 1)^{|J|} + \sum_{I' \subset I} \mu(I', I)g(I') = \ell^\delta - g(S).
\]
where $\mu(I', I) = (-1)^{|I'| - |I|}$, the Möbius function on the subsets of $S$ and $g(I') = \sum_{J \subset \tilde{I}} (\ell - 1)^{|J|} = \ell^\delta$. So, by the Möbius inversion formula, we have
\[
\ell^\delta = g(S) = \sum_{I \subset S} \sum_{J \subset \tilde{I}, J \text{satisfies } (\ast)} (\ell - 1)^{|J|}.
\]
Thus, $|B| = \ell^\delta + s - 1$. Therefore, the cardinality of $B$ is equal to the $\mathbb{Z}$-rank of $D$. It remains to show that $B$ generate $D$ modulo $\mathbb{F}_q^\ast$. The remaining part of the proof is so directly analogous to Greither, Hachami and Kučera’s proof in the number field case that the reader should refer to ([5, Proposition 1.2]).

For $\ell \neq p$, since $J = \emptyset$ is the only subset of $\tilde{I}$ which satisfies $(\ast)$, we have
\[
B = \{x_{\{i\}}^\sigma : \emptyset \neq I \subset S, \sigma \in S_I\} \cup \{x_{\{i\}}^{a_{ij} - 1} : i = 1, \ldots, s\},
\]
where $S_I = \{ \prod_{i \in I} a_i^{\sigma_i} : 0 \leq a_i \leq \ell - 2 \}$.

### 3. Proof of the main theorem

For $\emptyset \neq I \subset S$ and $J \subset \tilde{I}$, we define

$$y_{I,J} = x_{I,J}^{e_{I,J}} \text{ with } e_{I,J} = \prod_{i \in I} \prod_{1 \leq j \leq \delta_i, (i,j) \notin J} (1 - \sigma_{ij})^{\ell - 2}.$$  

Let $L$ be the subgroup of $k^*$ generated by $Q_1, \ldots, Q_s$. For $J \subset \tilde{I}$, we call $J$ satisfy the condition $(**)\text{ for } I$ if, for each $i \in I$,

$$\left| \{ j \in \{1, \ldots, \delta_i \} : (i,j) \in J \} \right| = \delta_i - 1.$$  

Clearly, the condition $(**)$ is a sufficient condition for the condition $(*)$ and so, if $\ell \neq p$, only $J = \emptyset$ satisfies the condition $(**)$. We define the subgroup $U$ of $C$ generated by $\{ y_{I,J}^{\sigma} : \emptyset \neq I \subset S, J \subset \tilde{I}, J \text{ satisfies } (**), \sigma \in G \}$.

**Proposition 3.1.** For any $u \in U$ and $\sigma \in G$, there are $\psi_u(\sigma) \in L$ and $f_u(\sigma) \in D$ such that $u^{1-\sigma} = \psi_u(\sigma)f_u(\sigma)^\ell$ and $\psi_u(\sigma)$ is uniquely determined modulo $L^\ell$.

**Proof.** Since $(\ell, q - 1) = 1$, $K^\ell \cap L = L^\ell$. From this, the uniqueness of $\psi_u(\sigma)$ modulo $L^\ell$ follows. As in [5], it suffices to prove the proposition for $u = y_{I,J}$ with $\emptyset \neq I \subset S$, $J \subset \tilde{I}$, $J$ satisfies $(**)$ and $\sigma = \sigma_{ij}$ with $i \in I$, $(i,j) \notin J$.

We use induction on $|I|$. Suppose that the proposition is true for all $u$ generated by $y_{I',J'}$ with $I' \subsetneq I$ and $J' \subsetneq \tilde{I}$ with $J'$ satisfying $(**)$, note that $(1 - \sigma_{ij})^{1-1}(1 - \sigma_{ij}) = (1 - \sigma_{ij})^{\ell - 1} = N_{i,j} + \ell \alpha$ for some $\alpha \in Z[\sigma_{ij}]$.

Thus

$$y_{I,J}^{1-\sigma_{ij}} = x_{I,J}^{N_{i,j} + \ell \alpha} \prod_{i' \in I - \{i\}} \prod_{1 \leq j' \leq \delta_i, (i',j') \notin J} (1 - \sigma_{ij'})^{\ell - 2}$$

for some $w \in D$. Note that $x_{I,J}^{N_{i,j}} = x_{I,J - \{i\}}^{\prod_{1 \leq j \leq \delta_i} N_{i,j}}$ and that $\prod_{1 \leq j \leq \delta_i} N_{i,j}$ is the norm corresponding to $\text{Gal}(K_I/K_{I-\{i\}})$.

If $I - \{i\} \neq \emptyset$, by Lemma 2.3, we have $x_{I,J}^{N_{i,j}} = (x_{I,\tilde{J}}^{1-})^r$ where $\tau, \tau' \in G$ with $\tau = (Q_i, K_{I-\{i\}}/k)$. Note that $J - \{i\} \subset I - \{i\}$ and satisfy $(**)$ for $I - \{i\}$. From the induction hypothesis, we have that

$$y_{I,J}^{1-\sigma_{ij}} = (y_{I,J - \{i\}})^{r'} w^\ell$$
can be written in the desired form and so it remains to prove the case $I = \{i\}$. But when $I = \{i\}$, we have

$$x_{i,j}^{N_{i,j}} = x_i^{\prod_{1 \leq j \leq s_i} N_{i,j}} = N_{k_i}^{q_i^{s_i}} k_i^{\ell q_i^{s_i}} = Q_i \in L.$$ 

It finishes the proof of the proposition.

From the proposition 3.1, it is obvious that for each $u \in U$, $\psi_u : G \to L/L^\ell$ is a homomorphism. Now we define a map $\Psi : U \to \text{Hom}(G, L/L^\ell)$ defined by $\Psi(u) = \psi_u$. Then $\Psi$ is a homomorphism. So we consider $u \in \ker(\Psi)$. From proposition 3.1, we have $u^{1-\sigma} = f_u(\sigma)^\ell$ with $f_u(\sigma) \in D$ for all $\sigma \in G$. Since

$$u^{1-\sigma} = u^{1-\sigma} u^\sigma(1-\tau) f_u(\sigma)^\ell = (f_u(\sigma) f_u(\tau))^\ell,$$

we see that $f_u : G \to D$ is a 1-cocycle for $u \in \ker(\Psi)$. Therefore, we have the following proposition as the classical case ([5, Proposition 2.5]).

**Proposition 3.2.** For any $u \in \ker(\Psi)$, there exists $\alpha(u) \in K^*$ and $\varphi(u) \in L$ such that

$$u = \varphi(u) \alpha(u)^\ell.$$

Note that $\varphi(u)$ is unique modulo $L^\ell$, and so $\varphi : \ker(\Psi) \to L/L^\ell$ is a homomorphism. We denote $\ker(\varphi)$ by $N$. From Proposition 3.2, any element of $N$ is the $\ell$-th power in $K$. Since $N \subset U \subset O_K$, it becomes the $\ell$-th power in $O_K^*$ and so $N \subset C \cap (O_K^*)^\ell$.

As Greither, Hachami and Kučera ([5, Lemma 2.7-2.8]), we have

**Lemma 3.3.** (i) $[U : N]$ divides $\ell^{s_1} | \text{Im}(\Psi)|$ and $|\text{Im}(\Psi)|$ divides $\ell^{s_2}$.

(ii) $\{y_{i,j} : \emptyset \neq I \subset S \text{ and } J \subset \overline{I}, J \text{ satisfies (**)} \} \cup \{y_{i,j}^{\sigma_i} : i = 1, \ldots, s \text{ and } J = \{i\} \setminus \{(i, 1)\} \}$ is free over $\mathbb{Z}/\ell\mathbb{Z}$ in the vector space $C/C^\ell$.

Now we are ready to prove **Main Theorem**.

**Proof of the main theorem.** By Proposition 2.2 and Lemma 3.3 (i), it suffices to prove that $\ell^{s_1} | (1+\delta_i)^{-t-1} \text{ divides } [O_K^* : C]$, where $|\text{Im}(\Psi)| = \ell^\delta, t \geq 0$. We denote $O_K^*$ by $E$ for simplicity. We consider the short exact sequence

$$0 \to C/C \cap E^\ell \cong E^\ell C/E^\ell \to E/E^\ell \to E/E^\ell C \to 0.$$

Since $E/E^\ell$ is $(\mathbb{Z}/\ell\mathbb{Z})$-vector space of dimension $[K : k] - 1 = \ell^\delta - 1$, we have

$$\text{rk}_\ell(E/C) = \dim(E/E^\ell C) = \ell^\delta - 1 - \dim(C/C \cap E^\ell),$$

(3.1)
where \( \text{rk}_\ell(E/C) \) denotes \( \ell \)-rank of \( E/C \) and \( \dim \) denotes \( \dim_{\mathbb{Q}/\mathbb{Z}} \) for simplicity. We denote the image of \( N \) and \( U \) in \( C/C^\ell \) by \( \bar{N} \) and \( \bar{U} \), respectively. Since \( N \subset C \cap E^\ell \),

\[
\text{dim}(C/C \cap E^\ell) \leq \text{dim}((C/C^\ell)/\bar{N}) = \ell^t - 1 - \text{dim}(\bar{N}).
\]

From (3.1) and (3.2), we get

\[
\text{rk}_\ell(E/C) \geq \dim \bar{N}.
\]

But from Lemma 3.3 (i), (ii), we have

\[
\text{dim} \bar{U} \geq \prod_{i=1}^{s}(1 + \delta_i) - 1 + s \quad \text{and} \quad \text{dim} \bar{U}/N \leq s + t.
\]

Therefore,

\[
\text{rk}_\ell(E/C) \geq \dim \bar{N} \geq \prod_{i=1}^{s}(1 + \delta_i) - t - 1,
\]

which completes the proof of the theorem. \( \square \)

**Acknowledgement.** The authors thank the referee for his careful reading of the manuscript and suggestions.

**References**


Cyclotomic units and divisibility of the class number

Department of Mathematics
KAIST
Daejon 305-701, Korea
E-mail: jaehyun@mathx.kaist.ac.kr
hyjung@mathx.kaist.ac.kr