Calculation formula and divisibility for relative class numbers of abelian function fields

Yusheng Zhao *, Lianrong Ma, Xianke Zhang

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

ARTICLE INFO

Article history:
Received 15 September 2008
Revised 2 April 2009
Available online 3 July 2009
Communicated by David Goss

MSC:
11R29
11R60

Keywords:
Carlitz-module
Cyclotomic function field
Class number
Character

ABSTRACT

In this paper abelian function fields are restricted to the subfields of cyclotomic function fields. For any abelian function field $K/k$ with conductor an irreducible polynomial over a finite field of odd characteristic, we give a calculating formula of the relative divisor class number $h_K$ of $K$. And using the given calculating formula we obtain a criterion for checking whether or not the relative divisor class number is divisible by the characteristic of $k$.

Let $\mathbb{F}_q$ be the finite field with $q$ elements and $q$ be a power of an odd prime number. Let $k = \mathbb{F}_q(T)$ be the rational function field of the indeterminate $T$ over $\mathbb{F}_q$. Denote by $R = \mathbb{F}_q[T]$ the polynomials of $T$ over $\mathbb{F}_q$, which is a ring called the integer ring of $k$. Fix an algebraic closure of $k$ and denote it by $k^{ac}$. Note that $k^{ac}$ has two special $\mathbb{F}_q$-automorphisms:

$$\tau, \sigma : k^{ac} \rightarrow k^{ac},$$

$$\tau(\alpha) = \alpha T \quad \text{(multiply by } T),$$

$$\sigma(\alpha) = \alpha^q \quad \text{(Frobenius)}$$

© 2009 Elsevier Inc. All rights reserved.
(here $\alpha \in k^{ac}$). Now define the action of any polynomial $f(T) \in R$ on $\alpha \in k^{ac}$ by

$$\alpha^{f(T)} = f(\tau + \sigma)(\alpha).$$

Via this action, $k^{ac}$ becomes an $R$-module, named Carlitz-module.

For any monic polynomial $M = M(T) \in R$, put

$$\Lambda_M = \{\alpha \in k^{ac}; \alpha^M = 0\},$$

Then $\Lambda_M$ is a submodule of $k^{ac}$ and there is an $R$-module isomorphism:

$$\Lambda_M \cong R/(M), \quad \lambda^N \mapsto N \pmod{M},$$

where $\lambda$ is a generator of the cyclic module $\Lambda_M$ (i.e., a primitive $M$-torsion element).

Consider the function field generated by $\Lambda_M$ (the $M$-torsion elements of the Carlitz-module $k^{ac}$) over the rational function field $k$, that is

$$L = k(\Lambda_M),$$

which is called a cyclotomic function field with conductor $M$. The Galois group of the cyclotomic function field $L/k$, denoted by $G = \text{Gal}(L/k)$, is naturally isomorphism to $(R/(M))^\times$:

$$\text{Gal}(L/k) \to (R/(M))^\times, \quad \sigma_N \mapsto N \pmod{M} \left(\text{where } \sigma_N(\lambda) = \lambda^N\right)$$

(for $N \in R$, $(N, M) = 1$, $\lambda \in L$). Thus usually we identify $G$ and $(R/(M))^\times$ and write $G = \text{Gal}(L/k) = (R/(M))^\times$.

The fixed subfield of $L$ by $\mathbb{F}_q^\times$, denoted by $L^+ = k(\lambda^{q-1})$, is called the maximal real subfield of $L$. The characters $\chi$ of $G = (R/(M))^\times$ are actually the Dirichlet-characters of $R$ modulo $M$. If $\chi([\mathbb{F}_q^\times]) = 1$, then $\chi$ is said to be real; otherwise, $\chi$ is non-real. In this paper, we restrict an abelian function field to a subfield of a cyclotomic function field $L = k(\Lambda_M)$ (see Ref. [2]).

In [5], to calculate the relative divisor class numbers $h^{-}(k(\Lambda_P))$ of cyclotomic function fields with irreducible conductors, Rosen gave a formula using determinants. From the formula, he got an upper bound of the relative class number and obtained a criterion for determining whether or not the relative divisor class number is divisible by the characteristic. In [1], Bae and Kang obtained the upper bound via different method and established a determinant formula computing the relative class number of $h^{-}(k(\Lambda_P))$. In [4], Ma and Zhang gave an upper bound and a computing formula for any abelian function field with irreducible conductor. But, like in [1], the calculating formulae are quite complicated because it is needed to get the inverses of the polynomials modulo the conductor. In this paper, we give a simpler calculating formula for the relative divisor class numbers of abelian function fields and study their divisibilities using the calculating formula.

In this paper, we always assume $L = L(\Lambda_P)$, where $M = P \in R$ is an irreducible polynomial of degree $d \geq 1$. Thus the Galois group $G = \text{Gal}(L/k) = (R/(P))^\times$ is a cyclic group with order $q^d - 1$. Let $\omega$ be a generator of $G$.

For any integer $m|(q^d - 1)$, the cyclotomic function field $L = k(\Lambda_P)$ has a unique subfield $K = K_m$ with degree $[K:k] = m$. Obviously its Galois group is

$$G_K = \text{Gal}(K/k) = \left((R/(P))^\times\right)/\left((R/(P))^\times\right)^m.$$
The character group of \( G_K \), denoted by \( \hat{G}_K \) or \( \hat{K} \), consists of those Dirichlet-characters \( \chi \) modulo \( P \) satisfying \( \chi^m = 1 \). A character \( \chi \in \hat{G}_K \) is real if and only if
\[
\chi(\omega) \left( \frac{q^d - 1}{q - 1} \right) = 1.
\]
The function field \( K^+ = K \cap L^+ \) is said to be the maximal real subfield of \( K \). Denote the class numbers of zero-degree-divisors of \( K \) and \( K^+ \) respectively by \( h_m \) and \( h^+_m \). The ratio
\[
h^-_m = \frac{h_m}{h^+_m}
\]
is called the relative divisor class number of \( K \), which is an integer. The following result is well-known for the relative divisor class number (e.g. see [2]):

**Lemma 1.** Let \( \hat{G}_K^− \) be the non-real characters in \( \hat{G}_K \), then
\[
h^-_m = \prod_{\chi \in \hat{G}_K^−} \sum_{\text{monic } A \in \mathbb{R} \text{ deg } A < d} \chi(A).
\]

Denote \( r = \frac{q^d - 1}{q - 1} \). Furthermore, assume \( r \mid m \) and denote \( c = \frac{m}{r} \). For any polynomial \( A = a_1T^d + \cdots + a_1T + a_0 \), \( a_1 \neq 0 \), denote \( \text{sgn}(A) = a_5 \). And let \( \text{sgn}_P(A) = \text{sgn}(B) \), where polynomial \( B \equiv A \pmod{P} \), \( \text{deg}(B) < d \). Consider the set of polynomials
\[
\{A_1, A_2, \ldots, A_r\} = \{A \mid \text{deg}(A) < d, \text{sgn}(A) = 1\}.
\]

Define the \( r \times r \) matrix \( C \) as:
\[
C = (\text{sgn}_P(A_i A_j)).
\]
Fix a generator \( \psi \) of the character group \( \hat{F}_q^\times \). For \( t = 1, 2, \ldots, c - 1 \), define the matrix
\[
S^{(t)} = \psi^t \left( \frac{q^d - 1}{m} \right) C.
\]
Here, the action of a character on the matrix \( C \) is via acting on every elements of \( C \). We obtain the following formula for calculating the relative divisor class number.

**Theorem 1.** Suppose that \( K = K_m \) is an abelian function field of degree \( m \). Let \( r \), \( c \) and \( S^{(t)} \) be as in Lemma 1. Assume that \( r \mid m \). Then the relative divisor class number of \( K \) is the product of the determinants \( \det S^{(t)} \), that is
\[
h^-_m = \prod_{t=1}^{c-1} \det S^{(t)}.
\]

From this calculating formula, we can get the following result about the divisibility of the class number:

**Theorem 2.** Let \( K \) be the abelian function field defined in Theorem 1. Let
\[
C^{(t)} = \left( (\text{sgn}_P(A_i A_j)) \frac{q^d - 1}{m} \right)^{t-1}.
\]
Then the relative divisor class number $h_m^- \mid$ is divisible by the characteristic $p$ of $K$ if and only if:

$$\exists t \in \{1, \ldots, c-1\} \text{ such that } \det C(t) = 0 \text{ (in the field } \mathbb{F}_q) .$$

**Example 1.** Let $q = 5, P = T^2 + 2$ is an irreducible polynomial in $\mathbb{F}_5[T]$. Consider the cyclotomic function field $K = k(\Lambda_P)$ with conductor $P$. Let $K_m = K_{12}$ be its subfield of degree $m = 12$. Then $r | m, (q^d - 1)/m = 2, c = m/r = 12/6 = 2$. Thus

$$\{A_1 = 1, A_2 = T, A_3 = T + 1, A_4 = T + 2, A_5 = T + 3, A_6 = T + 4\}$$

are all the monic polynomials of degree less than 2. Thus we obtain the matrices

$$(A_i A_j) = \begin{bmatrix}
1 & T & T + 1 & T + 2 & T + 3 & T + 4 \\
T & 3 & T + 3 & 2T + 3 & 3T + 3 & 4T + 3 \\
T + 1 & T + 3 & 2T + 4 & 3T + 1 & 2 \\
T + 2 & 2T + 3 & 3T + 1 & 4T + 2 & 4 \\
T + 3 & 3T + 3 & 4T + 1 & 4 & T + 2 \\
T + 4 & 4T + 3 & 2 & T + 1 & 2T & 3T + 4
\end{bmatrix} ,$$

$$C = \text{sgn}_P (A_i A_j) = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 3 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 2 \\
1 & 2 & 3 & 4 & 4 & 1 \\
1 & 3 & 4 & 4 & 1 & 2 \\
1 & 4 & 2 & 1 & 2 & 3
\end{bmatrix} .$$

Note that 2 is a generator of the cyclic group $\mathbb{F}_5^\times$. Let $\psi(2) = i$, then $\psi$ is a generator of $\mathbb{F}_5^\times$, and $\psi(4) = -1, \psi(3) = -i$. So we have $\psi^2(2) = -1, \psi^2(3) = -1, \psi^2(4) = 1$. Thus we obtain the matrix

$$S^{(1)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1
\end{bmatrix} .$$

Finally we get the relative divisor class number of $K_{12}$:

$$h_{12}^- = | \det S^{(1)} | = \begin{vmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & 1 \\
1 & -1 & -1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1
\end{vmatrix} = |160| = 2^5 \cdot 5 .$$

$$\det C^{(1)} = \begin{vmatrix}
1 & 1 & 1 & 1 & 1 \\
1 & 4 & 1 & 4 & 4 \\
1 & 1 & 4 & 1 & 4 \\
1 & 4 & 4 & 1 & 1 \\
1 & 4 & 1 & 1 & 4 \\
1 & 1 & 4 & 1 & 4
\end{vmatrix} = 1215 , \text{ thus } 5 | h_{12}^- .$$
Example 2. Let \( q = 7, \ P = T^2 + 1 \) is irreducible. \( d = 2, \ q^d - 1 = 48, \ q - 1 = 6, \ r = 8. \) Consider the cyclotomic function field \( L = k(A_2) \) with conductor \( P. \) Let \( K_m = K_{24} \) be its subfield of degree \( m = 24. \) Then \( r|m, \ \frac{q^d - 1}{m} = 2, \ c = m/r = 24/8 = 3. \) Thus \( A_1 = 1, \ A_2 = T, \ A_3 = T + 1, \ A_4 = T + 2, \ A_5 = T + 3, \ A_6 = T + 4, \ A_7 = T + 5, \ A_8 = T + 6 \) are all the monic polynomials of degree less than 2. Thus we obtain the matrices

\[
(A_iA_j) = \begin{bmatrix}
1 & T & T + 1 & T + 2 & T + 3 & T + 4 & T + 5 & T + 6 \\
T & 6 & T + 6 & 2T + 6 & 3T + 6 & 4T + 6 & 5T + 6 & 6T + 6 \\
T + 1 & T + 6 & 2T & 3T + 1 & 4T + 2 & 5T + 3 & 6T + 4 & 5 \\
T + 2 & 2T + 6 & 3T + 1 & 4T + 3 & 5T + 5 & 6T + 2 & T + 4 \\
T + 3 & 3T + 6 & 4T + 2 & 5T + 5 & 6T + 1 & 4 & T & 2T + 3 \\
T + 4 & 4T + 6 & 5T + 3 & 6T + 4 & T + 1 & 2T + 5 & 3T + 2 \\
T + 5 & 5T + 6 & 6T + 4 & 2 & T & 3T + 5 & 3T + 3 & 4T + 1 \\
T + 6 & 6T + 6 & 5 & T + 4 & 2T + 3 & 3T + 2 & 4T + 1 & 5T \\
\end{bmatrix}
\]

\[
C = \text{sgn}_P (A_iA_j) = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 6 & 1 & 2 & 3 & 4 & 5 & 6 \\
1 & 1 & 2 & 3 & 4 & 5 & 6 & 5 \\
1 & 2 & 3 & 4 & 5 & 6 & 2 & 1 \\
1 & 3 & 4 & 5 & 6 & 4 & 1 & 2 \\
1 & 4 & 5 & 6 & 4 & 1 & 2 & 3 \\
1 & 5 & 6 & 2 & 1 & 2 & 3 & 4 \\
1 & 6 & 5 & 1 & 2 & 3 & 4 & 5 \\
\end{bmatrix}.
\]

Note that 3 is a generator of the cyclic group \( \mathbb{F}_7^*, \) Take \( \psi(3) = a = e^{\frac{2\pi i}{7}}, \) then \( \psi \) is a generator of \( \mathbb{F}_7^* \) and \( \psi(2) = a^2, \ \psi(4) = a^4, \ \psi(5) = a^5, \ \psi(6) = a^3. \) Thus we have

\[
\psi^2(2) = a^4, \quad \psi^2(3) = a^2, \quad \psi^2(4) = a^2, \quad \psi^2(5) = a^4, \quad \psi^2(6) = 1; \\
\psi^4(2) = a^2, \quad \psi^4(3) = a^4, \quad \psi^4(4) = a^4, \quad \psi^4(5) = a^2, \quad \psi^4(6) = 1.
\]

So we obtain the matrices

\[
S^{(1)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & a^4 & a^2 & a^2 & a^4 & 1 & 1 \\
1 & a^4 & a^2 & a^2 & a^2 & a^4 & 1 & a^4 \\
1 & a^2 & a^2 & a^4 & 1 & a^2 & 1 & a^4 \\
1 & a^2 & a^4 & 1 & a^2 & 1 & a^4 & a^2 \\
1 & a^4 & 1 & a^4 & 1 & a^4 & 1 & a^4 \\
1 & 1 & a^4 & 1 & a^4 & a^2 & a^2 & a^4 \\
\end{bmatrix}, \quad S^{(2)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & a^2 & a^4 & a^4 & a^2 & 1 & 1 \\
1 & a^2 & a^4 & a^4 & a^2 & 1 & a^2 & 1 \\
1 & a^4 & a^4 & a^4 & a^2 & 1 & a^2 & 1 \\
1 & a^4 & a^2 & 1 & a^2 & 1 & a^4 & a^4 \\
1 & a^4 & a^2 & 1 & a^2 & 1 & a^4 & a^4 \\
1 & a^4 & a^2 & 1 & a^2 & 1 & a^4 & a^4 \\
1 & a^4 & a^2 & 1 & a^2 & 1 & a^4 & a^4 \\
\end{bmatrix}.
\]

The relative divisor class number is then obtained.

\[
h_{24} = |\det S^{(1)} \det S^{(2)}| = \left| (-1728 + 1728e^{-\frac{2\pi i}{7}})(-1728 + 1728e^{\frac{2\pi i}{7}}) \right| = 8957952 = 2^{12}3^7.
\]
\[
C^{(1)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 4 & 2 & 2 & 4 & 1 \\
1 & 1 & 4 & 2 & 2 & 4 & 1 \\
1 & 4 & 2 & 2 & 4 & 1 & 4 \\
1 & 2 & 2 & 4 & 1 & 2 & 1 \\
1 & 2 & 4 & 1 & 2 & 1 & 4 \\
1 & 4 & 1 & 4 & 1 & 4 & 2 \\
1 & 1 & 4 & 1 & 4 & 2 & 2 
\end{bmatrix}, \quad
C^{(2)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 2 & 4 & 4 & 2 & 1 \\
1 & 1 & 2 & 4 & 4 & 2 & 1 \\
1 & 2 & 4 & 4 & 2 & 1 & 2 \\
1 & 4 & 4 & 2 & 1 & 4 & 1 \\
1 & 4 & 2 & 1 & 4 & 1 & 2 \\
1 & 2 & 1 & 2 & 1 & 2 & 4 \\
1 & 1 & 2 & 1 & 2 & 4 & 2 
\end{bmatrix},
\]

\[\det C^{(1)} = -906, \quad \det C^{(2)} = -2542, \quad 7 \nmid 906, \quad 7 \nmid 2542, \quad \text{thus } 7 \nmid h^{-24}.\]

**Proof of Theorem 1.** Let \( \chi_0 \) be a generator of the cyclic group \( \hat{G} \), \( \lambda = \chi_0^{\frac{d-1}{m}} \). Then \( \hat{G}_K = \{ \lambda^0, \lambda^1, \ldots, \lambda^{m-1} \} \). \( \lambda^1 \) is a real character if and only if \((q - 1)^{\frac{d-1}{m}}t\), i.e., \((q - 1)^{\frac{d-1}{m}}rt\). It means that \( m \mid rt \), i.e., \( c \mid t \).

Assume, without loss of generality, \( \chi_0 \mid \mathbb{F}_q = \psi \). Then \( \lambda \mid \mathbb{F}_q = \psi^{\frac{d-1}{m}t} \). From Lemma 1 we know that

\[ h_m^{-} = \prod_{t=1}^{c-1} h(t), \]

where

\[ h(t) = \prod_{i=0}^{r-1} \sum_{A \in \mathbb{R} \text{monic} \deg A < d} \lambda^{ic+t} (A). \]

It is easy to see that for every \( i, \lambda^{ic+t} \mid \mathbb{F}_q = \lambda^t \mid \mathbb{F}_q = \psi^{\frac{d-1}{m}t} \). And, in addition, \( \lambda^{ic+t} \) \((0 \leq i \leq r - 1) \) are all the characters in \( \hat{G}_K^- \) whose restrictions on \( \mathbb{F}_q \) are \( \psi^{\frac{d-1}{m}t} \). Then we can calculate \( h(t) \). Denote \( \tilde{\psi}(A) = \psi((\text{sgn}_p(A))^{-1}) \).

\[ h(t) = \prod_{i=0}^{r-1} \sum_{A \in \mathbb{R} \text{monic} \deg A < d} \lambda^{ic} (A) \lambda^t (A) = \prod_{i=0}^{r-1} \sum_{A \in \mathbb{R} \text{monic} \deg A < d} \lambda^{ic} (A) \lambda^t (A) \tilde{\psi}^{\frac{d-1}{m}t} (A). \]

The function \( \lambda^t (A) \tilde{\psi}^{\frac{d-1}{m}t} (A) \) is unchanged if we replace \( A \) with a multiple \( \alpha A \) \((\alpha \in \mathbb{F}_q^*) \) or with a polynomial \( A + BP \) congruent to \( A \). In addition, \( \lambda^{ic} \) \((i = 0, \ldots, r - 1) \) are exactly all the characters of the group \( \hat{G} = (\mathbb{R} / (P))^x / \mathbb{F}_q^x \). Thus we have

\[ h(t) = \prod_{\chi \in \hat{G}} \sum_{A \in \hat{G}} \chi(A) (\lambda^t (A) \tilde{\psi}^{\frac{d-1}{m}t} (A)). \]

Applying the Dedekind determinant formula (see [3]) we obtain

\[ h^{(t)} = \det(\lambda^t (B^{-1} A) \tilde{\psi}^{\frac{d-1}{m}t} (B^{-1} A)). \]
where \( A, B \) vary over the elements of the group \( \tilde{G} = (R/(P))^{\times} / \mathbb{F}_{q}^{\times} \). Replacing \( B^{-1} \) by \( B \) merely permutes the rows of the matrix, and so

\[
h(t) = \pm \det(\lambda^t(BA)\psi \frac{q^d-1}{m} t(AB)) = \pm \det(\lambda^t(B)\lambda^t(A) \psi \frac{q^d-1}{m} t(AB)).
\]

By the properties of determinants, it follows that

\[
h(t) = \pm \lambda^t \left( \prod_{A \in \tilde{G}} A \right)^2 \det(\psi \frac{q^d-1}{m} t(AB)) = \pm \det(\psi \frac{q^d-1}{m} t(AB)).
\]

It is known that if \( \psi \) is a generator of \( \hat{F}^{\times} \) then so is \( \psi^{-1} \). \( A, B \) run through \( \tilde{G} = (R/(P))^{\times} / \mathbb{F}_{q}^{\times} \) is the same as they vary over all the monic polynomials of degree less than \( d \). Thus Theorem 1 has been proved. \( \square \)

**Proof of Theorem 2.** Consider the elements of \( C^{(t)} \) in \( \mathbb{F}_q \). Let \( \zeta \) be a primitive \( (q^d-1) \)-th root of unity. Denote \( E = \mathbb{Q}(\zeta) \). Let \( \mathcal{O} \) be the ring of integers of \( E \). \( E \) is unramified at all primes above \( p \) because \( p \nmid q^d-1 \). Denote a prime above \( p \) as \( \wp \). Since the minimal \( f \) such that \( p^f \equiv 1 \pmod{q^d-1} \) satisfies \( p^f = q^d \), the residue class field \( \mathcal{O}/\wp \) consists of \( q^d \) elements. So \( \mathcal{O}/\wp \) is isomorphic to the field \( R/(P) \). Let \( \rho : \mathcal{O}/\wp \to R/(P) \) be an isomorphism and \( \gamma : \mathcal{O} \to \mathcal{O}/\wp \) be the reduction modulo \( \wp \) on \( \mathcal{O} \). Acting the homomorphism \( \rho \circ \gamma \) to both sides of the formula obtained in Theorem 1 we find

\[
p | h_m \iff \exists t \in \{1, \ldots, c-1 \} \text{ such that } \rho \circ \gamma (\det S^{(t)}) = 0.
\]

For a primitive character \( \psi \) of \( \mathbb{F}_q^{\times} \), the homomorphism \( \rho \circ \gamma \circ \psi \) is a mapping of \( \mathbb{F}_q^{\times} \) to itself. And, we can choose a suitable \( \rho \) to make \( \rho \circ \gamma \circ \psi \) an identity map. Acting the homomorphism \( \rho \circ \gamma \) on \( S^{(t)} \) we obtain

\[
\rho \circ \gamma (\det S^{(t)}) = \rho \circ \gamma (\pm \det \psi^{t(q^d-1)/m} \text{sgn}_P(A_iA_j))
\]

\[
= \pm \det(\rho \circ \gamma \circ \psi^{t(q^d-1)/m} \text{sgn}_P(A_iA_j)) = \pm \det(\text{sgn}_P(A_iA_j)^{t(q^d-1)/m}).
\]

The proof of Theorem 2 is completed. \( \square \)

**References**