GALOIS GROUPS AND GENERA OF A KIND OF QUASI-CYCLOTOMIC FUNCTION FIELDS

MIN SHA AND LINSHENG YIN

Abstract. We call a \((q-1)\)-th Kummer extension of a cyclotomic function field a quasi-cyclotomic function field if it is Galois, but non-abelian, over the rational function field with the constant field of \(q\) elements. In this paper, we determine the structure of the Galois groups of a kind of quasi-cyclotomic function fields over the base field. We also give the genus formulae of them.

1. Introduction

We call a \((q-1)\)-th Kummer extension of a cyclotomic function field a quasi-cyclotomic function field if it is Galois, but non-abelian, over the rational function field \(k = \mathbb{F}_q(T)\). A large kind of such fields are described explicitly in [4] following the works in [1] and in [2]. In this paper, we describe the Galois groups of this kind of quasi-cyclotomic function fields by generators and relations following the method in [7] by using the results in [2] and [4]. We also give the genus formulae of them.

Now we recall the constructions of the quasi-cyclotomic function fields in [4]. Let \(\mathbb{F}_q = \mathbb{F}_q((1/T))\) be the rational function field over the finite field \(\mathbb{F}_q\) of \(q\) elements. In this paper we always assume the characteristic of \(k\) is an odd prime number \(p\).

Put \(A = \mathbb{F}_q[T]\). Let \(\Omega\) be the completion of the algebraic closure of the completion \(\mathbb{F}_q((1/T))\) of \(k\) at the place \(1/T\). Let \(k^{ac}\) be the algebraic closure of \(k\) in \(\Omega\). Let \(k^{ab}\) be the maximal abelian extension of \(k\) in \(k^{ac}\).

Let \(\bar{\pi} \in \Omega\) be the period of the Carlitz module, namely the lattice \(\bar{\pi}A\) of rank one corresponds to the Carlitz module, \(e_C\) the Carlitz exponential function defined by

\[ e_C(x) = x \prod_{0 \neq u \in \bar{\pi}A} (1 - \frac{x}{u}) \], \quad x \in \Omega. 

For \(A \in \mathbb{F}_q((1/T))\), let \(\{A\}\) be the representation in \((\mathbb{F}_q((1/T)) \setminus \mathbb{F}_q[T]) \cup \{0\}\) of \(A\) modulo \(\bar{\pi}A\), we define

\[ \sin(A) = \sqrt[-s]{-1} \cdot e_C(\bar{\pi}\{A\}/\text{sgn}\{\{A\}\}) \]

where \(\text{sgn}\) is the sign function on \(\mathbb{F}_q((1/T))\).

Let \(\mathcal{A}\) be the free abelian group generated by the symbols \(\{A\} \in k/\bar{\pi}A\). Define two homomorphisms

\[ e, \sin: \mathcal{A} \to k^{ab} \]

2010 Mathematics Subject Classification. Primary 11R58; Secondary 11R32, 11R60.

Key words and phrases. quasi-cyclotomic function field, Galois group, genus.

This work was supported by NSFC Project No.10871107.
such that $e([A]) = e_C(\pi_A)$ and $\sin[A] = \sin(A)$ if $A \not\in \mathbb{A}$, and $e([A]) = 1$ and $\sin([A]) = 1$ otherwise.

Fix a total order $<$ in $\mathbb{A}$. Write $d_A$ for the degree of $A \in \mathbb{A}$. Let $M \in \mathbb{A}$ be monic. Put

$$S_M = \{ \text{monic prime factors of } M \}.$$ 

Fix a generator $\gamma$ of $\mathbb{F}_q^*$. For $P, Q \in S_M$ with $P < Q$, let

$$\alpha_{PQ} = \sum_{d_A < d_Q, d_B < d_P} \sum_{s=1}^{q-2} s \left( \frac{[BQ + \gamma^{-s}A]}{PQ} - \frac{[AP + \gamma^{-s}B]}{PQ} \right).$$

It is easy to see $\sin \alpha_{PQ} = e(\alpha_{PQ})$. We put

$$u_{PQ} = \begin{cases} 
sina_{PQ}, & \text{if } 2|d_P, 2|d_Q \\
\sqrt{P}sina_{PQ}, & \text{if } 2|d_P, 2 \nmid d_Q \\
\sqrt{Q}sina_{PQ}, & \text{if } 2 \nmid d_P, 2|d_Q \\
\sqrt{PQ}sina_{PQ}, & \text{if } 2 \nmid d_P, 2 \nmid d_Q 
\end{cases}$$

Set $K = k(\epsilon_C(\frac{\pi}{M}))$, which is the cyclotomic function field of conductor $M$ and is abelian over $k$. For $P \in S_M$, write $P^* = (-1)^{\frac{d_P-1}{2}}P = (-1)^{d_P}P$, where $|P| = q^{d_P}$, then $\sqrt{P^*} \in K$, hence $\sqrt{P^*} \in K$. As $\sin \alpha_{PQ} \in K$, we have $u_{PQ} \in K$. Put $\tilde{K} = K(\sqrt[\pi]{u_{PQ}})$. By [Sect.5.2, 4], $\tilde{K}$ is a quasi-cyclotomic function field over $k$, whose degree over $K$ equals to $q - 1$.

2. The Galois Groups

Let $G = \text{Gal}(K/k)$ and $\tilde{G} = \text{Gal}(\tilde{K}/k)$ be the Galois groups of the extensions $K/k$ and $\tilde{K}/k$ respectively. In this section, we determine $\tilde{G}$ by generators and relations.

Write $w = q - 1$ and $u = u_{PQ}$ for simplicity. Clearly $\text{Gal}(\tilde{K}/K)$ is isomorphic to $\mathbb{Z}/w\mathbb{Z}$. Recall that $\gamma$ is a fixed generator of $\mathbb{F}_q^*$. Let $\epsilon \in \text{Gal}(\tilde{K}/K)$ be a generator such that $\epsilon(\sqrt{u}) = \gamma \sqrt{u}$. Denote the isomorphism $\mathbb{F}_q^* \to \mathbb{Z}/w\mathbb{Z}$, $\gamma^i \mapsto i$ by $\log_\gamma$.

Each element of $G$ has $w$ liftings in $\tilde{K}$.

**Lemma 2.1.** For $\sigma \in G$, choose $\nu_\sigma \in K^*$ such that $\sigma(u) = \nu_\sigma u$, we define a lifting $\tilde{\sigma} \in \tilde{G}$ of $\sigma$ by $\tilde{\sigma}(\sqrt[\pi]{u}) = \nu_\sigma \sqrt{u}$. Then $\tilde{G} = \{ \tilde{\sigma} \epsilon^j | \sigma \in G, 0 \leq j \leq w - 1 \}$, and the multiplication in $\tilde{G}$ is given by $\tilde{\sigma} \tilde{\tau} = \tilde{\sigma} \tilde{\tau} \epsilon^{\log_\gamma i(\sigma, \tau)}$, where $i(\sigma, \tau) = \frac{\nu_{\sigma(\log_\gamma \nu_\tau)}}{\nu_{\sigma(\log_\gamma \nu_\sigma)}} \in \mathbb{F}_q^*$.

For any $\tilde{\sigma} \in \tilde{G}$, $\epsilon$ and $(\epsilon)^w$ are in the center of $\tilde{G}$.

**Proof.** By [Sect.5.1.2, 4], there exists such $\nu_\sigma \in K^*$ for $\sigma \in G$. The rest of the proof is trivial, which we refer to the proof of [Lemma 1, 2].

Let $M = P_1^r_1 P_2^r_2 \cdots P_n^r_n$ be the prime decomposition of $M$. We have the isomorphism:

$$G \cong (\mathbb{A}/M\mathbb{A})^* \cong (\mathbb{A}/P_1^{r_1}\mathbb{A})^* \times (\mathbb{A}/P_2^{r_2}\mathbb{A})^* \times \cdots \times (\mathbb{A}/P_n^{r_n}\mathbb{A})^*. $$
Different from the case of characteristic 0, now each \((\mathbb{A}/P_i^r\mathbb{A})^*\) is not always cyclic. But we have the decomposition \((\mathbb{A}/P_i^r\mathbb{A})^* \cong (\mathbb{A}/P_i\mathbb{A})^{(1)} \times (\mathbb{A}/P_i\mathbb{A})^*\), where \((\mathbb{A}/P_i^r\mathbb{A})^{(1)}\) is a \(p\)-group of order \(|P_i|^r - 1\) and \((\mathbb{A}/P_i\mathbb{A})^*\) is a cyclic group of order \(|P_i| - 1\), see [Prop.1.6, 5]. Let \(\sigma_{P_i} \in G\) associate to a generator of \((\mathbb{A}/P_i\mathbb{A})^*\). Then we have
\[
G = G^{(p)} \times G',
\]
where \(G' = \langle \sigma_{P_1}, \ldots, \sigma_{P_n} \rangle = \langle \sigma_{P_i} \rangle \times \cdots \times \langle \sigma_{P_n} \rangle\), and \(G^{(p)}\) is the \(p\)-Sylow subgroup of \(G\). In fact, \(G^{(p)} \cong (\mathbb{A}/P_1^r\mathbb{A})^{(1)} \times \cdots \times (\mathbb{A}/P_n^r\mathbb{A})^{(1)}\).

Let \(\tilde{G}^{(p)}\) and \(\tilde{G}'\) are the subgroups of \(\tilde{G}\) consisting of all liftings of the elements in \(G^{(p)}\) and in \(G'\) respectively. It is easy to see they are normal subgroups of \(\tilde{G}\).

**Lemma 2.2.** Let \(\tilde{G}^{(p)}\) be the \(p\)-Sylow subgroup of \(\tilde{G}\). Then
\[
\tilde{G}^{(p)} \cong \tilde{G}(\tilde{p}) / \langle \epsilon \rangle \cong G^{(p)}.
\]
Furthermore, we have \(\tilde{G} = \tilde{G}(\tilde{p}) \times \tilde{G}'\).

**Proof.** Since \(|\tilde{G}| = w|G| = |G^{(p)}| \cdot |\tilde{G}'|\), we have \(|\tilde{G}^{(p)}| = |G^{(p)}|\). Since each \(\tilde{\sigma} \in \tilde{G}^{(p)}\) is a lifting of some \(\sigma \in G^{(p)}\), all liftings of \(\sigma\) in \(\tilde{K}\) are \(\tilde{\sigma} \epsilon^i (0 \leq i \leq w - 1)\). Then the map \(\sigma \mapsto \tilde{\sigma} \mod \epsilon^i\) gives the isomorphism \(G^{(p)} \cong \tilde{G}(\tilde{p}) / \langle \epsilon \rangle\). Since the order of \(\epsilon\) equals to \(q - 1\), we see \(\tilde{\sigma}\) is the unique lifting of \(\sigma\) belonging to \(\tilde{G}^{(p)}\).

Thus \(\sigma \mapsto \tilde{\sigma}\) gives the isomorphism \(G^{(p)} \cong \tilde{G}^{(p)}\).

Since \((\tilde{G}(\tilde{p}))^w = G^{(p)}\), we have that \(\tilde{G}(\tilde{p})\) lies in the center of \(\tilde{G}\), and so it is a normal subgroup. In addition, as \(|\tilde{G}| = |\tilde{G}^{(p)}| \cdot |\tilde{G}'|\) and \((|\tilde{G}^{(p)}|, |\tilde{G}'|) = 1\), we have \(\tilde{G} = \tilde{G}^{(p)} \times \tilde{G}'\).

Next we consider the group \(\tilde{G}'\). For the generators \(\sigma_{P_i} \in G'\) \((1 \leq i \leq n)\), we fix a lifting \(\tilde{\sigma}_{P_i}\) of \(\sigma_{P_i}\) in \(\tilde{K}\) as follows.

If \(P_i \neq P, Q\), we define \(\tilde{\sigma}_{P_i}(\sqrt[\tilde{p}]{u}) = \sqrt[\tilde{p}]{u}\).

In fact, by [Sect.3.3, 4.3 and 5.1, 2], we have \(\sigma_{P_i}(u) = u\).

If \(P_i = P\) or \(Q\), we define \(\tilde{\sigma}_{P_i}(\sqrt[\tilde{p}]{u}) = v_{\sigma_{P_i}} \sqrt[\tilde{p}]{u}\),

where \(v_{\sigma_{P_i}} \in K\) is given by
\[
v_{\sigma_{P_i}} = \left(\sqrt[-d_{P_i}]{(\sqrt[-d_{P_i}]{\sin c_{P_i}})}\right)^{-1} \quad \text{and} \quad v_Q = \left(\sqrt[-d_{P_i}]{(\sqrt[-d_{P_i}]{\sin c_{Q}})}\right)^{-1},
\]

here \(c_{P_i}\) and \(c_{Q}\) are defined in [Sect.4.2.5, 2]. By [Sect.3.4.2 and 3.4.3, 4], we have \(\frac{u}{\sigma_{P_i}} = (\sqrt[-d_{P_i}]{(\sqrt[-d_{P_i}]{\sin c_{P_i}})})^u\) with \(\sqrt[-d_{P_i}]{(\sqrt[-d_{P_i}]{\sin c_{P_i}})} \in K\). Similarly for \(\tilde{\sigma}_Q\).

Then we have
\[
\tilde{G}' = \langle \tilde{\sigma}_{P_1}, \ldots, \tilde{\sigma}_{P_n}, \epsilon \rangle.
\]
Now we study the relations among these generators of \(\tilde{G}'\). First \(\epsilon\) commutes with each generator. By the calculations in [Sect.3.5, 3.6 and 5.1, 2], we see that the generators \(\tilde{\sigma}_{P_i}\) commute with each other except for the relation
\[
\tilde{\sigma}_{P_i}\tilde{\sigma}_Q = \tilde{\sigma}_Q\tilde{\sigma}_P \epsilon^{-1}.
\]

In addition, by definition, if \(P_i \neq P, Q\), then \(\text{ord}(\tilde{\sigma}_{P_i}) = \text{ord}(\sigma_{P_i})\). Finally, we need to compute the orders of \(\tilde{\sigma}_P\) and \(\tilde{\sigma}_Q\).
Let $L \in S_M$ and let $I_L$ be the inertia group of $L$ in $K$. It is known that $I_L \cong (\mathbb{A}/L^r \mathbb{A})^* \cong (\mathbb{A}/L^r \mathbb{A})^{(1)} \times (\mathbb{A}/L^r \mathbb{A})^*$, where $r$ is the maximal power of $L$ in $M$. We fix an inertia group $\bar{I}_L$ of $L$ in $\bar{K}$. Let $\bar{I}_L$ be a prime ideal in $\bar{K}$ over $L$ such that the inertia group $I(\bar{I}_L/L) = \bar{I}_L$. Let $\bar{G}_i$ be the $i$-th ramification group of $L/\bar{L}$, $i \geq -1$. Then by [III 8.6, 6], $G_0 = \bar{I}_L$, $\bar{I}_L/\bar{G}_1$ is cyclic of order relatively prime to $p$, and $\bar{G}_1$ is the unique $p$-Sylow subgroup of $\bar{I}_L$, which is in the center of $\bar{I}_L$ by Lemma 2.1. Put $G_L = < \sigma_L >$ and $\bar{G}_L = \bar{G}_L \cap \bar{I}_L$, where $\bar{G}_L$ is the subgroup of $\bar{G}$ consisting of all liftings of the elements of $G_L$. Write $e_L$ the ramification index of $L$ in the extension $\bar{K}/K$.

**Proposition 2.3.** We have $\bar{G}_1 \cong (\mathbb{A}/L^r \mathbb{A})^{(1)}$ and $\bar{G}_L$ is a cyclic group generated by some lifting of $\sigma_L$. Furthermore $\bar{I}_L = \bar{G}_1 \times \bar{G}_L$. In particular, all the liftings of $\sigma_L$ have the same order $e_L \cdot \text{ord}(\sigma_L)$.

**Proof.** Set $H = < \epsilon >$. The canonical homomorphism $\bar{I}_L \to I_L$, $\bar{\sigma} \mapsto \bar{\sigma}|_K$, induces an isomorphism $\bar{I}_L/(\bar{I}_L \cap H) \cong I_L$. Since $\bar{K}$ is abelian over $K$, we see $\bar{I}_L \cap H$ is the inertia group of $L$ in the field extension $\bar{K}/K$ by [Prop. 9.8, 5]. So the order of $\bar{I}_L \cap H$ is $e_L$. Notice that $\bar{G}_L \cap H = \bar{I}_L \cap H$. Hence $|\bar{I}_L| = e_L|I_L|$ and $|\bar{G}_L| = e_L|G_L|$. Since $G_1$ is in the center of $I_L$ and $\bar{I}_L/\bar{G}_1$ is cyclic, we see $\bar{I}_L$ is abelian. Noting that $(|\bar{G}_L|, |G_1|) = 1$ and $|\bar{I}_L| = |G_1|$, we have $\bar{I}_L = \bar{G}_1 \times \bar{G}_L$. So $\bar{G}_L \cong \bar{I}_L/\bar{G}_1$ is cyclic. Since $I_L = \bar{I}_L/K = G_1|K \times \bar{G}_L/K = G_1|K \times G_L$ and $G_1|K \cong G_1/(G_1 \cap H) = G_1$, we have $\bar{G}_1 \cong (\mathbb{A}/L^r \mathbb{A})^{(1)}$.

As $G_1|K = G_L$, there exists a lifting $\bar{\sigma}_L$ of $\sigma_L$, belonging to $\bar{G}_L$. Since the order of $\epsilon$ is a factor of $|G_L|$, all the liftings of $\sigma_L$ have the same order. If the order of $\bar{\sigma}_L$ is less than $|\bar{G}_L|$, then it is easy to show that the order of each element is also less than $|\bar{G}_L|$. But $\bar{G}_L$ is cyclic. Hence $\bar{\sigma}_L$ is a generator of $\bar{G}_L$. $\square$

If $P_1 \neq P$ and $Q$, then $e_{P_1} = 1$. Now we compute the ramification indices $e_P$ and $e_Q$ of $P$ and $Q$ in the extension $\bar{K}/K$.

Let $R$ be a monic irreducible polynomial in $\mathbb{A}$ and $A \in \mathbb{A}$ be coprime to $R$. Recall that the $(q - 1)$th residue symbol $(\frac{a}{R}) \in \mathbb{F}_q^*$ is defined by

$$\left(\frac{A}{R}\right) \equiv A^{\frac{|P|}{|Q|}} \mod R.$$ 

Let $v_P$ be the normalized valuation in $k^a$ associated to $P$ defined in [Sect.6, 2]. By [Prop.6.2, 2] we have

$$v_P(e(a_{PQ})) \equiv \log_\gamma \left(\frac{Q}{P}\right) \mod w \quad \text{and} \quad v_Q(e(a_{PQ})) \equiv -\log_\gamma \left(\frac{P}{Q}\right) \mod w.$$

and $v_P(P)$ equals to the ramification index $|P|^{-1}(|P| - 1)$ of $P$ in $K/k$, where $r$ is the maximal power of $P$ in $M$. Thus $v_P(\sqrt{P}) \equiv \frac{w}{d_P} \mod w$. Similarly, we have $v_Q(\sqrt{Q}) \equiv \frac{w}{d_Q} \mod w$.

Furthermore, by the reciprocity law $(\frac{a}{q}) = (-1)^{d_PD_Q}(\frac{P}{Q})$, see [Theorem 3.5, 5], we have

$$v_P(u) \equiv \log_\gamma \left(\frac{P}{Q}\right) \mod w \quad \text{and} \quad v_Q(u) \equiv -\log_\gamma \left(\frac{Q}{P}\right) \mod w,$$
By [III 7.3, 6], we have \( e_P = \frac{w}{(w, v_P(u))} \) and \( e_Q = \frac{w}{(w, v_Q(u))} \), so
\[
e_P = \frac{w}{(w, \log_{\gamma}(\frac{Q}{P}))} \quad \text{and} \quad e_Q = \frac{w}{(w, \log_{\gamma}(\frac{Q}{P}))}.
\]
In particular, if \( 2|d_P d_Q \), we have \( e_P = e_Q \). Finally we get the following theorem.

**Theorem 2.4.** We have \( \bar{G} = \bar{G}^{(p)} \times \bar{G}' \), where \( \bar{G}^{(p)} \) is the \( p \)-Sylow subgroup of \( \bar{G} \), and \( \bar{G}' :=< \bar{\sigma}_{P_1}, \ldots, \bar{\sigma}_{P_n}, \epsilon > \). The generators \( \bar{\sigma}_{P_i} \) and \( \epsilon \) commute with each other except for the relation \( \bar{\sigma}_P \bar{\sigma}_Q = \bar{\sigma}_Q \bar{\sigma}_P \epsilon^{-1} \). In addition, for \( P_i \neq P, Q \), we have \( \text{ord}(\bar{\sigma}_P) = \text{ord}(\sigma_P) \), and for \( P_i = P \) or \( Q \), we have
\[
\text{ord}(\bar{\sigma}_P) = \frac{w}{(w, \log_{\gamma}(\frac{Q}{P}))} \cdot \text{ord}(\sigma_P) \quad \text{and} \quad \text{ord}(\bar{\sigma}_Q) = \frac{w}{(w, \log_{\gamma}(\frac{Q}{P}))} \cdot \text{ord}(\sigma_Q).
\]

3. **The Genus Formula**

In this section we compute the genus of \( \tilde{K} \). We calculate it by using Hasse’s genus formula on Kummer extensions, which states that for a \( m \)-th Kummer extension \( E/F \) of algebraic function fields, \( m \) is relatively prime to the characteristic of \( F \), \( [E : F] = m \), and there exists \( a \in F \) such that \( E = F(\sqrt[n]{a}) \), then we have
\[
g_E = 1 + \frac{m}{[F_E : F]} \left[ g_F - 1 + \frac{1}{2} \sum_{p \in \mathbb{P}_F} \left( 1 - \frac{1}{e_p} \right) \deg p \right],
\]
where \( g_E \) and \( g_F \) are the genus of \( E \) and \( F \) respectively, \( F_E \) and \( F_p \) are the constant fields of \( E \) and \( F \) respectively, \( \mathbb{P}_F \) is the set of primes of \( F \), and \( e_p \) is the ramification index of \( p \) in \( E/F \). See [III 7.3, 6].

We first need to compute the genus of \( K \). In [3], Hayes calculated it in the case that the conductor \( M \) of \( K \) has only one prime factor. Here we use the Riemann-Hurwitz theorem to calculate the genus of \( K \) in general case.

Let \( E/F \) be a finite, separable, geometric extension of algebraic function fields, the Riemann-Hurwitz theorem says
\[
2g_E - 2 = [E : F](2g_F - 2) + \deg D_{E/F},
\]
where \( D_{E/F} \) is the different divisor of \( E/F \), see [Theorem 7.16, 5].

Recall that \( M \) has the prime decomposition \( M = P_1^{r_1} P_2^{r_2} \cdots P_n^{r_n} \).

**Proposition 3.1.** We have
\[
g_K = \left[ \frac{q - 2}{2(q - 1)} - 1 \right] \Phi(M) + \frac{1}{2} \sum_{i=1}^{n} s_i d_i \Phi(M/P_i^{r_i}) + 1,
\]
where \( d_i = \deg P_i \), \( s_i = r_i \Phi(P_i - q^{d_i(r_i - 1)} \Phi(\mathbb{P}/p)} \Phi(M) = |(\mathbb{A}/M)^*|.
\]

**Proof.** Let \( L \in S_M \) and \( r \) the maximal power of \( L \) in \( M \). Put \( d = \deg L \) and \( E = k(\mathbb{Q}(\sqrt{p})) \). Let \( i_{K/E} \) be the homomorphism from the divisor group of \( E \) to that of \( K \) defined by \( i_{K/E}(p) = \sum \epsilon(\mathbb{P}/p) \mathbb{P} \), where \( p \) is a prime of \( E \). By [Page 87, 5], we have
\[
D_{K/k} = D_{K/E} + i_{K/E}(D_{E/k}).
\]

It is known that \( L \) is totally ramified in \( E/k \). Let \( I \) be the unique prime ideal of \( E \) over \( L \). Let \( L_1, L_2, \ldots, L_g \) be all the different prime ideals of \( K \) over \( L \). For each \( L_j \), \( j = 1, 2, \ldots, g \), we now calculate its coefficient in \( D_{K/k} \). Since \( L_j \) is unramified in
\(K/E\), its coefficient in \(D_{K/E}\) is 0. By [Theorem 4.1, 3], the coefficient of \(I\) in \(D_{E/k}\) is \(s = r\Phi(L^r) - q^{d(r-1)}\), and so
\[
i_{K/E}(sI) = sl_{K/E}(I) = s \sum_{\mathfrak{p} \mid I} e(\mathfrak{p}\mathfrak{l}) \mathfrak{l}_{\mathfrak{p}} = s \sum \mathfrak{l}_{\mathfrak{p}}.
\]
Thus for each \(\mathfrak{l}_{\mathfrak{p}}\), its coefficient in \(D_{K/k}\) is \(s\).

Let \(\infty\) be the infinite prime of \(k\). There are \(\frac{\Phi(M)}{2}\) different infinite primes in \(K\) over \(\infty\), and the ramification index is \(q - 1\). Thus the coefficient of each infinite prime of \(K\) in \(D_{K/k}\) is \(q - 2\), also see Corollary in Page 85 in [5].

We have determined \(D_{K/k}\). By Riemann-Hurwitz theorem, we get the desired formula. \(\Box\)

The constant field of \(\bar{K}\) is clearly \(\mathbb{F}_q\). In last section we have computed the ramification indices in \(\bar{K}/K\) of all the finite primes of \(K\). To calculate the genus of \(\bar{K}\), we need to compute that of the infinite primes.

Let \(k_\infty \subset \Omega\) be the completion of \(k\) at the place \(1/T\). Let \(K^+ = K \cap k_\infty\) be the maximal real subfield of \(K\). By [Sect.4.3, 2], we know \(\text{sign}_Q \alpha = e(\alpha_Q) \in K^+\). It is known that for any monic square-free polynomial \(f(T)\) in \(\mathbb{F}_q[T]\) with even degree, we have \(\sqrt{f(T)} \in k_\infty\). So \(u \in K^+\).

Let \(E = K^+(\sqrt{u})\). Then \(\bar{K} = EK\) and \([E : K^+] = w\). Let \(\infty\) be any infinite prime of \(K^+\), \(\infty_1\) an infinite prime of \(K\) over \(\infty\), \(\infty_2\) an infinite prime of \(E\) over \(\infty\), and \(\bar{\infty}\) an infinite prime of \(\bar{K}\) over \(\infty_1\). By [Theorem 12.14, 5], the ramification index \(e(\infty_1/\infty) = w\). Then by Abhyankar's Lemma, see [III 8.9, 6], the ramification index \(e(\bar{\infty}/\infty) = w\). Since \(e(\bar{\infty}/\infty) = e(\bar{\infty}/\infty_1)\cdot e(\infty_1/\infty),\) we have \(e(\bar{\infty}/\infty_1) = 1\).

Thus \(\infty_1\) is unramified in \(\bar{K}/K\). Since \(\bar{K}\) is Galois over \(K\), all infinite primes of \(K\) are unramified in \(\bar{K}/K\). Now we can get the genus formula of \(\bar{K}\).

**Theorem 3.2.** We have
\[
g_{\bar{K}} = 1 + w \left[ g_K - 1 + \frac{1}{2} \left( 1 - \frac{1}{e_P} \right) d_P \Phi(M/P^{r_P}) + \frac{1}{2} \left( 1 - \frac{1}{e_Q} \right) d_Q \Phi(M/Q^{r_Q}) \right],
\]
where \(r_P\) and \(r_Q\) are the maximal powers of \(P\) and \(Q\) in \(M\) respectively, \(e_P = \frac{\mu}{(w, \log_{\mathbb{F}_q}(\bar{\mathbb{Q}}))}\) and \(e_Q = \frac{\mu}{(w, \log_{\mathbb{F}_q}(\bar{\mathbb{Q}}))}\).

**Proof.** By Hasse's formula, we have
\[
g_{\bar{K}} = 1 + w \left[ g_K - 1 + \frac{1}{2} \sum_{\text{prime } P \text{ in } K \atop p \mid P \text{ or } p \mid Q} \left( 1 - \frac{1}{e_P} \right) \text{deg} P \right],
\]
where the sum is over all the unequivalent primes over \(P\) or \(Q\), \(e_P\) is the ramification index of \(P\) in \(K/K\), and \(\text{deg} P = f(P/P)d_P\).

We assume that there are \(g_P\) and \(g_Q\) different prime ideals in \(K\) over \(P\) and \(Q\) respectively. Then
\[
g_{\bar{K}} = 1 + w \left[ g_K - 1 + \frac{1}{2} \left( 1 - \frac{1}{e_P} \right) g_P f_P d_P + \frac{1}{2} \left( 1 - \frac{1}{e_Q} \right) g_Q f_Q d_Q \right],
\]
where \(f_P\) and \(f_Q\) are the residue class degrees of \(P\) and \(Q\) in \(K/k\) respectively.

Since \(g_P f_P = \Phi(M/P^{r_P})\) and \(g_Q f_Q = \Phi(M/Q^{r_Q})\), we get the formula. \(\Box\)
Galois Groups and Genera of Quasi-Cyclotomic Function Fields

4. THE GENERAL CASE

In this section, we consider the general case. We follow the method in [7] to determine the Galois group in this case.

Let \( K = K(\sqrt[n]{u}) \), where \( u = u_{P_1Q_1} \cdots u_{P_mQ_m} \) and \( P_i < Q_i \in S_M \). We assume \( (P_i, Q_i) \neq (P_j, Q_j) \) for \( i \neq j \). Then \( K \) is also a quasi-cyclotomic function field over \( k \), whose degree over \( K \) equals to \( q - 1 \). Notice that there may exist \( P_i \) or \( Q_i \) appearing repeatedly in this sequence \( P_1, Q_1, \ldots, P_m, Q_m \).

Let \( G = \text{Gal}(\tilde{K}/k) \). Applying the same arguments, Lemma 2.1 and Lemma 2.2 are also true here. Then we have \( \tilde{G} = \tilde{G}^{(p)} \times \tilde{G}' \), where the meanings of the notations are similar as before.

We consider the field \( K = K(\sqrt[n]{u_{P_1Q_1}}, \ldots, \sqrt[n]{u_{P_mQ_m}}) \). It is Galois over \( k \) with degree \( w^m \Phi(M) \). Each element of \( G \) has \( w^m \) liftings to \( \tilde{K} \). For each \( P \in S_M \), we define a lifting \( \tilde{\sigma}_P \) of \( \sigma_P \) to \( \tilde{K} \) as before. If \( P \neq P_i \), then \( \tilde{\sigma}_P(\sqrt[n]{u_{P_iQ_i}}) = \sqrt[n]{u_{P_iQ_i}} \).

Otherwise, \( \tilde{\sigma}_P(\sqrt[n]{u_{P_iQ_i}}) = v_{\sigma_P} \sqrt[n]{u_{P_iQ_i}} \) and \( \tilde{\sigma}_Q_i(\sqrt[n]{u_{P_iQ_i}}) = v_{\sigma_Q_i} \sqrt[n]{u_{P_iQ_i}} \). We denote the restriction of \( \tilde{\sigma}_P \) on \( \tilde{K} \) by \( \tilde{\sigma}_P \). Then the group \( \tilde{G}' \) is generated by \( \{ \tilde{\sigma}_P, \epsilon | P \in S_M \} \), where \( \epsilon \) is defined as before.

Now we consider the relations between these generators. If \( P \in S_M \) and \( P \neq P_i, Q_i (1 \leq i \leq m) \), it is easy to see \( \tilde{\sigma}_P \) commutes with all generators, and the order of \( \tilde{\sigma}_P \) equals to that of \( \sigma_P \). By the discussion in section 2, we have \( \tilde{\sigma}_P, \tilde{\sigma}_Q_i = \tilde{\sigma}_P, \tilde{\sigma}_Q_i, \epsilon_i^{-1} \) for each \( i \), where \( \epsilon_i \) acts trivially on \( K \) and \( \sqrt[n]{u_{P_{i}Q_i}} \), for \( j \neq i \), and \( \epsilon_i(\sqrt[n]{u_{P_{j}Q_i}}) = \gamma \sqrt[n]{u_{P_{j}Q_i}} \). Since \( \epsilon_i | \tilde{K} = \epsilon \), we see \( \tilde{\sigma}_P, \tilde{\sigma}_Q_i = \tilde{\sigma}_P, \tilde{\sigma}_Q_i, \epsilon_i^{-1} \). The other multiplication relations among \( \tilde{\sigma}_P, \tilde{\sigma}_Q_1, \ldots, \tilde{\sigma}_P, \tilde{\sigma}_Q_m \) are complicated, but it is easy to determine. Since Proposition 2.3 is also true here, the orders of \( \tilde{\sigma}_P \) and \( \tilde{\sigma}_Q_i \) can be determined by the ramification natures of \( P_i \) and \( Q_i \) in \( \tilde{K}/K \). In other words, let \( P \) be one of \( P_1, Q_1, \ldots, P_m, Q_m \), let \( L_1, \ldots, L_s \) be all the monic prime factors paired with \( P \) with the form \( u_{P_i} \), \( 1 \leq i \leq s \), and let \( R_1, \ldots, R_t \) be all the monic prime factors paired with \( P \) with the form \( u_{P_iP_j} \), \( 1 \leq i \leq t \), then \( \overline{\text{ord}}(\tilde{\sigma}_P) = w^{\text{log}_n(\frac{1}{w\text{ord}_v(\frac{P_i}{M}P_j)})} \cdot \text{ord}(\sigma_P) \). Therefore, we determine the group \( \tilde{G} \) by generators and relations.

In fact, we have got the ramification indexes \( \epsilon_P, \epsilon_Q_i (1 \leq i \leq m) \) in the above paragraph. We can also get that all the infinite primes of \( K \) are unramified in the field extension \( \tilde{K}/K \) by applying the same argument as the paragraph above Theorem 3.2. Hence, we can get the genus formula in the general case by applying the same argument as Theorem 3.2.

References

[1] S. Bae, E.-U. Gekeler, P. Kang and L. Yin, Anderson’s double complex and gamma monomials for rational function fields, Trans. Amer. Math. Soc. 355 (2003), 3463-3474.
[2] S. Bae, L. Yin, Carlitz-Hayes plus Anderson’s epsilon, J. reine angew. Math. 571 (2004), 19-37.
[3] D.R. Hayes, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. 189 (1974), 77-91.
[4] C. Liu, L. Yin, Double coverings for quadratic extensions and function fields, J. Number Theory 130 (2010), 469-477.
[5] M. Rosen, Number theory in function fields, GTM 210, Springer-Verlag, 2002.
[6] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag, 1993.
[7] L. Yin, C. Zhang, Arithmetic of quasi-cyclotomic fields, J. Number Theory 128 (2008), 1717-1730.

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, P.R. China
E-mail address: sham07@mails.tsinghua.edu.cn

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, P.R. China
E-mail address: lsyin@math.tsinghua.edu.cn