Journal of Number Theory 132 (2012) 2574–2581

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Galois groups and genera of a kind of quasi-cyclotomic function fields ☆

Min Sha *, Linsheng Yin

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

ARTICLE INFO

Article history:
Received 31 July 2011
Revised 13 February 2012
Accepted 21 May 2012
Available online 20 July 2012
Communicated by David Goss

MSC:
primary 11R58
secondary 11R32, 11R60

Keywords:
Cyclotomic function field
Quasi-cyclotomic function field
Galois group
Genus

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 were described explicitly in [4] following the works in [1] and [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 [8] 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 $k = \mathbb{F}_q(T)$ be the rational function field over the finite field $\mathbb{F}_q$ of q elements. In this paper we always assume that the characteristic of k is an odd prime number p. Put $\mathbb{A} = \mathbb{F}_q[T]$. Let Ω be the

☆ This work was supported by NSFC Project No. 10571097.
* Corresponding author.
E-mail addresses: shamin2010@gmail.com (M. Sha), lsyin@math.tsinghua.edu.cn (L. Yin).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.05.015

completion of the algebraic closure of $\mathbb{F}_q((1/T))$ at the place $1/T$. Let k^{ac} be the algebraic closure of k in Ω. 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 $\bar{\pi}\mathbb{A}$ of rank one corresponds to the Carlitz module. The Carlitz exponential function $\mathbf{e}_C$ is defined by

$$\mathbf{e}_C(x) = x \prod_{0 \neq u \in \bar{\pi}\mathbb{A}} \left(1 - \frac{x}{u}\right), \quad x \in \Omega.$$

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

$$\sin(A) = \sqrt[q-1]{-1} \cdot \mathbf{e}_C\big(\bar{\pi}\{A\}/\mathrm{sgn}\big(\{A\}\big)\big),$$

where sgn is a fixed sign function on $\mathbb{F}_q((1/T))$. For the definition of sign function, see [3, Definition 7.2.1].

Let $\mathcal{A}$ be the free abelian group generated by the symbols $[A]$, $A \in k \setminus \mathbb{A}$. Define two homomorphisms

$$\sin, \mathbf{e} : \mathcal{A} \to k^{ab*}$$

such that $\sin([A]) = \sin(A)$ and $\mathbf{e}([A]) = \mathbf{e}_C(\bar{\pi}A)$ for $A \notin \mathbb{A}$, and $\sin([A]) = 1$ and $\mathbf{e}([A]) = 1$ 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 γ of $\mathbb{F}_q^*$. For $P, Q \in S_M$ with $P < Q$, let

$$\mathbf{a}_{PQ} = \sum_{\substack{d_A < d_Q \\ A:\ \text{monic}}} \sum_{\substack{d_B < d_P \\ B:\ \text{monic}}} \sum_{s=1}^{q-1} s\left(\left[\frac{BQ + \gamma^{-s}A}{PQ}\right] - \left[\frac{AP + \gamma^{-s}B}{PQ}\right]\right).$$

Notice that there is a print mistake in [4], where s runs from 1 to $q-2$ in the definition of $\mathbf{a}_{PQ}$. We also want to indicate that the homomorphism $\mathbf{e}$ gives the same value in the $\mathbf{a}_{PQ}$ here and in the $\mathbf{a}_{PQ}$ of [2].

We put

$$u_{PQ} = \begin{cases} \sin \mathbf{a}_{PQ}, & \text{if } 2|d_P,\ 2|d_Q, \\ \sqrt{P}\sin \mathbf{a}_{PQ}, & \text{if } 2|d_P,\ 2\nmid d_Q, \\ \sqrt{Q}\sin \mathbf{a}_{PQ}, & \text{if } 2\nmid d_P,\ 2|d_Q, \\ \sqrt{PQ}\sin \mathbf{a}_{PQ}, & \text{if } 2\nmid d_P,\ 2\nmid d_Q. \end{cases}$$

Set $K = k(\mathbf{e}_C(\frac{\bar{\pi}}{M}))$, which is the cyclotomic function field of conductor M whose Galois group over k is canonically isomorphic to $(\mathbb{A}/M\mathbb{A})^*$. Since $u_{PQ} \in K$, put $\widetilde{K} = K(\sqrt[q-1]{u_{PQ}})$. By [4, Theorem 3], $\widetilde{K}$ is a quasi-cyclotomic function field over k, which implies that $[\widetilde{K} : k] = (q-1)\Phi(M)$, where $\Phi(M)$ is the number of elements in $(\mathbb{A}/M\mathbb{A})^*$.

2. The Galois groups

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

In the sequel, we write $w = q-1$ and $u = u_{PQ}$ for simplicity.

First, we want to indicate a basic fact without proof. We will use it several times without indication.

Lemma 2.1. *There exists $a \in \mathbb{F}_q^*$ such that* $\sin \mathbf{a}_{PQ} = a\mathbf{e}(\mathbf{a}_{PQ})$.

Clearly $\mathrm{Gal}(\widetilde{K}/K)$ is isomorphic to $\mathbb{Z}/w\mathbb{Z}$. Recall that γ is a fixed generator of $\mathbb{F}_q^*$. Let $\epsilon \in \mathrm{Gal}(\widetilde{K}/K)$ be a generator such that

$$\epsilon\left(\sqrt[w]{u}\right) = \gamma \sqrt[w]{u}.$$

Denote by $\log_\gamma$ the isomorphism

$$\log_\gamma : \mathbb{F}_q^* \to \mathbb{Z}/w\mathbb{Z}, \quad \gamma^i \mapsto \bar{i}.$$

Each element of G has w liftings in $\widetilde{G}$. Then we have a coarse description about $\widetilde{G}$.

Lemma 2.2. *For any $\sigma \in G$, choosing $v_\sigma \in K^*$ such that $\sigma(u) = v_\sigma^w u$, we can define a lifting $\tilde{\sigma} \in \widetilde{G}$ of σ by $\tilde{\sigma}(\sqrt[w]{u}) = v_\sigma \sqrt[w]{u}$. Then $\widetilde{G} = \{\tilde{\sigma}\epsilon^j \mid \sigma \in G, 0 \leqslant j \leqslant w-1\}$, and the multiplication in $\widetilde{G}$ is given by $\widetilde{\sigma\tau} = \tilde{\sigma}\tilde{\tau}\epsilon^{\log_\gamma i(\sigma,\tau)}$, where $i(\sigma,\tau) = \frac{v_{\sigma\tau}}{v_\sigma \sigma(v_\tau)} \in \mathbb{F}_q^*$. For any $\tilde{\sigma} \in \widetilde{G}$, ϵ and $(\tilde{\sigma})^w$ belong to the center of $\widetilde{G}$.*

Proof. By [4, Section 5.1.2], there exists such $v_\sigma \in K^*$ for any $\sigma \in G$. The rest of the proof is trivial, we refer to the proof of [8, Lemma 1]. $\square$

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:

$$G \cong (\mathbb{A}/M\mathbb{A})^* \cong \left(\mathbb{A}/P_1^{r_1}\mathbb{A}\right)^* \times \left(\mathbb{A}/P_2^{r_2}\mathbb{A}\right)^* \times \cdots \times \left(\mathbb{A}/P_n^{r_n}\mathbb{A}\right)^*.$$

Different from the case of characteristic 0, now each $(\mathbb{A}/P_i^{r_i}\mathbb{A})^*$ is not always cyclic. But we have the decomposition $(\mathbb{A}/P_i^{r_i}\mathbb{A})^* \cong (\mathbb{A}/P_i^{r_i}\mathbb{A})^{(1)} \times (\mathbb{A}/P_i\mathbb{A})^*$, where $(\mathbb{A}/P_i^{r_i}\mathbb{A})^{(1)}$ is a p-group of order $|P_i|^{r_i-1}$ and $(\mathbb{A}/P_i\mathbb{A})^*$ is a cyclic group of order $|P_i|-1$, where $|P_i| = q^{d_{P_i}}$, see [5, Proposition 1.6]. For $1 \leqslant i \leqslant n$, since the inertia group of P_i in K is isomorphic to $(\mathbb{A}/P_i^{r_i}\mathbb{A})^*$, we choose a $\sigma_{P_i} \in G$ with $\langle \sigma_{P_i} \rangle \cong (\mathbb{A}/P_i\mathbb{A})^*$ such that σ_{P_i} is contained in the inertia group of P_i. Then we have

$$G = G^{(p)} \times G',$$

where $G' = \langle \sigma_{P_1} \rangle \times \cdots \times \langle \sigma_{P_n} \rangle$, and $G^{(p)}$ is the p-Sylow subgroup of G. In fact, $G^{(p)} \cong (\mathbb{A}/P_1^{r_1}\mathbb{A})^{(1)} \times \cdots \times (\mathbb{A}/P_n^{r_n}\mathbb{A})^{(1)}$.

Let $\widetilde{G^{(p)}}$ and $\widetilde{G}'$ be the subgroups of $\widetilde{G}$ consisting of all liftings of the elements in $G^{(p)}$ and in G' respectively. It is easy to see that both of them are normal subgroups of $\widetilde{G}$. Then we can get a decomposition of $\widetilde{G}$.

Lemma 2.3. *Let $\widetilde{G}^{(p)}$ be the p-Sylow subgroup of $\widetilde{G}$. Then*

$$\widetilde{G}^{(p)} \cong \widetilde{G^{(p)}}/\langle \epsilon \rangle \cong G^{(p)}.$$

Furthermore, we have $\widetilde{G} = \widetilde{G}^{(p)} \times \widetilde{G}'$, and $\widetilde{G}^{(p)}$ is contained in the center of $\widetilde{G}$.

Proof. Since $|\widetilde{G}| = w|G| = |G^{(p)}| \cdot |\widetilde{G'}|$, we have $|\widetilde{G}^{(p)}| = |G^{(p)}|$. In addition, since the order of ϵ and p are coprime, for each element of $G^{(p)}$, there exists at most one lifting contained in $\widetilde{G}^{(p)}$. So for each $\sigma \in G^{(p)}$, there exists a unique lifting σ' of σ such that $\sigma' \in \widetilde{G}^{(p)}$. Then the map $\sigma \mapsto \sigma'$ mod $\langle\epsilon\rangle$ gives the isomorphism $G^{(p)} \cong \widetilde{G^{(p)}}/\langle\epsilon\rangle$ and the map $\sigma \mapsto \sigma'$ gives the isomorphism $G^{(p)} \cong \widetilde{G}^{(p)}$.

Since $\widetilde{G}^{(p)} = (\widetilde{G}^{(p)})^w$, by Lemma 2.2 we see that $\widetilde{G}^{(p)}$ is contained in the center of $\widetilde{G}$. So $\widetilde{G}^{(p)}$ is a normal subgroup of $\widetilde{G}$. In addition, as $|\widetilde{G}| = |\widetilde{G}^{(p)}| \cdot |\widetilde{G}'|$ and $\gcd(|\widetilde{G}^{(p)}|, |\widetilde{G}'|) = 1$, we have $\widetilde{G} = \widetilde{G}^{(p)} \times \widetilde{G}'$. $\square$

Next we need to investigate the subgroup $\widetilde{G}'$.

For each generator $\sigma_{P_i} \in G'$ $(1 \leqslant i \leqslant n)$, according to Lemma 2.2 we fix a lifting $\tilde{\sigma}_{P_i}$ of σ_{P_i} in $\widetilde{G}$ as follows.

If $P_i \neq P, Q$, we define

$$\tilde{\sigma}_{P_i}\big(\sqrt[w]{u}\big) = \sqrt[w]{u}.$$

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

If $P_i = P$ or Q, we define

$$\tilde{\sigma}_{P_i}\big(\sqrt[w]{u}\big) = v_{\sigma_{P_i}} \sqrt[w]{u},$$

where $v_{\sigma_{P_i}} \in K$ is given by

$$v_{\sigma_P} = \big(\sqrt[w]{(-1)^{d_Q}} \sin \mathbf{c}_{\sigma_P}\big)^{-1} \quad \text{and} \quad v_{\sigma_Q} = \big(\sqrt[w]{(-1)^{d_P}} \sin \mathbf{c}_{\sigma_Q}\big)^{-1},$$

here $\mathbf{c}_{\sigma_P}$ and $\mathbf{c}_{\sigma_Q}$ were defined in [2, Section 4.2.5]. By [4, Sections 3.4.2 and 3.4.3], we have $\frac{u}{\sigma_P(u)} = (\sqrt[w]{(-1)^{d_Q}} \sin \mathbf{c}_{\sigma_P})^w$ with $\sqrt[w]{(-1)^{d_Q}} \sin \mathbf{c}_{\sigma_P} \in K^*$.

Hence, we have

$$\widetilde{G}' = \langle \tilde{\sigma}_{P_1}, \ldots, \tilde{\sigma}_{P_n}, \epsilon\rangle.$$

Now we study the relations among these generators of $\widetilde{G}'$. First ϵ commutes with each generator. For $L, R \in S_M$, $L < R$, set $\alpha_{LR} = \frac{\sigma_L(v_{\sigma_R})/v_{\sigma_R}}{\sigma_R(v_{\sigma_L})/v_{\sigma_L}}$. By Lemma 2.2, we have $\tilde{\sigma}_L\tilde{\sigma}_R = \tilde{\sigma}_R\tilde{\sigma}_L\epsilon^{\log_\gamma \alpha_{LR}}$. By [2, Section 3.5: The Log Wedge Formula, Section 3.6: The Auxiliary Formula and Section 5.1: The Main Formula], we see that the generators $\tilde{\sigma}_{P_i}$ commute with each other except for the relation

$$\tilde{\sigma}_P\tilde{\sigma}_Q = \tilde{\sigma}_Q\tilde{\sigma}_P\epsilon^{-1}.$$

So in fact, $\widetilde{G}' = \langle \tilde{\sigma}_{P_1}, \ldots, \tilde{\sigma}_{P_n}\rangle$.

By definition, if $P_i \neq P, Q$, then we have $\operatorname{ord}(\tilde{\sigma}_{P_i}) = \operatorname{ord}(\sigma_{P_i})$. 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 $I_L \cong (\mathbb{A}/L^r\mathbb{A})^* \cong (\mathbb{A}/L^r\mathbb{A})^{(1)} \times (\mathbb{A}/L\mathbb{A})^*$, where r is the maximal power of L such that $L^r | M$. We fix an inertia group $\widetilde{I}_L$ of L in $\widetilde{K}$. Let $\widetilde{L}$ be a prime ideal in $\widetilde{K}$ above L such that the inertia group $I(\widetilde{L}/L) = \widetilde{I}_L$. Let $\widetilde{G}_i$ be the i-th ramification group of $\widetilde{L}|L$, $i \geqslant -1$. Then by [7, III 8.6], $\widetilde{G}_0 = \widetilde{I}_L$, $\widetilde{I}_L/\widetilde{G}_1$ is cyclic of order relatively prime to p, and $\widetilde{G}_1$ is the unique p-Sylow subgroup of $\widetilde{I}_L$ which is contained in the center of $\widetilde{I}_L$ by Lemma 2.2.

Put $G_L = \langle\sigma_L\rangle \subset I_L$ and $\widetilde{G}_L = \widetilde{G_L} \cap \widetilde{I}_L$, where $\widetilde{G_L}$ is the subgroup of $\widetilde{G}$ consisting of all liftings of the elements of G_L. Denote by e_L the ramification index of any prime ideal of $\widetilde{K}$ lying above L in the extension $\widetilde{K}/K$.

Proposition 2.4. *$\widetilde{I}_L$ is an abelian group with $\widetilde{I}_L = \widetilde{G}_1 \times \widetilde{G}_L$, where $\widetilde{G}_1 \cong (\mathbb{A}/L^r\mathbb{A})^{(1)}$ and $\widetilde{G}_L$ is a cyclic group generated by a lifting of σ_L. Furthermore, all the liftings of σ_L have the same order $e_L \cdot \mathrm{ord}(\sigma_L)$.*

Proof. Set $H = \langle \epsilon \rangle$. The canonical homomorphism $\widetilde{I}_L \to I_L$, $\tilde{\sigma} \mapsto \tilde{\sigma}|_K$, induces an isomorphism $\widetilde{I}_L/(\widetilde{I}_L \cap H) \cong I_L$. Since $\widetilde{K}$ is abelian over K, $\widetilde{I}_L \cap H$ is the inertia group of L in the field extension $\widetilde{K}/K$ by [5, Proposition 9.8]. So the order of $\widetilde{I}_L \cap H$ is e_L, and thus $|\widetilde{I}_L| = e_L|I_L|$. Noticing that $\widetilde{G}_L \cap H = \widetilde{I}_L \cap H$ and the above homomorphism also induces an isomorphism $\widetilde{G}_L/(\widetilde{G}_L \cap H) \cong G_L$, we have $|\widetilde{G}_L| = e_L|G_L|$.

Since $\widetilde{G}_1$ is contained in the center of $\widetilde{I}_L$ and $\widetilde{I}_L/\widetilde{G}_1$ is cyclic, we see that $\widetilde{I}_L$ is abelian. Noticing that $\gcd(|\widetilde{G}_L|, |\widetilde{G}_1|) = 1$ and $|\widetilde{I}_L| = |\widetilde{G}_1| \cdot |\widetilde{G}_L|$, we have $\widetilde{I}_L = \widetilde{G}_1 \times \widetilde{G}_L$. So $\widetilde{G}_L \cong \widetilde{I}_L/\widetilde{G}_1$ is cyclic. Since $I_L = \widetilde{I}_L|_K = \widetilde{G}_1|_K \times \widetilde{G}_L|_K = \widetilde{G}_1|_K \times G_L$ and $\widetilde{G}_1|_K \cong \widetilde{G}_1/(\widetilde{G}_1 \cap H) = \widetilde{G}_1$, we have $\widetilde{G}_1 \cong (\mathbb{A}/L^r\mathbb{A})^{(1)}$.

As $\widetilde{G}_L|_K = G_L$, there exists a lifting σ'_L of σ_L belonging to $\widetilde{G}_L$. Since the order of ϵ is a factor of the order of σ_L, all the liftings of σ_L have the same order. If the order of σ'_L is less than $|\widetilde{G}_L|$, then it is easy to show that the order of each element is also less than $|\widetilde{G}_L|$. But $\widetilde{G}_L$ is cyclic. Hence σ'_L must be a generator of $\widetilde{G}_L$. $\square$

Remark 2.5. The extension $\widetilde{K}/k$ gives us an example of a non-abelian function field extension with abelian inertia groups.

If $P_i \neq P$ and Q, then $e_{P_i} = 1$. Now we need to calculate the ramification indices e_P and e_Q.

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

$$\left(\frac{A}{R}\right) \equiv A^{\frac{|R|-1}{q-1}} \mod R.$$

Let v_P be the additive valuation in k^{ab} associated to P defined in [2, Section 6]. Notice that the restriction of v_P in $k(\mathbf{e}_C(\frac{\bar{\pi}}{P}))$ is the normalized valuation of $k(\mathbf{e}_C(\frac{\bar{\pi}}{P}))$ associated to P. By [2, Proposition 6.2], we have

$$v_P\big(\mathbf{e}(\mathbf{a}_{PQ})\big) \equiv \log_\gamma\left(\frac{Q}{P}\right) \quad \text{and} \quad v_Q\big(\mathbf{e}(\mathbf{a}_{PQ})\big) \equiv -\log_\gamma\left(\frac{P}{Q}\right) \pmod{w}.$$

In addition, $v_P(P)$ equals to the ramification index $|P|-1$ of P in $k(\mathbf{e}_C(\frac{\bar{\pi}}{P}))/k$. Thus $v_P(\sqrt{P}) \equiv \frac{w}{2}d_P \pmod{w}$. Similarly, we have $v_Q(\sqrt{Q}) \equiv \frac{w}{2}d_Q \pmod{w}$.

Furthermore, combining with the reciprocity law $(\frac{Q}{P}) = (-1)^{d_P d_Q}(\frac{P}{Q})$, see [5, Theorem 3.5], we have

$$v_P(u) \equiv \log_\gamma\left(\frac{P}{Q}\right) \quad \text{and} \quad v_Q(u) \equiv -\log_\gamma\left(\frac{Q}{P}\right) \pmod{w}.$$

By [7, III 7.3], noticing that the valuations there are different from what we use here, we have $e_P = \frac{w}{\gcd(w, v_P(u))}$ and $e_Q = \frac{w}{\gcd(w, v_Q(u))}$. So

$$e_P = \frac{w}{\gcd(w, \log_\gamma(\frac{P}{Q}))} \quad \text{and} \quad e_Q = \frac{w}{\gcd(w, \log_\gamma(\frac{Q}{P}))}.$$

Finally we get the following theorem.

Theorem 2.6. *We have $\widetilde{G} = \widetilde{G}^{(p)} \times \widetilde{G}'$, where $\widetilde{G}^{(p)}$ is the p-Sylow subgroup of $\widetilde{G}$ which is contained in the center of $\widetilde{G}$, and $\widetilde{G}' = \langle \tilde{\sigma}_{P_1}, \ldots, \tilde{\sigma}_{P_n}, \epsilon \rangle$. The generators $\tilde{\sigma}_{P_i}$ and ϵ commute with each other except for the relation $\tilde{\sigma}_P \tilde{\sigma}_Q = \tilde{\sigma}_Q \tilde{\sigma}_P \epsilon^{-1}$. In addition, for $P_i \neq P, Q$, we have $\operatorname{ord}(\tilde{\sigma}_{P_i}) = \operatorname{ord}(\sigma_{P_i})$, and for $P_i = P$ or Q, we have*

$$\operatorname{ord}(\tilde{\sigma}_P) = \frac{w}{\gcd(w, \log_\gamma(\frac{P}{Q}))} \cdot \operatorname{ord}(\sigma_P) \quad \textit{and} \quad \operatorname{ord}(\tilde{\sigma}_Q) = \frac{w}{\gcd(w, \log_\gamma(\frac{Q}{P}))} \cdot \operatorname{ord}(\sigma_Q).$$

Notice that for each $1 \leqslant i \leqslant n$, $\operatorname{ord}(\sigma_{P_i}) = \Phi(P_i)$.

Corollary 2.7. *$\widetilde{K}/k$ is a solvable extension.*

Proof. Notice that the commutator subgroup of $\widetilde{G}$ is $\langle \epsilon \rangle$. $\square$

Corollary 2.8. *In the extension $\widetilde{K}/K$, all ramified prime ideals of K are tamely ramified.*

Corollary 2.9. *For any prime ideal $\mathfrak{p}$ of K not above P and Q, it is unramified in $\widetilde{K}/K$.*

Corollary 2.10. *The prime ideals of K above P (resp. Q) are unramified if and only if $(\frac{P}{Q}) = 1$ (resp. $(\frac{Q}{P}) = 1$).*

In addition, all infinite primes of K are unramified in $\widetilde{K}/K$, see Lemma 3.3.

Corollary 2.11. *If $2 | d_P d_Q$, then we have $e_P = e_Q$.*

Corollary 2.12. *Suppose $2 \nmid d_P d_Q$. We have:*

(1) *If $e_P = 1$, then $e_Q = 2$.*
(2) *If $e_P = w$, then $e_Q = w$ or $\frac{w}{2}$. Moreover, $e_Q = w$ if and only if $4 | w$.*

Proof. Notice that

$$\log_\gamma\left(\frac{P}{Q}\right) \equiv \log_\gamma\left(\frac{Q}{P}\right) + \frac{w}{2} \pmod{w}. \qquad \square$$

If we exchange the positions of e_P and e_Q, the above corollary is also true.

Corollary 2.13. *Let L be a monic irreducible polynomial in $\mathbb{A}$, then L is ramified in $\widetilde{K}/k$ if and only if $L | M$.*

3. The genus formula

In this section we compute the genus of $\widetilde{K}$. We calculate it by using Hasse's genus formula on Kummer extensions, which states that for an m-th Kummer extension E/F of algebraic function fields, where m is relatively prime to the characteristic of F, we have

$$g_E = 1 + \frac{m}{[\mathbb{F}_E : \mathbb{F}_F]}\left[g_F - 1 + \frac{1}{2}\sum_{\mathfrak{p} \in \mathbb{P}_F}\left(1 - \frac{1}{e_\mathfrak{p}}\right)\deg \mathfrak{p}\right],$$

where g_E and g_F are the genus of E and F respectively, $\mathbb{F}_E$ and $\mathbb{F}_F$ are the constant fields of E and F respectively, $\mathbb{P}_F$ is the set of primes of F, and $e_\mathfrak{p}$ is the ramification index of $\mathfrak{p}$ in E/F, see [7, III 7.3].

Recall that M has the prime decomposition $M = P_1^{r_1} P_2^{r_2} \cdots P_n^{r_n}$. For the genus of K, we quote a formula from [6, Theorem 12.7.2].

Theorem 3.1. *We have*

$$g_K = \left[\frac{q-2}{2(q-1)} - 1\right]\Phi(M) + \frac{1}{2}\sum_{i=1}^{n} s_i d_i \Phi\big(M/P_i^{r_i}\big) + 1,$$

where $d_i = d_{P_i}$, $s_i = r_i \Phi(P_i^{r_i}) - q^{d_i(r_i-1)}$ *and* $\Phi(M) = |(\mathbb{A}/M)^*|$.

Lemma 3.2. *The constant field of* $\widetilde{K}$ *is* $\mathbb{F}_q$.

Proof. Since the constant field of K is $\mathbb{F}_q$, it suffices to show that $u \notin \mathbb{F}_q$.

Suppose that $u \in \mathbb{F}_q$. Then for any $\sigma \in G$, $\sigma(u) = u$. We can get a lifting $\tilde{\sigma}$ of σ defined by $\tilde{\sigma}(\sqrt[w]{u}) = \sqrt[w]{u}$. Hence $\widetilde{G}$ is an abelian group. This leads to a contradiction. $\square$

In Section 2 we have computed the ramification indices in $\widetilde{K}/K$ of all finite primes of K. To calculate the genus of $\widetilde{K}$, we need to compute those of the infinite primes.

Lemma 3.3. *The infinite primes of* K *are unramified in* $\widetilde{K}/K$.

Proof. 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 [2, Section 4.3], we know $\sin \mathbf{a}_{PQ} \in k_\infty$. 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 $u \in k_\infty$. Thus $u \in K^+$.

Let $E = K^+(\sqrt[w]{u})$. Then $\widetilde{K} = EK$ and $[E : K^+] = w$. Let ∞ be an arbitrary infinite prime of K^+, ∞_1 an infinite prime of K above ∞, ∞_2 an infinite prime of E above ∞, and $\widetilde{\infty}$ an infinite prime of $\widetilde{K}$ above ∞_1. By [5, Theorem 12.14], the ramification index $e(\infty_1/\infty) = w$. Then by Abhyankar's Lemma, see [7, III 8.9], the ramification index $e(\widetilde{\infty}/\infty) = w$. Since $e(\widetilde{\infty}/\infty) = e(\widetilde{\infty}/\infty_1)\cdot e(\infty_1/\infty)$, we have $e(\widetilde{\infty}/\infty_1) = 1$. Thus ∞_1 is unramified in $\widetilde{K}/K$. Since $\widetilde{K}$ is Galois over K, all infinite primes of K are unramified in $\widetilde{K}/K$. $\square$

Now we can get the genus formula of $\widetilde{K}$.

Theorem 3.4. *We have*

$$g_{\widetilde{K}} = 1 + w\left[g_K - 1 + \frac{1}{2}\left(1 - \frac{1}{e_P}\right)d_P\Phi\big(M/P^{r_P}\big) + \frac{1}{2}\left(1 - \frac{1}{e_Q}\right)d_Q\Phi\big(M/Q^{r_Q}\big)\right],$$

where r_P *and* r_Q *are the maximal powers of* P *and* Q *such that* $P^{r_P}|M$ *and* $Q^{r_Q}|M$ *respectively,* $e_P = \frac{w}{\gcd(w, \log_\gamma(\frac{P}{Q}))}$ *and* $e_Q = \frac{w}{\gcd(w, \log_\gamma(\frac{Q}{P}))}$.

Proof. By Hasse's formula, we have

$$g_{\widetilde{K}} = 1 + w\left[g_K - 1 + \frac{1}{2}\sum_{\substack{\text{prime } \mathfrak{p} \text{ in } K\\ \mathfrak{p}|P \text{ or } \mathfrak{p}|Q}} \left(1 - \frac{1}{e_{\mathfrak{p}}}\right)\deg \mathfrak{p}\right],$$

where the sum is over all the inequivalent primes above P or Q, $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ in $\widetilde{K}/K$, and for $\mathfrak{p}|P$, $\deg \mathfrak{p} = f(\mathfrak{p}/P)d_P$, $f(\mathfrak{p}/P)$ is the residue class degree, similarly for $\mathfrak{p}|Q$.

We assume that there are g_P and g_Q different prime ideals in K above P and Q respectively. Then

$$g_{\widetilde{K}} = 1 + w\left[g_K - 1 + \frac{1}{2}\left(1 - \frac{1}{e_P}\right)g_P f_P d_P + \frac{1}{2}\left(1 - \frac{1}{e_Q}\right)g_Q f_Q d_Q\right],$$

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. $\square$

Acknowledgment

We are very grateful to the referee for his careful reading and many valuable suggestions. Especially, we thank him for telling us the genus formula of the cyclotomic function field in [6].

References

[1] S. Bae, E.-U. Gekeler, P. Kang, 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. Goss, Basic Structures of Function Field Arithmetic, Springer-Verlag, 1996.
[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, Grad. Texts in Math., vol. 210, Springer-Verlag, 2002.
[6] G.D.V. Salvador, Topics in the Theory of Algebraic Function Fields, Birkhäuser, 2006.
[7] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.
[8] L. Yin, C. Zhang, Arithmetic of quasi-cyclotomic fields, J. Number Theory 128 (2008) 1717–1730.