GENUS FIELDS OF CYCLIC l–EXTENSIONS OF RATIONAL FUNCTION FIELDS

VÍCTOR BAUTISTA–ANCONA, MARTHA RZEDOWSKI–CALDERÓN, AND GABRIEL VILLA–SALVADOR

Abstract. We give a construction of genus fields for Kummer cyclic l–extensions of rational congruence function fields, l a prime number. First we find this genus field for a field contained in a cyclotomic function field using Leopoldt's construction by means of Dirichlet characters and the Hilbert class field defined by Rosen. The general case follows from this. This generalizes the result obtained by Peng for a cyclic extension of degree l.

1. Introduction

The concept of genus field was defined by Gauss [7] in 1801 in the context of binary quadratic forms. For any finite extension $K/\mathbb{Q}$, the genus field is defined as the maximal unramified extension $K_{\mathfrak{ge}}$ of K such that $K_{\mathfrak{ge}}$ is the composite of K and an abelian extension k^* of $\mathbb{Q}$: $K_{\mathfrak{ge}} = Kk^*$. This definition is due to A. Frölich [6]. If K_H denotes the Hilbert class field of K, $K \subseteq K_{\mathfrak{ge}} \subseteq K_H$. H. Leopoldt [10] determined the genus field $K_{\mathfrak{ge}}$ of an abelian extension K of $\mathbb{Q}$ using Dirichlet characters.

For function fields, the notion of Hilbert class field has no proper analogue since the maximal abelian extension of any congruence function field $K/\mathbb{F}_q$ contains $K_m := K\mathbb{F}_{q^m}$ for all positive integers m and therefore the maximal unramified abelian extension of K is of infinite degree over K.

M. Rosen [14] gave a definition of an analogue of the Hilbert class field for a conguence function field K and a fixed finite nonempty set S_∞ of prime divisors of K. Using this definition, a proper concept of genus field can be given along the lines of the classical case. R. Clement [4] considered a cyclic extension of $\mathbb{F}_q(T)$ of degree a prime number l dividing $q-1$ and found the genus field using class field theory. Later, S. Bae and J. K. Koo [3] generalized the results of Clement following the methods of Frölich [6]. In fact, Bae and Koo defined the genus field for global function fields and developed the analogue of the classical genus theory (see Definition 2.2). B. Anglès and J.-F. Jaulent [1] used narrow S–class groups to establish the fundamental results of genus theory for finite extensions of global fields, where S is an arbitrary finite set of places. Using the genus theory for quadratic function fields, Y. Li and S. Hu [11] obtained an analogue in the function field framework of the number field case by constructing infinitely many real (resp. imaginary) quadratic extensions K over $\mathbb{F}_q(T)$ whose ideal class group capitulates in a proper subfield of the Hilbert class field of K.

Date: January 28th., 2013.

2000 *Mathematics Subject Classification.* Primary 11R60; Secondary 11R29, 11R58.

Key words and phrases. Genus fields, congruence function fields, global fields, Dirichlet characters, cyclotomic function fields, cyclic extensions, Kummer extensions.

G. Peng [13] explicitly described the genus theory for Kummer function fields. C. Wittmann [17] extended Peng's results to the case $l \nmid q(q-1)$ and used them to study the l–part of the ideal class groups of cyclic extensions of prime degree l. Hu and Li [8] described explicitly the ambiguous ideal classes and the genus field of an Artin–Schreier extension of a rational congruence function field. In analogy with the number field case, S. Bae, S. Hu and H. Jung [2] defined the generalized Rédei–matrix of local Hilbert symbols with coefficients in $\mathbb{F}_l$. As applications they determined the generalized Rédei matrices for Kummer, biquadratic and Artin–Schreier extensions of $\mathbb{F}_q(T)$ and showed that their algorithm for finding the invariant λ_2 for Kummer extensions is different and simpler compared to that of Wittmann. They used their results to determine completely the 4–rank of the ideal class group for a large class of Artin–Schreier extensions that have been used in cryptanalysis and which may lead to a possible method of attack against the discrete logarithm problem on an elliptic curve.

In [12] the genus field of a finite geometric abelian extension of $k := \mathbb{F}_q(T)$ was described and as applications the genus fields of cyclic extensions of prime degree over k were found explicitly. The results of Peng and of Hu and Li can be obtained in this way. In that paper were obtained the p–cyclic extensions of k where p is the characteristic.

In this paper we use the results obtained in [12] to describe explicitly the genus field of cyclic extensions of degree l^n where $l^n \mid q-1$. The case $n = 1$ is the result of Peng. Our methods are based on Leopoldt's ideas and therefore are very different from Peng's methods which are based on the global function field analogue of P. E. Conner and J. Hurrelbrink's exact hexagon [5]. In [12] we describe the case $n = 1$ a little differently from how it was described originally. Here we show that using our methods it is possible to give the same description as the one in the original paper.

2. Cyclotomic function fields

First we give some notations and some results in the theory of cyclotomic function fields [16]. Let $k = \mathbb{F}_q(T)$ be a rational congruence function field, $\mathbb{F}_q$ denoting the finite field of q elements. Let $R_T = \mathbb{F}_q[T]$ be the ring of polynomials, that is, we choose R_T as the ring of integers of k. R_T^+ denotes the set of monic irreducible polynomials in R_T. For $N \in R_T \setminus \{0\}$, Λ_N denotes the N–torsion of the Carlitz module and $k(\Lambda_N)$ denotes the N–th cyclotomic function field. For any function field $K/\mathbb{F}_q$, $K_m := K\mathbb{F}_{q^m}$ denotes the constant field extension. For any $m \in \mathbb{N}$, C_m denotes a cyclic group of order m.

We have $G_N := \operatorname{Gal}(k(\Lambda_N)/k) \cong \big(R_T/(N)\big)^*$ with the identification $\sigma_A \lambda_N = \lambda_N^A$ for $A \in R_T$. For any finite extension K/k we will use the symbol $S_\infty(K)$ to denote either one prime or the set of all primes in K above $\mathfrak{p}_\infty$, the pole divisor of T in k. We understand by a *Dirichlet character* any group homomorphism $\chi \colon \big(R_T/(N)\big)^* \to \mathbb{C}^*$ and we define the *conductor* $\mathfrak{f}_\chi$ of χ as the monic polynomial of minimum degree such that χ can be defined modulo $\mathfrak{f}_\chi$, $\chi \colon \big(R_T/(\mathfrak{f}_\chi)\big)^* \to \mathbb{C}^*$.

Given any group of characters $X \subseteq \widehat{G_N} (= \operatorname{Hom}(G_N, \mathbb{C}^*))$, the field associated to X is the subfield of $k(\Lambda_N)$ fixed under $\cap_{\chi \in X} \ker \chi$. Conversely, for any field $K \subseteq k(\Lambda_N)$, the group of Dirichlet characters associated to K is $\widehat{\operatorname{Gal}(K/k)}$.

For any character χ we consider the canonical decomposition $\chi = \prod_{P \in R_T^+} \chi_P$, where χ_P has conductor a power of P. We have $\mathfrak{f}_\chi = \prod_{P \in R_T^+} \mathfrak{f}_{\chi_P}$.

If X is a group of Dirichlet characters, we write $X_P := \{\chi_P \mid \chi \in X\}$ for $P \in R_T^+$. If K is any extension of k, $k \subseteq K \subseteq k(\Lambda_N)$ and $P \in R_T^+$, then the ramification index of P in K is $e_P = |X_P|$.

In $k(\Lambda_N)/k$, $\mathfrak{p}_\infty$ has ramification index $q-1$ and decomposes into $\frac{|G_N|}{q-1}$ different prime divisors of $k(\Lambda_N)$ of degree 1. Furthermore, with the identification $G_N \cong \big(R_T/(N)\big)^*$, the inertia group $\mathfrak{I}$ of $\mathfrak{p}_\infty$ is $\mathbb{F}_q^* \subseteq \big(R_T/(N)\big)^*$, more precisely, $\mathfrak{I} = \{\sigma_a \mid a \in \mathbb{F}_q^*\}$. In this case the inertia and the decomposition groups coincide. The primes that ramify in $k(\Lambda_N)/k$ are $\mathfrak{p}_\infty$ and the polynomials $P \in R_T^+$ such that $P \mid N$.

We recall Rosen's definition for a relative Hilbert class field of a congruence function field K.

Definition 2.1 ([14])**.** Let K be a function field with field of constants $\mathbb{F}_q$. Let S be a nonempty finite set of prime divisors of K. The *Hilbert class function field of K relative to S*, $K_{H,S}$, is the maximal unramified abelian extension of K where every element of S decomposes fully.

From now on, for any finite extension K of k we will consider S as the set of prime divisors dividing $\mathfrak{p}_\infty$, the pole divisor of T in k and we write K_H instead of $K_{H,S}$.

Definition 2.2. Let K be a finite geometric extension of k. The *genus field* $K_{\mathfrak{ge}}$ of K is the maximal extension of K contained in K_H that is the composite of K and an abelian extension of k. Equivalently, $K_{\mathfrak{ge}} = Kk^*$ where k^* is the maximal abelian extension of k contained in K_H.

When K/k is an abelian extension, $K_{\mathfrak{ge}}$ is the maximal abelian extension of k contained in K_H. Our main goal in this section is to find $K_{\mathfrak{ge}}$ when K/k is a cyclic extension of degree l^n where $l^n \mid q-1$ and K is a subfield of a cyclotomic function field.

Proposition 2.3. *If $K \subseteq k(\Lambda_N)$ and the group of characters associated to K is X, then the maximal abelian extension J of K unramified at every finite prime $P \in R_T^+$, contained in a cyclotomic extension, is the field associated to $Y = \prod_{P \in R_T^+} X_P = \prod_{P \mid N} X_P$.*

Proof. [12, Proposition 3.3]. □

In this case $\mathfrak{p}_\infty$ has no inertia in J/K but it might be ramified.

Proposition 2.4. *If E/k is an abelian extension such that $\mathfrak{p}_\infty$ is tamely ramified, then there exist $N \in R_T$ and $m \in \mathbb{N}$ such that $E \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$.*

Proof. [12, Proposition 3.4]. □

Theorem 2.5. *Assume $K \subseteq k(\Lambda_N)$ for some polynomial N. Let X be the group of Dirichlet characters associated to K, $Y = \prod_{P \mid N} X_P$, $Y_1 = \{\chi \in Y \mid \chi(a) = 1$ for all $a \in \mathbb{F}_q^*\}$ and J_1 the field associated to Y_1. Then the genus field of K is $K_{\mathfrak{ge}} = KJ_1$.*

Proof. [12, Theorem 3.6]. □

Now we consider K/k a cyclic geometric extension of degree l^n where l is a prime number and such that $l^n \mid q-1$. Therefore K/k is a Kummer extension and then

$K = k(\sqrt[l^n]{\gamma D})$ where $\gamma \in \mathbb{F}_q^*$ and $D \in R_T$ is a monic polynomial l^n–power free. If $K \subseteq k(\Lambda_N)$ for some $N \in R_T$, we have $K = k(\sqrt[l^n]{(-1)^{\deg D} D})$ ([15]). For the convenience of the reader we present a proof of this fact.

Here we will assume that $q \geq 3$. First we want to know when a field $k(\sqrt[l^n]{P})$, where $l^n \mid q-1$ and $P \in R_T^+$, is contained in $k(\Lambda_P)$. The Galois group $\operatorname{Gal}(k(\Lambda_P)/k) \cong \big(R_T/(P)\big)^* \cong \mathbb{F}_{q^d}^*$ is a cyclic group of order $q^d - 1$, where d is the degree of P. Therefore there exists a unique extension of the form $k(\sqrt[l^n]{\alpha P})$, $\alpha \in \mathbb{F}_q^*$, contained in $k(\Lambda_P)$. Note that if $\alpha \notin \big(\mathbb{F}_q^*\big)^{l^n}$, $k(\sqrt[l^n]{P}) \neq k(\sqrt[l^n]{\alpha P})$ since otherwise $\sqrt[l^n]{\alpha} \in k$ and so $\alpha \in \big(\mathbb{F}_q^*\big)^{l^n}$.

Proposition 2.6. *For $P \in R_T^+$, $k(\sqrt[l^n]{(-1)^d P}) \subseteq k(\Lambda_P)$.*

Proof. Let $\Phi_P(u) = \frac{u^P}{u}$ be the P–th cyclotomic polynomial. We have

$$\Phi_P(u) = \prod_{\substack{A\neq 0, A\in R_T\\ \deg A<\deg P}} (u - \lambda^A) = \sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} u^{q^i - 1},$$

where $\lambda \in \Lambda_P \setminus \{0\}$, that is, λ is an R_T–generator of Λ_P. Then

$$\Phi_P(0) = (-1)^{q^d-1} \prod_{\substack{A\neq 0, A\in R_T\\ \deg A<\deg P}} \lambda^A = P.$$

Now, every polynomial $A \in R_T$, $A \neq 0$ can be uniquely written as a product of an element $\alpha \in \mathbb{F}_q^*$ and a monic polynomial A_1: $A = \alpha A_1$. Now, $\lambda^A = \lambda^{\alpha A_1} = \alpha \lambda^A$. Note that there are exactly $q-1$ polynomials $A \in R_T$, $A \neq 0$ such that A_1 occurs in its factorization as above, one for each of the $q-1$ elements of $\mathbb{F}_q^*$. Therefore

$$\begin{aligned} P = (-1)^{q^d-1} \prod_{\substack{A\neq 0, A\in R_T\\ \deg A<\deg P}} \lambda^A &= (-1)^{q^d-1} \prod_{\substack{A_1 \text{ monic}\\ \alpha\in\mathbb{F}_q^*}} \alpha\lambda^{A_1} \\ &= (-1)^{q^d-1} \Big(\prod_{\alpha\in\mathbb{F}_q^*} \alpha\Big)^{\frac{q^d-1}{q-1}} \Big(\prod_{A_1 \text{ monic}} \lambda^{A_1}\Big)^{q-1}. \end{aligned}$$

Note that $\prod_{\alpha\in\mathbb{F}_q^*} \alpha = -1$ and that $\xi := \prod_{A_1 \text{ monic}} \lambda^{A_1} \in k(\Lambda_P)$. Thus

$$(-1)^{q^d-1}(-1)^{(q^d-1)/(q-1)} \xi^{q-1} = (-1)^d \xi^{q-1} = P,$$

with $\xi \in k(\Lambda_P)$. It follows that $\xi = \sqrt[q-1]{(-1)^d P} \in k(\Lambda_P)$. In particular $\sqrt[l^n]{(-1)^d P} = \xi^{(q-1)/l^n} \in k(\Lambda_P)$. $\square$

Corollary 2.7. *For any monic polynomial $D \in R_T$, we have $k(\sqrt[l^n]{(-1)^{\deg D} D}) \subseteq k(\Lambda_D)$.* $\square$

Next, we study the behavior of $\mathfrak{p}_\infty$ in K/k.

Proposition 2.8. *Let $K = k(\sqrt[l^n]{\gamma D})$ where $\gamma \in \mathbb{F}_q^*$ and $D \in R_T$ is a monic polynomial l^n–power free. Then if e_∞, f_∞ and h_∞ denote the ramification index, the inertia degree and the decomposition index of $\mathfrak{p}_\infty$ respectively in K/k, then*

$$e_\infty = l^{n-t}, \quad f_\infty = l^m, \quad \text{and} \quad h_\infty = l^{t-m},$$

where $\deg D = l^{t'} a$ *with* $\gcd(a, l) = 1$, $t = \min\{n, t'\}$ *and* $\mathbb{F}_q(\sqrt[l^t]{(-1)^{\deg D}\gamma}) = \mathbb{F}_{q^{l^m}}$.

Proof. The computation of the ramification index is due to Hasse (see [16, Theorem 5.8.12]).

By Corollary 2.7 we have that $\mathfrak{p}_\infty$ decomposes fully in $k(\sqrt[l^t]{(-1)^{\deg D}D}) \subseteq k(\Lambda_D)$, and $\mathfrak{p}_\infty$ is fully inert in $k\mathbb{F}_{q^{l^m}}/k$ since $\mathfrak{p}_\infty$ is of degree one (see [16, Theorem 6.2.1]). Therefore the inertia degree of $\mathfrak{p}_\infty$ in $k(\sqrt[l^t]{D})\mathbb{F}_{q^{l^m}}/k$ is l^m. It follows that $k(\sqrt[l^t]{(-1)^{\deg D}D})$ is the inertia field of $\mathfrak{p}_\infty$ in $k(\sqrt[l^t]{D})\mathbb{F}_{q^{l^m}}/k$. Therefore $\mathfrak{p}_\infty$ is fully decomposed in $k(\sqrt[l^t]{\gamma D})\mathbb{F}_{q^{l^m}}/k(\sqrt[l^t]{\gamma D})$:

$$\begin{tikzcd}
k(\sqrt[l^t]{\gamma D}) \arrow[r, dash] \arrow[d, dash, "l^t"'] & k(\sqrt[l^t]{\gamma D})\mathbb{F}_{q^{l^m}} = k(\sqrt[l^t]{\gamma D})k(\sqrt[l^t]{(-1)^{\deg D}D}) \arrow[d, dash] \\
k \arrow[r, dash, "l^t", "\substack{\mathfrak{p}_\infty\ \text{totally} \\ \text{decomposed}}"'] & k(\sqrt[l^t]{(-1)^{\deg D}D})
\end{tikzcd}$$

Therefore $f_\infty = l^m$. The result follows. □

3. The case $n = 1$

The case $n = 1$ is due to Peng [13]. In [12] we gave another proof of the result of Peng with the techniques developed there. The description for the genus field in [12] is different from that given in [13]. In this section we obtain the same description as in the original paper.

We will use that for any $\alpha \in \mathbb{F}_q^*$ and $1 \le e \le l-1$, we have $k(\sqrt[l]{\alpha P^e}) = k(\sqrt[l]{\alpha^f P})$ where $fe \equiv 1 \bmod l$. Since we have l classes $\bmod (\mathbb{F}_q^*)^l$ in $\mathbb{F}_q^*$, the l different fields $k(\sqrt[l]{\alpha P})$, $\alpha \in \mathbb{F}_q^*$ are given by the classes $\bmod (\mathbb{F}_q^*)^l$. Therefore $k(\sqrt[l]{\alpha^f P}) \subseteq k(\Lambda_P)$ if and only if $\alpha^f \equiv (-1)^d \bmod (\mathbb{F}_q^*)^l$.

Here we have that $K := k(\sqrt[l]{\gamma D}) \subseteq k(\Lambda_D)\mathbb{F}_{q^l}$ with $D \in R_T$ a monic l–power free polynomial, $\gamma \in \mathbb{F}_q^*$ and $D = P_1^{e_1} \cdots P_r^{e_r}$ where $P_i \in R_T^+$, $1 \le e_i \le l-1$, $1 \le i \le r$. Furthermore we arrange the product so that $l \mid \deg P_i$ for $1 \le i \le s$ and $l \nmid \deg P_j$ for $s+1 \le j \le r$, $0 \le s \le r$. We have $\mathbb{F}_q^* \subseteq (\mathbb{F}_{q^l}^*)^l$. Fix $\varepsilon \in \mathbb{F}_{q^l} \setminus \mathbb{F}_q$.

First,

Proposition 3.1. *The behavior of $\mathfrak{p}_\infty$ in K/k is the following:*

(a).- *If $l \nmid \deg D$, $\mathfrak{p}_\infty$ is ramified.*
(b).- *If $l \mid \deg D$ and $\gamma \in (\mathbb{F}_q^*)^l$, $\mathfrak{p}_\infty$ decomposes.*
(c).- *If $l \mid \deg D$ and $\gamma \notin (\mathbb{F}_q^*)^l$, $\mathfrak{p}_\infty$ is inert.*

Proof. This is a particular case of Proposition 2.8. □

Now by [12, Remark 4.3], we have $[K_{\mathfrak{ge}} : K] = [E_{\mathfrak{ge}} : E]t$, where

$$t = \deg S_\infty(K) = \begin{cases} 1 & \text{if } \mathfrak{p}_\infty \text{ is not inert in } K/k \\ l & \text{if } \mathfrak{p}_\infty \text{ is inert in } K/k \end{cases}$$

and $E := K\mathbb{F}_{q^l} \cap k(\Lambda_D) = k(\sqrt[l]{(-1)^{\deg D}D})$.

When $K = E$, that is, when $K \subseteq k(\Lambda_D)$, if χ is the character of order l associated to K, $\chi = \chi_{P_1} \cdots \chi_{P_r}$, we consider $Y = \langle \chi_{P_i} \mid 1 \le i \le r \rangle$. The field associated to Y is $F = k(\sqrt[l]{(-1)^{\deg P_1}P_1}, \ldots, \sqrt[l]{(-1)^{\deg P_r}P_r})$, and $K_{\mathfrak{ge}} = F$ if $l \nmid \deg D$ or if $l \mid \deg P_i$ for all i (that is, $s = r$). This is because in the first case $\mathfrak{p}_\infty$ is already ramified in K and in the second $\mathfrak{p}_\infty$ is unramified in F/k.

When $l \mid \deg D$ and $l \nmid \deg P_r$, $\mathfrak{p}_\infty$ ramifies in F/k and is unramified in K/k. In this case $[F : E_{\mathfrak{ge}}] = l$. Let $a_{s+1}, \ldots, a_{r-1} \in \mathbb{Z}$ be such that $l \mid \deg(P_j P_r^{a_j})$, that is, $\deg P_j + a_j \deg P_r \equiv 0 \bmod l$, $s+1 \leq j \leq r-1$. Let

$$F_1 := k\big(\sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}}\big).$$

Then $S_\infty(E)$ decomposes in F_1/E, $K \subseteq F_1 \subseteq E_{\mathfrak{ge}}$ and $[F : F_1] = l$. It follows that $E_{\mathfrak{ge}} = F_1$.

We obtain

Proposition 3.2. *When $K \subseteq k(\Lambda_D)$, we have $K_{\mathfrak{ge},l} = E_{\mathfrak{ge},l} =$*

(a).- $k\big(\sqrt[l]{\varepsilon}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r}\big)$ *if $l \nmid \deg D$ or if $l \mid \deg P_i$ for all $1 \leq i \leq r$,*

(b).- $k\big(\sqrt[l]{\varepsilon}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}}\big)$, *where the exponent a_j satisfies $\deg P_j + a_j \deg P_r \equiv 0 \bmod l$, $s+1 \leq j \leq r-1$, if $l \mid \deg D$ and $l \nmid \deg P_r$.* □

Now we consider a general K.

Remark 3.3. In any case, for all $1 \leq i \leq r$ and for every $a \in \mathbb{F}_q^*$, the extension $k(\sqrt[l]{\gamma D}, \sqrt[l]{aP_i})/k(\sqrt[l]{\gamma D})$ is unramified at every finite prime. This follows from the fact that $\mathrm{Gal}(k(\sqrt[l]{\gamma D}, \sqrt[l]{aP_i})/k) \cong C_l \times C_l$ and we have tame ramification. Therefore the inertia group of any prime divisor is $\{1\}$ or C_l. On the other hand the only finite prime divisors ramified in $k(\sqrt[l]{\gamma D}, \sqrt[l]{aP_i})/k)$ are P_i, $1 \leq i \leq r$ and they are already ramified in $k(\sqrt[l]{\gamma D})/k$.

Let $\mathfrak{D}$ be the decomposition group of $S_\infty(K)$ in $K_{\mathfrak{ge},l}/K$. Then $K_{\mathfrak{ge}} = K_{\mathfrak{ge},l}^{\mathfrak{D}}$ ([12, Theorem 4.2]).

Case 1: If $l \nmid \deg D$, then $\mathfrak{p}_\infty$ ramifies in K/k and $S_\infty(K)$ is inert in $K_{\mathfrak{ge},l}/K$. If $K = E$, the inertia of $S_\infty(K)$ occurs in $E_{\mathfrak{ge},l}/E_{\mathfrak{ge}}$, so that $\mathfrak{D} = \mathrm{Gal}(E_{\mathfrak{ge},l}/E_{\mathfrak{ge}})$ and by Proposition 3.2, $K_{\mathfrak{ge}} = E_{\mathfrak{ge}} = E_{\mathfrak{ge},l}^{\mathfrak{D}} = k\big(\sqrt[l]{(-1)^{\deg P_1}P_1}, \ldots, \sqrt[l]{(-1)^{\deg P_r}P_r}\big) = k\big(\sqrt[l]{\gamma D}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r}\big)$.

If $K \neq E$, $K_{\mathfrak{ge}} = K_{\mathfrak{ge},l}^{\mathfrak{D}}$ and $[K_{\mathfrak{ge},l} : K_{\mathfrak{ge}}] = l$. If $l \mid \deg P_i$, $\mathfrak{p}_\infty$ decomposes in $k(\sqrt[l]{P_i}/k$. It follows that $\mathfrak{p}_\infty$ is not inert. Therefore in this case $k(\sqrt[l]{\gamma D}, \sqrt[l]{P_i}) \subseteq K_{\mathfrak{ge}}$. Thus $k\big(\sqrt[l]{\gamma D}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}\big) \subseteq K_{\mathfrak{ge}}$.

For $s+1 \leq j \leq r-1$, $l \nmid \deg P_j$. Then $\mathfrak{p}_\infty$ ramifies both in $k(\sqrt[l]{\gamma D})/k$ and in $k(\sqrt[l]{\beta_j P_j})/k$ for $\beta_j \in \mathbb{F}_q^*$. Then $\mathfrak{p}_\infty$ ramifies in all but one subextension of degree l over k of $k(\sqrt[l]{\gamma D}, \sqrt[l]{\beta_j P_j})/k$. The only subextension where $\mathfrak{p}_\infty$ is unramified is $k\big(\sqrt[l]{\gamma\beta_j^{-c_j} D P_j^{-c_j}}\big)$ with c_j such that $\deg DP_j^{-c_j} = \deg D - c_j \deg P_j \equiv 0 \bmod l$. In order that $\mathfrak{p}_\infty$ decompose in this last extension it is necessary that $\gamma\beta_j^{-c_j} \in (\mathbb{F}_q^*)^l$. Thus, let $\beta_j := \gamma^{b_j}$ be such that $1 - c_j b_j \equiv 0 \bmod l$. That is, $b_j \equiv c_j^{-1} \bmod l$.

It follows that $F_1 = k\big(\sqrt[l]{\gamma D}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{\gamma^{b_{s+1}}P_{s+1}}, \ldots, \sqrt[l]{\gamma^{b_{r-1}}P_{r-1}}\big) \subseteq K_{\mathfrak{ge}}$ and $[K_{\mathfrak{ge},l} : F_1] = l$. We obtain that $K_{\mathfrak{ge}} = F_1$.

Case 2 Now we consider the case $l \mid \deg P_i$ for all $1 \leq i \leq r$. If $K = E \subseteq k(\Lambda_D)$, $K_{\mathfrak{ge}} = k(\sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r}) = k\big(\sqrt[l]{\gamma}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r}\big)$.

If $K \neq E$, $K_{\mathfrak{ge}} = K_{\mathfrak{ge},l} = E_{\mathfrak{ge},l} = k\big(\sqrt[l]{\varepsilon}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r}\big) = k\big(\sqrt[l]{\gamma}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r}\big)$.

Case 3 Let $l \mid \deg D$, $l \nmid \deg P_r$. If $K = E$ then

$$K_{\mathfrak{ge}} = k\big(\sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}}\big)$$

with $\deg P_j + a_j \deg P_r \equiv 0 \bmod l$, $s+1 \leq j \leq r-1$.

If $K \neq E$, $K_{\mathfrak{ge},l} = K_{\mathfrak{ge}} = k\big(\sqrt[l]{\varepsilon}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}}\big) = k\big(\sqrt[l]{\gamma}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}}\big)$.

We have obtained the result of Peng:

Theorem 3.4 (G. Peng [13]). *Let $D = P_1^{e_1} \cdots P_r^{e_r} \in R_T$ be a monic l–power free polynomial, where $P_i \in R_T^+$, $1 \leq e_i \leq l-1$, $1 \leq i \leq r$. Let $0 \leq s \leq r$ be such that $l \mid \deg P_i$ for $1 \leq i \leq s$ and $l \nmid \deg P_j$ for $s+1 \leq j \leq r$. Let $K := k(\sqrt[l]{\gamma D})$ where $\gamma \in \mathbb{F}_q^*$. Let a_j, b_j, c_j be defined such that: $\deg P_i + a_i \deg P_r \equiv 0 \bmod l$, $\deg D - c_j \deg P_j \equiv 0 \bmod l$ and $b_j \equiv c_j^{-1} \bmod l$, $s+1 \leq j \leq r$. Then $K_{\mathfrak{ge}}$ is given by:*

(a).- $k\big(\sqrt[l]{\gamma}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r}\big)$ *if $l \mid \deg P_r$.*

(b).- $k\big(\sqrt[l]{\gamma}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}}\big)$ *when $l \mid \deg D$ and $l \nmid \deg P_r$.*

(c).- $k\big(\sqrt[l]{\gamma D}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{\gamma^{b_{s+1}} P_{s+1}}, \ldots, \sqrt[l]{\gamma^{b_{r-1}} P_{r-1}}\big)$ *if $l \nmid \deg D$.* $\square$

4. Cyclic extensions of degree l^n

First we assume $K = k\big(\sqrt[l^n]{\gamma D}\big) \subseteq k(\Lambda_N)$ for some $N \in R_T$. Let $D = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, $1 \leq \alpha_i \leq l^n - 1$, $1 \leq i \leq r$, with $P_1, \ldots, P_r \in R_T^+$. Let $\alpha_i = l^{a_i} c_i$, $\gcd(l, c_i) = 1$, $1 \leq i \leq r$, $0 \leq a_i \leq n-1$. Since K/k is geometric, we have that at least one a_i must be 0. Let χ_D be the Dirichlet character associated to $E := k\big(\sqrt[l^n]{(-1)^{\deg D} D}\big)$. Then χ_{P_i} is the character associated to $E_i = k\big(\sqrt[l^{n-a_i}]{(-1)^{\deg P_i} P_i}\big)$ since

$$\sqrt[l^n]{(-1)^{\deg P_i^{\alpha_i}} P_i^{\alpha_i}} = \sqrt[l^n]{(-1)^{l^{a_i} c_i \deg P_i} P_i^{l^{a_i} c_i}} = \sqrt[l^{n-a_i}]{(-1)^{\deg P_i^{c_i}} P_i^{c_i}}$$

and

$$k\big(\sqrt[l^{n-a_i}]{(-1)^{\deg P_i^{c_i}} P_i^{c_i}}\big) = k\big(\sqrt[l^{n-a_i}]{(-1)^{\deg P_i} P_i}\big).$$

Therefore $M := E_1 \cdots E_r$ is the maximal abelian extension of E unramified at every finite prime.

Now the ramification index of $\mathfrak{p}_\infty$ in E/k is l^{n-t} where $\deg D = l^{t'} s$, $\gcd(l, s) = 1$ and $t = \min\{n, t'\}$. Let $\deg P_i = l^{b_i'} d_i$, $\gcd(d_i, l) = 1$ and let $b_i := \min\{n - a_i, b_i'\}$. Then $\mathfrak{p}_\infty$ has ramification index $l^{n-a_i-b_i}$ in E_i/k. We have

$$l^{t'} s = \deg D = \sum_{i=1}^r \alpha_i \deg P_i = \sum_{i=1}^r l^{a_i} c_i l^{b_i'} d_i = \sum_{i=1}^r l^{a_i + b_i'}(c_i d_i), \tag{4.1}$$

and $\alpha_i \deg P_i = l^{a_i + b_i'} c_i d_i \leq \deg D = l^{t'} s$.

From Abhyankar Lemma ([16, Theorem 12.4.4]), we have that the ramification index of $\mathfrak{p}_\infty$ in M/k is $\operatorname{lcm}\big[l^{n-a_1-b_1}, \cdots, l^{n-a_r-b_r}\big] = l^{n-a_0-b_0}$ where $a_0 + b_0 = \min\{a_i + b_i \mid 1 \leq i \leq r\}$. We may order the product $P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ so that $a_1 + b_1 \leq a_2 + b_2 \leq \cdots \leq a_r + b_r$ and therefore we may assume $a_0 + b_0 = a_1 + b_1$. Since $E \subseteq M$, we have that $l^{n-t} \leq l^{n-a_i-b_i}$ for some i, that is, $a_1 + b_1 \leq t$.

We have

$$M = k\big(\sqrt[l^{n-a_1}]{(-1)^{\deg P_1} P_1}, \sqrt[l^{n-a_2}]{(-1)^{\deg P_2} P_2}, \ldots, \sqrt[l^{n-a_r}]{(-1)^{\deg P_r} P_r}\big)$$

and the ramification index of $S_\infty(E)$ in M/E is $\frac{l^{n-a_1-b_1}}{l^{n-t}} = l^{t-a_1-b_1}$. Let $E_{\mathfrak{ge}}$ be the genus field of E. Then $E \subseteq E_{\mathfrak{ge}} \subseteq M$ and $[M : E_{\mathfrak{ge}}] = l^{t-a_1-b_1} = |D(S_\infty(E))|$

where $D(S_\infty(E))$ denotes the decomposition group of $S_\infty(E)$ in $M/E_{\mathfrak{ge}}$. Now $E_i = k\big(\sqrt[l^{n-a_i}]{(-1)^{\deg P_i} P_i}\big) = k\big(\sqrt[l^n]{(-1)^{\deg P_i^{l^{a_i}}} P_i^{l^{a_i}}}\big)$, $1 \le i \le r$.

We have $a_1 + b_1 \le t$. If $a_1 + b_1 = t$, then $M = E_{\mathfrak{ge}}$.

Note that if $a_i + b_i < t$, then $b_i < t - a_i \le n - a_i$. Hence $b_i' = b_i$ in this case.

If $a_1 + b_1 < t \le t'$, from (4.1) we obtain

$$l^{t'} s = l^{a_1+b_1}\big(\sum_{i=1}^{r} l^{a_i + b_i' - a_1 - b_1} c_i d_i\big).$$

Hence, $a_1 + b_1 = a_2 + b_2$. That is, the minimum value of $\{a_i + b_i \mid 1 \le i \le r\}$ is achieved at least twice.

Let u be such that $a_u + b_u < t \le a_{u+1} + b_{u+1}$. We assume $u \ge 2$.

We define E_i' as follows. If $l^{n-a_i-b_i} \le l^{n-t}$, equivalently if $t \le a_i + b_i$, then $E_i' = E_i$ since the ramification index of $\mathfrak{p}_\infty$ in E_i/k is less than or equal to l^{n-t}. In other words, $E_i' = E_i$, for $u + 1 \le i \le r$.

For $2 \le i \le u$, we define E_i' as follows. We consider the special case $b_1 = \min\{b_i \mid 1 \le i \le u\}$. Let

$$E_i' = k\Big(\sqrt[l^{n-a_i}]{(-1)^{\deg P_i P_1^{x_i}} P_i P_1^{x_i}}\Big) \tag{4.2}$$

be such that

$$\deg\big(P_i P_1^{x_i}\big) = \deg P_i + x_i \deg P_1 = l^{b_1+m_i} y_i,$$

where $n - a_i - (b_1 + m_i) = n - t$ and $\gcd(y_i, l) = 1$. That is we choose x_i such that the ramification index of $\mathfrak{p}_\infty$ in E_i'/k is l^{n-t}. We will see that this is always possible. Recall that $b_i = b_i'$ in this case.

Remark 4.1. We will use the following elementary fact. Let l be a prime number, $m \in \mathbb{N}$ and let $d_1, d_i \in \mathbb{N}$ be relatively prime to l: $\gcd(d_1, l) = \gcd(d_i, l) = 1$. Then there exist $y_i, z_i \in \mathbb{N}$ such that $\gcd(y_i, l) = 1$ and $y_i l^m - z_i d_1 = d_i$.

We have

$$\big(P_i P_1^{x_i}\big) = \deg P_i + x_i \deg P_1 = l^{b_i} d_i + x_i l^{b_1} d_1 = l^{b_1}\big(l^{b_i - b_1} d_i + x_i d_1\big).$$

Therefore we need x_i such that

$$l^{b_i-b_1} d_i + x_i d_1 = l^{m_i} y_i$$

with $n - a_i - (b_1 + m_i) = n - t$, equivalently, $m_i = t - a_i - b_1$, and $\gcd(y_i, l) = 1$. Note that $m_i = t - a_i - b_1 = t - a_i - b_i + (b_i - b_1) \ge t - a_i - b_i > 0$.

Let $x_i := l^{b_i - b_1} z_i$ for some z_i, that is,

$$l^{b_i-b_1} d_i + l^{b_i-b_1} z_i d_1 = l^{m_i} y_i.$$

Therefore, we need $z_i, y_i \in \mathbb{Z}$ such that $\gcd(y_i, l) = 1$ and

$$d_i + z_i d_1 = l^{m_i - b_i + b_1} y_i. \tag{4.3}$$

Since $m_i - b_i + b_1 = (t - a_i - b_1) - b_i + b_1 = t - a_i - b_i > 0$, and $\gcd(d_i, l) = 1$, it follows, by Remark 4.1, that there exist $z_i, y_i \in \mathbb{N}$ with $\gcd(y_i, l) = 1$ satisfying (4.3). Note that $\gcd(z_i, l) = 1$.

In short, let $x_i = l^{b_i-b_1} z_i \in \mathbb{N}$ be such that $E_i' = k\Big(\sqrt[l^{n-a_i}]{(-1)^{\deg P_i P_1^{x_i}} P_i P_1^{x_i}}\Big)$ and the ramification index of $\mathfrak{p}_\infty$ in E_i'/k is l^{n-t}.

Finally let $E_1'=k\big(\sqrt[l^{n-a_1}]{(-1)^{\deg P_1^w}P_1^w}\big)$ where we choose $w\in\mathbb{N}\cup\{0\}$ such that $E\subseteq M_1:=E_1'E_2'\cdots E_u'E_{u+1}\cdots E_r=E_{\mathfrak{ge}}$. We will prove that this is possible. Let

$$\xi_i:=\begin{cases}\pm P_1^w & \text{if } i=1,\\ \pm P_iP_1^{x_i} & \text{if } 2\le i\le u,\\ \pm P_i & \text{if } u+1\le i\le r,\end{cases}$$

where the sign $\pm$ is chosen to be $(-1)^{\deg Q}$, where $Q=P_1, P_iP_1^{x_i}$ or P_i respectively.

We have

$$\begin{aligned}\prod_{i=1}^r\big(\xi_i^{l^{a_i}}\big)^{c_i}&=\pm\Big[\prod_{i=2}^r P_i^{l^{a_i}c_i}\cdot\prod_{i=2}^u P_1^{l^{a_i}c_ix_i}\Big]P_1^{l^{a_1}c_1w}\\ &=\pm\prod_{i=2}^r P_i^{\alpha_i}\cdot P_1^{w'}=\pm\frac{D}{P_1^{\alpha_1}}P_1^{w'}=\pm DP_1^{w'-\alpha_1},\end{aligned}\tag{4.4}$$

where

$$w'=\sum_{i=2}^u l^{a_i}c_ix_i+l^{a_1}c_1w.\tag{4.5}$$

We want w' to be chosen so that $\prod_{i=1}^r\big(\xi_i^{l^{a_i}}\big)^{c_i}\in M_1^{l^n}$.

Using (4.1), (4.3), that $b_1\le b_i$ and $b_i=b_i'$ for $1\le i\le u$, and that $t\le t'$, we obtain

$$w'=l^{a_1}c_1(w+1)+l^{t-b_1}d_1^{-1}\Big(\sum_{i=2}^u c_iy_i-l^{t'-t}s+\sum_{i=u+1}^r l^{a_i+b_i'-t}c_id_i\Big).\tag{4.6}$$

From (4.4) we have that $E\subseteq M_1$ if $w'\equiv\alpha_1 \bmod l^n$. From (4.6) we have that $w'\equiv\alpha_1\bmod l^n$ iff there exists $\kappa\in\mathbb{Z}$ such that

$$\kappa l^{n-a_1}-c_1w=d_1^{-1}l^{t-a_1-b_1}\Big(\sum_{i=2}^u c_iy_i-l^{t'-t}s+\sum_{i=u+1}^r l^{a_i+b_i'-t}c_id_i\Big).\tag{4.7}$$

Since $\gcd(c_1,l)=1$, $n-a_1>0$ and $d_1\mid\sum_{i=2}^u c_iy_i-l^{t'-t}s+\sum_{i=u+1}^r l^{a_i+b_i'-t}c_id_i$, it follows that (4.7) can be solved for $\kappa,w\in\mathbb{N}$. Observe that $l^{t-a_1-b_1}\mid w$, that is, $w=l^{t-a_1-b_1}\rho$ for some $\rho\in\mathbb{N}$. With this w we obtain $E\subseteq E_1'\cdots E_u'E_{u+1}\cdots E_r=M_1$.

We have $\deg P_1^w=w\deg P_1=l^{t-a_1-b_1}\rho l^{b_1}d_1=l^{t-a_1}\rho d_1$. It follows that the ramification index of $\mathfrak{p}_\infty$ in E_1' is $\le l^{n-a_1-(t-a_1)}=l^{n-t}$. Therefore $M_1\subseteq E_{\mathfrak{ge}}$.

To show that $M_1=E_{\mathfrak{ge}}$, we let $\mu_i:=\sqrt[l^{n-a_i}]{(-1)^{\deg P_i}P_i}$, $1\le i\le r$. We have $M=k(\mu_1,\dots,\mu_r)$. Now

$$\begin{aligned}\sqrt[l^{n-a_i}]{(-1)^{\deg P_1^{x_i}}P_1^{x_i}}&=\sqrt[l^{n-a_i}]{(-1)^{\deg P_1^{x_i}}P_1^{l^{b_i-b_1}z_i}}\\ &=\sqrt[l^{n-a_1}]{(-1)^{\deg P_1^{l^{b_i-b_1+a_i-a_1}z_i}}P_1^{l^{b_i-b_1+a_i-a_1}z_i}},\end{aligned}$$

that is

$$\sqrt[l^{n-a_i}]{(-1)^{\deg P_1^{x_i}}P_1^{x_i}}=\mu_1^{l^{(a_i+b_i)-(a_1+b_1)}z_i}$$

for $2\le i\le u$.

Therefore, since $w = l^{t-(a_1+b_1)}\rho$,

(4.8)

$$M_1 = k\big(\mu_1^{l^{t-(a_1+b_1)}\rho}, \mu_2\mu_1^{l^{(a_i+b_i)-(a_1+b_1)}z_2}, \cdots, \mu_u\mu_1^{l^{(a_u+b_u)-(a_1+b_1)}z_u}, \mu_{u+1}\cdots, \mu_r\big).$$

Finally, $M = M_1[\mu_1]$ and since $(a_i+b_i)-(a_1+b_1) < t-(a_1+b_1)$, it follows that $\mu_1^{l^{t-(a_1+b_1)}} \in M_1$. In particular $[M : M_1] \leq l^{t-(a_1+b_1)} = [M : E_{\mathfrak{ge}}]$. Since $M_1 \subseteq E_{\mathfrak{ge}}$ we obtain $M_1 = E_{\mathfrak{ge}}$.

In the general case $K = k\big(\sqrt[l^n]{\gamma D}\big)$, we use the following result proved in [12, Theorem 4.2]. We present the proof for the convenience of the reader.

Theorem 4.2. *Let K/k be any abelian finite geometric tamely ramified extension. Then $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$ for some $N \in R_T$ and $m \in \mathbb{N}$. Let $E = k(\Lambda_N) \cap K\mathbb{F}_{q^m}$. Then $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$.*

Proof. We have $E \cap K = E_{\mathfrak{ge}} \cap K = k(\Lambda_N) \cap K$. Therefore $E_m \subseteq K_m$ and since $[K_m : k] = [E - m : k]$ it follows that $E_m = K_m$.

$$\begin{tikzcd}
k(\Lambda_N) \arrow[rrr, dash] \arrow[d, dash] & & & k(\Lambda_N)\mathbb{F}_{q^m} \arrow[d, dash] \\
C \arrow[rrr, dash] \arrow[dd, dash] & & & K_{\mathfrak{ge},m} \arrow[dd, dash] \\
& & K_{\mathfrak{ge}} \arrow[ur, dash] \arrow[dl, dash] & \\
E_{\mathfrak{ge}} \arrow[r, dash] \arrow[d, dash] & E_{\mathfrak{ge}}K \arrow[rr, dash] \arrow[dd, dash] & & E_{\mathfrak{ge},m} \arrow[d, dash] \\
E \arrow[rrr, dash] \arrow[dd, dash] & & & E\mathbb{F}_{q^m} = K\mathbb{F}_{q^m} \arrow[dd, dash] \\
& K \arrow[urr, dash] & & \\
k \arrow[rrr, dash] \arrow[ur, dash] & & & k\mathbb{F}_{q^m}
\end{tikzcd}$$

Since $K\mathbb{F}_{q^m}/K$ and $E_{\mathfrak{ge}}/E$ are unramified, we obtain that $E_{\mathfrak{ge}}K/K$ is unramified. Also, because $S_\infty(E)$ decomposes fully in $E_{\mathfrak{ge}}$, $S_\infty(EK)$ decomposes fully in $E_{\mathfrak{ge}}K$. Now, $S_\infty(E\cap K)$ has inertia degree one in $E/E\cap K$ so $S_\infty(K)$ has inertia degree one in EK/K. Therefore $E_{\mathfrak{ge}}K \subseteq K_{\mathfrak{ge}}$. Finally, if $C := K_{\mathfrak{ge},m} \cap k(\Lambda_N)$, on the one hand $E_{\mathfrak{ge}} \subseteq C$ and on the other hand C/E is unramified since $K_{\mathfrak{ge}}/EK$ is unramified; also $S_\infty(E)$ decomposes fully in C/E. It follows that $C = E_{\mathfrak{ge}}$. By the Galois correspondence, we have $K_{\mathfrak{ge},m} = E_{\mathfrak{ge},m}$. Now $K_{\mathfrak{ge},m}/E_{\mathfrak{ge},m}K$ is an extension of constants and the field of constants $K_{\mathfrak{ge},m}$ is $\mathbb{F}_{q^t}$ where t is the degree of any infinite prime in K. It can be proved that $\mathbb{F}_{q^t} \subseteq E_{\mathfrak{ge},m}K$. The result follows. $\square$

In our case, $E = k\big(\sqrt[l^n]{(-1)^{\deg D}D}\big)$. Therefore we obtain our main result.

Theorem 4.3. *Let $D \in R_T$ be a monic l–power free polynomial and let $\gamma \in \mathbb{F}_q^*$. Let $K = k\big(\sqrt[l^n]{\gamma D}\big)$. Let $D = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ where $\alpha_i = l^{a_i} c_i$, $0 \le a_i \le n-1$, $\gcd(c_i, l) = 1$, $1 \le i \le r$. Let $\deg D = l^{t'} s$, $\gcd(s, l) = 1$ and let $\deg P_i = l^{b_i'} d_i$, $\gcd(d_i, l) = 1$. Let $t = \min\{n, t'\}$, $b_i = \min\{b_i', n - a_i\}$. We order the product so that $a_1 + b_1 \le a_2 + b_2 \le \ldots \le a_u + b_u < t \le a_{u+1} + b_{u+1} \le \cdots \le a_r + b_r$. We also assume that $b_1 = \min\{b_i \mid 1 \le i \le u\}$. There exist $x_i = l^{b_i - b_1} z_i$, where $z_i \in \mathbb{N}$, $\gcd(z_i, l) = 1$, $2 \le i \le u$ and $y_i \in \mathbb{N}$, where $\gcd(y_i, l) = 1$, $2 \le i \le u$ such that*

$$d_i + z_i d_1 = l^{t - a_i - b_i} y_i$$

and there exists $w = l^{t - a_1 - b_1} \rho$ with $\rho \in \mathbb{N}$ such that

$$\kappa l^{n - a_1} - c_1 w = d_1^{-1} l^{t - a_1 - b_1} \Big(\sum_{i=2}^{u} c_i y_i - l^{t' - t} s + \sum_{i=u+1}^{r} l^{a_i + b_i' - t} c_i d_i \Big)$$

for some $\kappa \in \mathbb{Z}$. Then $K_{\mathfrak{ge}}$ is given by

$$\begin{aligned} K_{\mathfrak{ge}} = k\Big(& \sqrt[l^n]{\gamma D}, \sqrt[l^{n-a_1}]{(-1)^{\deg P_1^w} P_1^w}, \sqrt[l^{n-a_2}]{(-1)^{\deg P_2 P_1^{x_2}} P_2 P_1^{x_2}}, \ldots, \\ & \sqrt[l^{n-a_u}]{(-1)^{\deg P_u P_1^{x_u}} P_u P_1^{x_u}}, \sqrt[l^{n-a_{u+1}}]{(-1)^{\deg P_{u+1}} P_{u+1}}, \ldots, \\ & \sqrt[l^{n-a_r}]{(-1)^{\deg P_r} P_r} \Big). \end{aligned}$$

$\square$

Acknowledgment. The authors thank the referee for his (her) suggestions, which improved the exposition.

References

[1] Anglès, Bruno; Jaulent, Jean–François, *Théorie des genres des corps globaux*, Manuscripta Math. **101**, no. 4, 513–532, (2000).
[2] Bae, Sunghan; Hu, Su; Jung, Hwanyup, *The generalized Rédei-matrix for function fields*, Finite Fields Appl. **18**, 760–780, (2012)
[3] Bae, Sunghan; Koo, Ja Kyung, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60**, no. 3, 301–310, (1996).
[4] Clement, Rosario, *The genus field of an algebraic function field*, J. Number Theory **40**, no. 3, 359–375, (1992).
[5] Conner, P.E.; Hurrelbrink, J., *Class number parity*, Series in Pure Mathematics **8**, Singapore etc.: World Scientific,1988.
[6] Fröhlich, Albrecht, *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics, **24**, American Mathematical Society, Providence, RI, 1983.
[7] Gauss, Carl Friedrich, *Disquisitiones arithmeticae*, 1801.
[8] Hu, Su; Li, Yan, *The genus fields of Artin–Schreier extensions*, Finite Fields Appl. **16**, no. 4, 255–264, (2010).
[9] Ishida, Makoto, *The genus fields of algebraic number fields*, Lecture Notes in Mathematics, Vol. **555**, Springer-Verlag, Berlin-New York, 1976.
[10] Leopoldt, Heinrich W., *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9**, 351–362, (1953).
[11] Li, Yan; Hu, Su, *Capitulation problem for global function fields*, Arch. Math. **97**, 413–421, (2011).
[12] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus Fields of Abelian Extensions of Congruence Rational Function Fields*, arXiv:1206.4946v1. To appear in Finite Fields Appl.
[13] Peng, Guohua, *The genus fields of Kummer function fields*, J. Number Theory **98** , no. 2, 221–227, (2003).
[14] Rosen, Michael, *The Hilbert class field in function fields*, Exposition. Math. **5**, no. 4, 365–378, (1987).

[15] Rosen, Michael, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York, 2002.

[16] Villa Salvador, Gabriel Daniel, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 2006.

[17] Wittmann, Christian, *l–class groups of cyclic function fields of degree l*, Finite Fields Appl. **13**, no. 2, 327–347, (2007).

Facultad de Matemáticas, Universidad Autónoma de Yucatán
E-mail address: vbautista@uady.mx

Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N.
E-mail address: mrzedowski@ctrl.cinvestav.mx

Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N.
E-mail address: gvillasalvador@gmail.com