

**AUTOMORPHISM GROUP AND SUBFIELDS OF THE  
GENERALIZED GIULIETTI-KORCHMÁROS FUNCTION FIELD**

by  
**MEHMET ÖZDEMİR**

Submitted to the Graduate School of Engineering and Natural Sciences  
in partial fulfillment of  
the requirements for the degree of  
Doctor of Philosophy

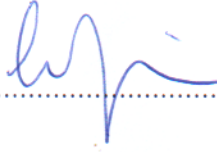
Sabanci University

Spring 2011

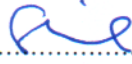
AUTOMORPHISM GROUP AND SUBFIELDS OF THE GENERALIZED  
GIULIETTI-KORCHMÁROS FUNCTION FIELD

APPROVED BY

Assoc. Prof. Dr. Cem Güneri  
(Thesis Supervisor)



Prof. Dr. Henning Stichtenoth  
(Thesis Coadvisor)



Prof. Dr. Alev Topuzođlu



Assoc. Prof. Dr. Erkay Savař



Prof. Dr. İsmail řuayip Gülođlu



DATE OF APPROVAL: 03-08-2011

©Mehmet Özdemir 2011

All Rights Reserved

AUTOMORPHISM GROUP AND SUBFIELDS OF THE GENERALIZED  
GIULIETTI-KORCHMÁROS FUNCTION FIELD

Mehmet Özdemir

Mathematics, Doctor of Philosophy Thesis, 2011

Thesis Supervisor: Assoc. Prof. Dr. Cem Güneri

Thesis Coadvisor: Prof. Dr. Henning Stichtenoth

Keywords: function fields, maximal curves, Weierstrass points, automorphism  
groups, subfields.

**Abstract**

A function field over a finite field which has the largest possible number of rational places, with respect to Hasse-Weil bound, is called maximal. The most important example of a maximal function field is the Hermitian function field  $\mathcal{H}$ . It has the largest possible genus among maximal function fields defined over the same finite field, and it is the unique function field with this genus, up to isomorphism. Moreover, it has a very large automorphism group. Until recently there was no known maximal function field which is not a subfield of  $\mathcal{H}$ . In 2009, Giulietti and Korchmáros constructed the first example of a maximal function field over the finite field  $\mathbb{F}_{q^6}$ , where  $q$  is a prime power, which is not subfield of  $\mathcal{H}$  over the same finite field. They also determined the automorphism group of this example. Later, a generalization of Giulietti and Korchmáros construction to  $\mathbb{F}_{q^{2n}}$  for any odd number  $n \geq 3$  was given by Garcia, Güneri and Stichtenoth and was shown to be maximal.

In this thesis, we determine the automorphism group of the generalized Giulietti-Korchmáros function field. Moreover, some subfields of the generalized Giulietti-Korchmáros function field and their genera are also determined.

# GENELLEŐTİRİLMİŐ GIULIETTI- KORCHMÁROS FONKSİYON CİSMİNİN OTOMORFİZMA GRUBU VE ALTCİSİMLERİ

Mehmet Özdemir

Matematik, Doktora Tezi, 2011

Tez DanıŐmanı: Doç. Dr. Cem Güneri

Tez EŐ DanıŐmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: fonksiyon cisimleri, maksimal eđriler, Weierstrass noktaları,  
otomorfizma grubu, altcisimler.

## Özet

Sonlu cisim üzerinde tanımlı ve Hasse-Weil sınırına göre olası en büyük sayıda rasyonel yer sayısına sahip fonksiyon cismine maksimal denir. En önemli maksimal fonksiyon cismi örneđi Hermitian fonksiyon cismi  $\mathcal{H}$ 'dir.  $\mathcal{H}$ , aynı sonlu cisim üzerinde tanımlı maksimal fonksiyon cisimleri arasında en büyük cinse sahiptir, ve bu cinse sahip, izomorfizma denkliđine göre, tek maksimal fonksiyon cisimidir. Ayrıca oldukça büyük bir otomorfizma grubuna sahiptir. Çok yakın zamana kadar  $\mathcal{H}$ 'in altcismi olmayan bir maksimal fonksiyon cismi örneđi bulunamamıŐtır. 2009 yılında Giulietti ve Korchmáros  $\mathbb{F}_{q^6}$  sonlu cismi üstünde,  $q$  bir asal sayı kuvveti olmak üzere, ve aynı sonlu cisim üzerinde tanımlı Hermitian fonksiyon cisminin altcismi olmayan ilk maksimal fonksiyon cismi örneđini inşa ettiler. Ayrıca bu fonksiyon cisminin otomorfizma grubunu da buldular. Daha sonra Garcia, Güneri ve Stichtenoth, Giulietti-Korchmáros fonksiyon cisminin herhangi bir tek tam sayı  $n \geq 3$  için  $\mathbb{F}_{q^{2n}}$  üzerinde tanımlı genellemesini buldular ve genelleŐtirilmiŐ Giulietti-Korchmáros fonksiyon cisminin de maksimal olduđunu gösterdiler.

Bu tezde genelleŐtirilmiŐ Giulietti-Korchmáros fonksiyon cisminin otomorfizma grubu tarif edilmiŐtir. Ayrıca, bu cismin bazı alt cisimleri ve bu alt cisimlerin cinsleri de bulunmuŐtur.

*Sevgili Aileme...*

## Acknowledgements

First and foremost, I owe my deepest gratitude to my advisor, Asoc. Prof. Dr. Cem Güneri, and my co-advisor, Prof. Dr. Henning Stichtenoth, who has supported me throughout my thesis with their patience and knowledge whilst allowing me the room to work in my own way. This thesis would not have been possible without their guidance and help. I would also like to thank to all the other professors at Sabancı University, especially to Prof. Dr. Alev Topuzođlu and Prof. Dr. Albert Erkip.

My friends have always motivated and supported me during my thesis. I am very thankful to Dr. Abdullah Özkanlar, Dr. Alp Bassa, Dr. Ayça Çeşmeliöđlu, Dr. Çınar Öncel, Dr. Deniz Turgut, Dr. Erdem Bala, Esen Aksoy, Dr. Harun Kürkçü, Dr. İbrahim İnanç, Dr. İhsan Taşkın, Mustafa Çoban, Dr. Mustafa Parlak, Özcan Yazıcı, Özgür Polat, Seher Tutdere, Dr. Ünal Şen, Yusuf Adıbelli and other math graduate students. I should not forget my beloved little nieces, Sena and Seda, their endless love and the magic pencils:) that they sent me have made me work harder.

The last two years of this work is supported by Sabancı University Academic Support Program, I would also like to express my gratitude to Dr. Huriye Arıkan, Dr. Aytaç Göğüş, Emel Taralp, Ulaş Bilgiç. Last, but not least, I would like to thank to all people who are somehow concerned with my Phd.

# Table of Contents

<b>Abstract</b>	<b>iv</b>
<b>Özet</b>	<b>v</b>
<b>Acknowledgements</b>	<b>vii</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Basics . . . . .	1
1.2 Maximal Function Fields and Automorphism Groups of Function Fields	5
1.3 GK and Generalized GK Function Field . . . . .	9
<b>2 THE AUTOMORPHISM GROUP OF THE GENERALIZED GK FUNCTION FIELD</b>	<b>16</b>
2.1 The Group $G(P_\infty)$ . . . . .	16
2.2 $P_\infty$ is a Weierstrass Point of $\mathcal{C}$ . . . . .	23
<b>3 SOME SUBFIELDS OF <math>\mathcal{C}</math></b>	<b>29</b>
3.1 Preliminaries . . . . .	29
3.2 Examples . . . . .	35
<b>Bibliography</b>	<b>40</b>



# CHAPTER 1

## INTRODUCTION

In this chapter, we will recall some of the basic concepts and facts about algebraic function fields over finite fields that will be used in later sections. We will also review earlier works on maximal function fields which are relevant to this thesis. Our preference will be the language of function fields although the notion of curve and relevant geometric terminology will also be used sometimes. Since the theory of function fields and curves are essentially equivalent, this should not cause any confusion.

### 1.1 Basics

Let  $F/K$  be an algebraic function field of genus  $g$  and  $D$  be a divisor of  $F$ . The *Riemann-Roch space* associated with  $D$  is defined as

$$\mathcal{L}(D) = \{x \in F \mid (x) \geq -D\} \cup \{0\}. \quad (1.1)$$

We denote the dimension of  $\mathcal{L}(D)$  by  $\ell(D)$ . This dimension can be computed via Riemann-Roch theorem [13, Theorem 1.5.15] which states that

$$\ell(D) = \deg D + 1 - g + \ell(W - D), \quad (1.2)$$

where  $W$  is a canonical divisor of  $F$ .

For any place  $P$  of  $F$  the integer  $n$  is called a *pole number* of  $P$  if there exists an element  $x \in F$  with  $(x)_\infty = nP$ , where  $(x)_\infty$  denotes the pole divisor of  $x$ . Otherwise,  $n$  is called a *gap number* of  $P$ . It is immediately seen from the definition of  $\mathcal{L}$ -space that  $n$  is a gap number for  $P$  if and only if  $\mathcal{L}(nP) = \mathcal{L}((n-1)P)$ . The

set of pole numbers of  $P$  is a semigroup, and there are exactly  $g$  gap numbers for a rational place  $P$  of  $F$  [13, Theorem 1.6.8].

The sequence of gap numbers at a rational place  $P$  is called the *gap sequence* at  $P$ . All but finitely many rational places of a function field have the same gap sequence. Such places are called *ordinary places* of  $F/K$ . A non-ordinary place is called a *Weierstrass point*. If  $g \geq 2$  and  $K$  is algebraically closed then a function field  $F$  has a Weierstrass point [9, Corollary 7.57, Theorem 7.103].

Let  $F'/K'$  be another function field of genus  $g'$  such that  $F' \supset F$  and  $K' \supset K$ . Assume further that  $F'/F$  is a finite separable extension. Then, Hurwitz Genus Formula [13, Theorem 3.4.13] yields

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \text{Diff}(F'/F), \quad (1.3)$$

where  $\text{Diff}(F'/F)$  is the *different divisor* of  $F'/F$  defined by

$$\text{Diff}(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P)P'. \quad (1.4)$$

Here  $d(P'|P)$  stands for the different exponent of  $P'$  over  $P$ . Later, we will see that there is a useful way of calculating  $d(P'|P)$  in finite Galois function field extensions. We will now recall some properties of Galois extensions of function fields (i.e.  $F'/F$  is a finite Galois extension). Throughout,  $v_P$  denotes the discrete valuation of  $F/K$  associated with the place  $P$ .

**Lemma 1.1.1.** [13, Lemma 3.5.2, Theorem 3.7.1] *Let  $F'/F$  be an algebraic extension of function fields,  $P \in \mathbb{P}_F$ ,  $P' \in \mathbb{P}_{F'}$  with  $P'|P$ . For an automorphism  $\sigma$  of  $F'/F$ , the set  $\sigma(P') = \{\sigma(x) \mid x \in P'\}$  is a place of  $F'$ . Moreover, we have*

- (a)  $v_{\sigma(P')}(x) = v_{P'}(\sigma^{-1}(x))$  for any  $x \in F'$ .
- (b)  $\sigma(P')$  lies over  $P$ . Hence,  $\text{Aut}(F'/F)$  acts on the set of places of  $F'$  lying over  $P$ .
- (c)  $e(\sigma(P')|P) = e(P'|P)$  and  $f(\sigma(P')|P) = f(P'|P)$ , where  $e(P'|P)$  and  $f(P'|P)$  stand for ramification index and relative degree of  $P'$  over  $P$ , respectively.

(d) If we further assume that  $F'/F$  is Galois, then  $\text{Aut}(F'/F)$  acts transitively on the set of places of  $F'$  lying over  $P$  (i.e. for any  $P_1$  and  $P_2$  above  $P$  there exists  $\sigma \in \text{Aut}(F'/F)$  such that  $\sigma(P_1) = P_2$ ).

We will now recall properties of some special types of Galois extensions, namely Kummer extensions and Artin-Schreier extensions.

**Proposition 1.1.1.** [13, Proposition 3.7.3] Let  $F/K$  be an algebraic function field with  $K$  containing all  $n$ -th roots of unity, where  $n > 1$  is relatively prime to the characteristic of  $K$ . If  $u \in F$  is an element that satisfies

$$u \neq w^d \quad \text{for all } w \in F \text{ and } d \mid n, d > 1, \quad (1.5)$$

then the extension  $F(y)/F$  with  $y^n = u$  is called a Kummer extension of  $F$ . We have:

a) The polynomial  $\phi(t) = t^n - u$  is the minimal polynomial of  $y$  over  $F$ . The extension  $F(y)/F$  is Galois of degree  $n$ . Its Galois group is cyclic, and the automorphisms of  $F(y)/F$  are given by  $\sigma(y) = \zeta y$ , where  $\zeta$  is an  $n$ -th root of unity in  $K$ .

b) Let  $P \in \mathbb{P}_F$  and  $P' \in \mathbb{P}_{F(y)}$  with  $P' \mid P$ . Then

$$e(P'|P) = \frac{n}{r_P} \quad \text{and} \quad d(P'|P) = \frac{n}{r_P} - 1, \quad (1.6)$$

where  $r_P := \gcd(n, v_P(u))$ .

**Proposition 1.1.2.** [13, Proposition 3.7.8] For an algebraic function field  $F/K$  of characteristic  $p > 0$ , suppose that  $u \in F$  is an element which satisfies the condition

$$u \neq w^p - w \quad \text{for all } w \in F. \quad (1.7)$$

The extension  $F(y)/F$  with  $y^p - y = u$  is called an Artin-Schreier extension of  $F$ .

For  $P \in \mathbb{P}_F$  we define the integer  $m_P$  by

$$m_P = \begin{cases} m & \text{if there exists } z \in F \text{ satisfying } v_P(u - (z^p - z)) = -m < 0 \text{ and } p \nmid m \\ -1 & \text{if } v_P(u - (z^p - z)) \geq 0 \text{ for some } z \in F. \end{cases}$$

Then we have:

- (a)  $F(y)/F$  is a Galois extension of degree  $p$  with cyclic Galois group. The automorphisms of  $F(y)/F$  are given by  $\sigma(y) = y + \nu$ , where  $\nu = 0, 1, \dots, p-1$ .
- (b)  $P$  is unramified in  $F(y)/F$  if and only if  $m_P = -1$ .
- (c)  $P$  is totally ramified in  $F(y)/F$  if and only if  $m_P > 0$ . In this case, the different exponent  $d(P'|P)$  is given by

$$d(P'|P) = (p-1)(m_P + 1). \quad (1.8)$$

For a Galois extension of function fields  $F'/F$  with Galois group  $G = \text{Gal}(F'/F)$ , the  $i$ -th ramification group of  $P'|P$  for  $i \geq -1$  is defined as

$$G_i(P'|P) := \{\sigma \in G \mid v_{P'}(\sigma(z) - z) \geq i + 1 \text{ for all } z \in O_{P'}\}. \quad (1.9)$$

For simplicity, we will write  $G_i(P')$  instead of  $G_i(P'|P)$ .  $G_{-1}(P')$  and  $G_0(P')$  are special subgroups of  $\text{Gal}(F'/F)$  and they are also denoted by  $G_Z(P')$  and  $G_T(P')$ , respectively. It is easy to see that

$$G_Z(P') = \{\sigma \in \text{Gal}(F'/F) \mid \sigma(P') = P'\}. \quad (1.10)$$

$G_Z(P')$  and  $G_T(P')$  are called *decomposition and inertia groups* of  $P'$  over  $P$ , respectively. The inertia group  $G_T(P')$  is a normal subgroup of  $G_Z(P')$ , and the orders of these groups are

$$|G_Z(P')| = e(P'|P) \cdot f(P'|P), \quad |G_T(P')| = e(P'|P) \quad [13, \text{Theorem 3.8.2}]. \quad (1.11)$$

The following proposition gives more information about higher ramification groups.

**Proposition 1.1.3.** [13, Proposition 3.8.5] *Let  $G_i$  be the  $i$ -th ramification group of  $P'$  over  $P$ . We have:*

- a)  $G_{-1} \supseteq G_0 \supseteq \dots \supseteq G_i \supseteq G_{i+1} \supseteq \dots$  and  $G_m = \{id\}$  for  $m$  sufficiently large.
- b) Let  $\sigma \in G_0$ ,  $i \geq 0$  and let  $t$  be a  $P'$ -prime element. Then

$$\sigma \in G_i \iff v_{P'}(\sigma(t) - t) \geq i + 1. \quad (1.12)$$

c) If  $\text{char} F = p > 0$  then  $G_1$  is a normal subgroup of  $G_0$ . The order of  $G_1$  is a power of  $p$ , and the factor group  $G_0/G_1$  is cyclic of order relatively prime to  $p$ .

The following useful theorem is known as Hilbert's Different Formula. It relates the different exponent  $d(P'|P)$  and the ramification groups  $G_i(P')$ .

**Theorem 1.1.1.** [13, Theorem 3.8.7]) Let  $F'/F$  be a Galois extension of function fields and  $P' \in \mathbb{P}_{F'}$  be a place lying over  $P \in \mathbb{P}_F$ . Then

(i)

$$d(P'|P) = \sum_{i=0}^{\infty} (|G_i(P')| - 1). \quad (1.13)$$

(ii) If  $P'|P$  is totally ramified (i.e.,  $\text{Gal}(F'|F) = G_0(P'|P)$ ) and  $t \in F'$  is a prime element of  $P'$ , then

$$d(P'|P) = \sum_{\text{id} \neq \sigma \in \text{Gal}(F'/F)} v_{P'}(\sigma(t) - t). \quad (1.14)$$

## 1.2 Maximal Function Fields and Automorphism Groups of Function Fields

Let  $F/K$  be an algebraic function field of genus  $g$  with constant field  $K$ , where  $K$  is a finite field. Let  $N(F)$  denote the number of rational places of  $F$ . By the Hasse-Weil theorem [13, Theorem 5.2.3], this number is bounded by

$$|N(F) - (|K| + 1)| \leq 2\sqrt{|K|}g. \quad (1.15)$$

A function field is called *maximal* if its number  $N(F)$  of rational places attains the upper bound in the above inequality. If  $|K|$  is not square and  $F/K$  is maximal then we have

$$N(F) = |K| + 1 + 2g\sqrt{|K|} \quad (1.16)$$

which implies that  $g = 0$ . So,  $F$  is a rational function field in this case. Hence, we will always assume that  $|K|$  is square, i.e.  $K = \mathbb{F}_{q^2}$  for some prime power  $q$ . Hence,  $F/K$  is maximal if and only if

$$N(F) = q^2 + 1 + 2gq. \quad (1.17)$$

**Remark 1.2.1.** Let  $F$  be a maximal function field over  $\mathbb{F}_{q^2}$  and  $F_r = F\mathbb{F}_{q^{2r}}$  be a constant field extension of  $F/\mathbb{F}_{q^2}$  for an odd integer  $r$ . Then,  $F_r$  is also a maximal function field over  $\mathbb{F}_{q^{2r}}$ .

**Example 1.2.1.** The most well-known example of a maximal function field is the Hermitian function field  $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$  which is defined by

$$x^q + x = y^{q+1}. \quad (1.18)$$

$\mathcal{H}$  can be considered as a Kummer extension of  $\mathbb{F}_{q^2}(x)$  of degree  $q + 1$ . There are  $q^2 + 1$  degree one places of  $\mathbb{F}_{q^2}(x)$ , namely the unique pole  $(x = \infty)$  of  $x$  and places  $(x = a)$  for  $a \in \mathbb{F}_{q^2}$ . We have  $r_{(x=\infty)} = \gcd(q + 1, -q) = 1$  which by, Proposition 1.1.1, implies

$$e(R_\infty|(x = \infty)) = q + 1 \quad d(R_\infty|(x = \infty)) = q, \quad (1.19)$$

where  $R_\infty$  is the unique degree one place of  $\mathcal{H}$  lying above  $(x = \infty)$ . We also have  $r_{(x=a)} = \gcd(q + 1, 1) = 1$  where  $(x = a) \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$  with  $a^q + a = 0$ . This gives

$$e(R_{a0}|(x = a)) = q + 1 \quad d(R_{a0}|(x = a)) = q, \quad (1.20)$$

where  $R_{a0}$  is the unique degree one place of  $\mathcal{H}$  lying above  $(x = a)$ . The places  $(x = a) \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$  with  $a^{q^2} - a = 0$  and  $a^q + a \neq 0$  split into  $q + 1$  degree one places  $R_{ab}$  with  $a^q + a = b^{q+1}$  in  $\mathcal{H}$  by Kummer's theorem (see [13, Corollary 3.3.8]). This shows that  $N(\mathcal{H}) = (q^2 - q)(q + 1) + q + 1 = q^3 + 1$ . Any place  $P$  of  $\mathbb{F}_{q^2}(x)$  which is not rational is unramified as  $r_P = \gcd(q + 1, v_P(x^q + x)) = \gcd(q + 1, 0) = q + 1$  which implies  $d(R|P) = 0$  for  $R|P$ . Now we can calculate the genus  $g(\mathcal{H})$  of  $\mathcal{H}$  by Hurwitz genus formula. We have

$$2g(\mathcal{H}) - 2 = -2(q + 1) + q \cdot q + q, \quad (1.21)$$

hence,  $g(\mathcal{H}) = \frac{q(q-1)}{2}$ . As  $q^3 + 1 = q^2 + 1 + 2g(\mathcal{H})q$ ,  $\mathcal{H}$  is a maximal function field over  $\mathbb{F}_{q^2}$ .

**Remark 1.2.2.** Let  $\mathcal{H}_r = \mathcal{H}\mathbb{F}_{q^{2r}}$  be a constant field extension of  $\mathcal{H}$  with  $r$  an odd positive integer. Then  $\mathcal{H}_r$  is also maximal by Remark 1.2.1. Note that a rational place in  $\mathcal{H}$  is unramified in  $\mathcal{H}_r/\mathcal{H}$  and there exists a unique rational place in  $\mathcal{H}_r$  lying

over it [13, Lemma 5.1.9]. For the places  $R_{ab}$  of  $\mathcal{H}_r$  lying above  $(x = a) \in \mathbb{P}_{\mathbb{F}_{q^{2r}}(x)}$  with  $a \in \mathbb{F}_{q^{2r}} \setminus \mathbb{F}_{q^2}$ , we have

$$r_{(x=a)} = q + 1 \quad e(R_{ab}|(x = a)) = 1, \quad (1.22)$$

where  $a^q + a = b^{q+1}$ . Hence such a place  $R_{ab}$  is a rational place of  $\mathcal{H}_r$ . Therefore, the rational places of  $\mathcal{H}_r$  apart from  $R_{ab}$  with  $a \in \mathbb{F}_{q^2}$  and  $R_\infty$  lie above some rational place  $(x = a)$  with  $a \in \mathbb{F}_{q^{2r}} \setminus \mathbb{F}_{q^2}$ , and these places split completely in  $\mathcal{H}_r$ . Note that not all places  $(x = a)$  with  $a \in \mathbb{F}_{q^{2r}} \setminus \mathbb{F}_{q^2}$  split in  $\mathcal{H}_r$ . This can easily be seen by comparing  $N(\mathcal{H}_r) = q^{2r} + 1 + q(q-1)q^r$  (since  $\mathcal{H}_r$  is maximal) and the number that is obtained if each  $(x = a)$  with  $a \in \mathbb{F}_{q^{2r}} \setminus \mathbb{F}_{q^2}$  splits completely.

**Theorem 1.2.1.** *(Ihara) [13, Proposition 5.3.3] If  $F/\mathbb{F}_{q^2}$  is a maximal function field, then*

$$g(F) \leq \frac{q(q-1)}{2}. \quad (1.23)$$

So,  $\mathcal{H}$  has the maximum possible genus among all maximal function fields over  $\mathbb{F}_{q^2}$ . In fact, it is the unique maximal function field, up to isomorphism, with this genus [12].

Finding new maximal function fields with different genera has been of significance for a long time. One of the main problems is to describe the following set:

$$M(q^2) = \{g \geq 0 \mid \text{there exist a maximal function field } F/\mathbb{F}_{q^2} \text{ with genus } g\}. \quad (1.24)$$

By Theorem 1.2.1, the largest number in this set is  $\frac{q(q-1)}{2}$ , which comes from the Hermitian function field. The following result is due to Serre.

**Theorem 1.2.2.** *[10, Proposition 6] Let  $F/K$  be an algebraic function field which is maximal. Then, any subfield  $E$  of  $F$  with  $K \subsetneq E$  is also maximal.*

Serre's result can be used to obtain new maximal function fields from old ones by considering the automorphism group  $\text{Aut}(F/K)$  of the maximal function field  $F$  and then finding fixed fields of some subgroups of  $\text{Aut}(F/K)$  inside  $F$ . The automorphism group of a function field  $F/K$  is the set

$$\text{Aut}(F/K) = \{\sigma \in \text{Aut}(F) \mid \sigma(k) = k \text{ for all } k \in K\}. \quad (1.25)$$

If  $K$  is a finite field then  $Aut(F/K)$  is a finite group. In characteristic 0, the cardinality of the automorphism group is bounded by Hurwitz Bound

$$Aut(F/K) \leq 84(g(F) - 1) \quad [9, \text{Theorem 11.56}]. \quad (1.26)$$

In prime characteristic, however, automorphism groups can be much larger (see [9, Theorem 11.127]). The Hermitian function field is also interesting in this respect since it has a large automorphism group. Let us now describe it.

**Automorphism Group of Hermitian Function Field:** Let  $\mathcal{H}$  be the Hermitian function field over  $\mathbb{F}_{q^2}$ . The automorphism group of  $\mathcal{H}$ , which will be denoted by  $A$ , is

$$A = \{\sigma \in Aut(\mathcal{H}) \mid \sigma(a) = a \text{ for all } a \in \mathbb{F}_{q^2}\}. \quad (1.27)$$

The group  $A$  is known [14, 15], and it is described as follows. Let  $R_\infty$  be the unique common pole of  $x$  and  $y$  in  $\mathcal{H}$ . Then, the group

$$A(R_\infty) = \{\sigma \in A \mid \sigma(R_\infty) = R_\infty\} \quad (1.28)$$

consists of the following set of automorphisms (cf. [7, Eqn. (2.2)]):

$$\sigma(y) = ay + b \quad \sigma(x) = a^{q+1}x + ab^qy + c \quad (1.29)$$

$$a \in \mathbb{F}_{q^2}^*, b \in \mathbb{F}_{q^2}, c^q + c = b^{q+1}$$

Clearly,  $|A(R_\infty)| = q^3(q^2 - 1)$ . Note that  $A(R_\infty)$  is the decomposition group of  $R_\infty$  in the extension  $\mathcal{H}/F^A$ , where  $F^A$  is the fixed field of  $A$ . There is another automorphism  $w$  of  $\mathcal{H}$  which is an involution (cf. [7, Eqn. (2.7)]):

$$w(y) = \frac{y}{x} \quad w(x) = \frac{1}{x} \quad (1.30)$$

The automorphism group  $A$  of  $\mathcal{H}$  is generated by  $w$  and  $A(R_\infty)$ , i.e.

$$A = \langle A(R_\infty), w \rangle. \quad (1.31)$$

$A$  is isomorphic to  $PGU(3, q^2)$ , and its order is  $q^3(q^2 - 1)(q^3 + 1)$ . Clearly, this order violates the Hurwitz Bound (1.26).



**Remark 1.2.3.** Let  $\overline{\mathcal{H}} = \mathcal{H}\overline{\mathbb{F}}_{q^2}$  be a constant field extension of  $\mathcal{H}$ , where  $\overline{\mathbb{F}}_{q^2}$  is the algebraic closure of  $\mathbb{F}_{q^2}$ . Let  $\overline{A}$  be the automorphism group of  $\overline{\mathcal{H}}$ , i.e.

$$\overline{A} = \{\sigma \in \text{Aut}(\overline{\mathcal{H}}) \mid \sigma(a) = a \text{ for all } a \in \overline{\mathbb{F}}_{q^2}\}. \quad (1.32)$$

Then, each automorphism in the automorphism group  $A$  of  $\mathcal{H}$  induces an automorphism in  $\overline{A}$ , and likewise any automorphism in the group  $A(R_\infty)$  gives us an automorphism in  $\overline{A}(\overline{R}_\infty)$  (cf. Eqn. (1.28)), where  $\overline{R}_\infty \in \mathbb{P}_{\overline{\mathcal{H}}}$  is the unique place lying above  $R_\infty$ . By [15, Theorem 7], we further have

$$|\overline{A}| = q^3(q^2 - 1)(q^3 + 1), \quad (1.33)$$

$$|\overline{A}(\overline{R}_\infty)| = q^3(q^2 - 1), \quad (1.34)$$

which are the orders of  $A$  and  $A(R_\infty)$  respectively. Therefore, a constant field extension of  $\mathcal{H}$  has the same automorphism group as  $\mathcal{H}$ .

The subgroups of  $A$  were extensively investigated, and a large class of the subfields of the Hermitian function field is known and described in [2] and [7]. By Serre's result, these are also maximal over  $\mathbb{F}_{q^2}$  and hence yield members for the set  $M(q^2)$ .

For a long time, all known examples of maximal function fields were shown to be subfields of  $\mathcal{H}$ . In the next section, we will present the first example of a maximal function field which is not a subfield of the Hermitian function field.

### 1.3 GK and Generalized GK Function Field

Let  $q$  be a prime power and consider the function field  $E = \mathbb{F}_{q^6}(x, y, z)$  over  $\mathbb{F}_{q^6}$  with defining equations

$$x^q + x = y^{q+1} \quad (1.35)$$

$$y^{q^2} - y = z^{\frac{q^3+1}{q+1}}. \quad (1.36)$$

$E$  was introduced by Giulietti and Korchmáros [8], and therefore will be called the GK function field.

**Theorem 1.3.1.** [8] *The GK function field  $E$  is maximal over  $\mathbb{F}_{q^6}$  with*

$$g(E) = \frac{(q^3 + 1)(q^2 - 2)}{2} + 1 \quad N(E) = q^8 - q^6 + q^5 + 1. \quad (1.37)$$

GK function field was later generalized by Garcia, Güneri and Stichtenoth to a family of function fields  $\mathcal{C}_n$  over  $\mathbb{F}_{q^{2n}}$  for any odd integer  $n \geq 3$  as follows [5]:

**Generalized GK Function Field:** Let  $n \geq 3$  be an odd integer, and consider the function field  $\mathcal{C}_n$  over  $\mathbb{F}_{q^{2n}}$  defined by the following equations:

$$x^q + x = y^{q+1} \quad (1.38)$$

$$y^{q^2} - y = z^{\frac{q^n+1}{q+1}} \quad (1.39)$$

**Theorem 1.3.2.** [5]  $\mathcal{C}_n$  is a maximal function field over  $\mathbb{F}_{q^{2n}}$  for any odd integer  $n \geq 3$  with

$$|N(\mathcal{C}_n)| = q^{2n+2} - q^{n+3} + q^{n+2} + 1 \quad g(\mathcal{C}_n) = \frac{(q-1)(q^{n+1} + q^n - q^2)}{2}. \quad (1.40)$$

**Remark 1.3.1.** (i)  $\mathcal{C}_n$  coincides with the GK function field for  $n = 3$ .

(ii) If  $q = 2$ , the GK function field is a subfield of the Hermitian function field over  $\mathbb{F}_{2^6}$  [8, page 235]. For  $q > 2$ , the GK function field  $\mathcal{C}_3$  is not a subfield of the Hermitian function field over  $\mathbb{F}_{q^6}$  [8, Theorem 5]. However, for  $n > 3$  it is not known yet whether  $\mathcal{C}_n$  is a subfield of the Hermitian function field, which is defined by

$$x^{q^n} + x = y^{q^{n+1}} \quad (1.41)$$

over  $\mathbb{F}_{q^{2n}}$ .

(iii) Recently, Duursma and Mak [3] showed that  $\mathcal{C}_n$  is not a Galois subfield of the Hermitian function field, i.e. for  $n \geq 3$  there is no embedding of  $\mathcal{C}_n$  over  $\mathbb{F}_{q^{2n}}$  into  $\mathcal{H}$  such that  $\mathcal{H}/\mathcal{C}_n$  is Galois.

We will now describe the rational places of  $\mathcal{C}_n$  [5]. We henceforth assume that  $K = \mathbb{F}_{q^{2n}}$ . The pole ( $x = \infty$ ) of  $x$  in  $K(x)$  is totally ramified in  $\mathcal{C}_n/K(x)$ , we denote the unique place of  $\mathcal{C}_n$  above ( $x = \infty$ ) as  $P_\infty$ . Observe that  $P_\infty$  is also totally ramified over  $K(y)$  and over  $K(z)$ , i.e.  $P_\infty$  is the unique pole of  $x, y$  and  $z$ . Any degree one place of  $\mathcal{C}_n$  apart from  $P_\infty$  lies over the places ( $x = a$ ) in  $K(x)$ , ( $y = b$ ) in  $K(y)$ , ( $z = c$ ) in  $K(z)$ , where  $a, b, c \in K$  satisfy

$$a^q + a = b^{q+1} \quad (1.42)$$

$$b^{q^2} - b = c^{\frac{q^n+1}{q+1}} \quad (1.43)$$

We will denote this place by  $P_{abc}$ . The diagrams in Figures 1.1, 1.2, 1.3, 1.4 and 1.5 will be useful to visualize the rational places of  $\mathcal{C}_n$  with their ramification indices.

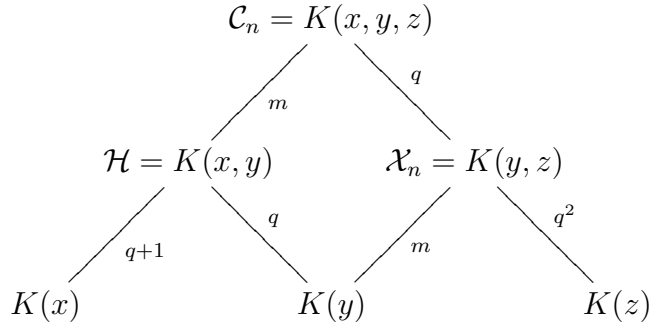


Figure 1.1: Field extensions and extension degrees,  $m = \frac{q^n+1}{q+1}$ .

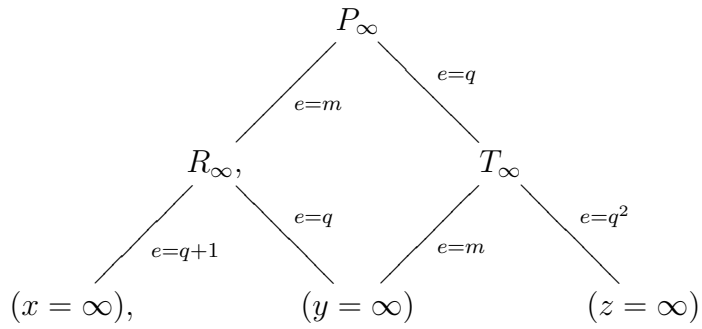


Figure 1.2: Places at  $\infty$  with ramification indices,  $m = \frac{q^n+1}{q+1}$ .

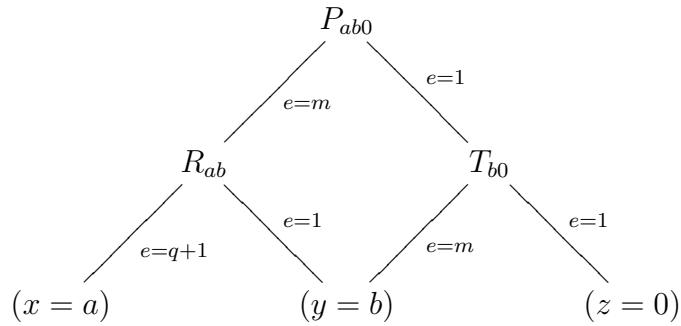


Figure 1.3: Places  $P_{abc}$  with  $a^q + a = 0$ ,  $m = \frac{q^n+1}{q+1}$ .

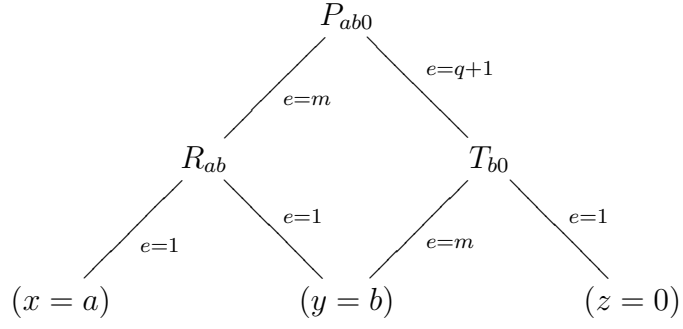


Figure 1.4: Places  $P_{abc}$  with  $a^{q^2} - a = 0$  and  $a^q + a \neq 0$ ,  $m = \frac{q^n+1}{q+1}$ .

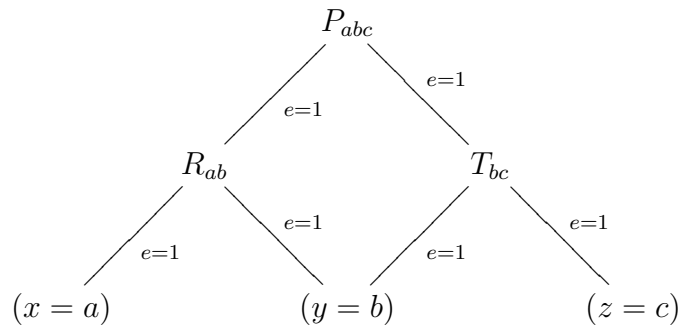


Figure 1.5: Places  $P_{abc}$  with  $a^{q^2} - a \neq 0$ .

In these diagrams,  $\mathcal{H}$  denotes the constant field extension of the Hermitian function field over  $\mathbb{F}_{q^2}$  to the field  $K$ . Since  $n$  is odd, it is also maximal (cf. Remark 1.2.1).  $\mathcal{X}_n$  is defined by the equation (1.39). Its maximality was proved by Abdon, Bezerra and Quoos in [1]. As it is shown in the diagram of poles, poles of  $x$  in  $K(x)$ ,  $y$  in  $K(y)$  and  $z$  in  $K(z)$  are denoted by  $(x = \infty)$ ,  $(y = \infty)$  and  $(z = \infty)$ , respectively. The common pole of  $y$  and  $z$  in  $K(z, y)$  is  $T_\infty$ , and the common pole of  $x$  and  $y$  in  $K(x, y)$  is  $R_\infty$ . We will now explain how the information in these diagrams can be deduced.

We will also denote the degree one places of  $K(x, y)$  and  $K(y, z)$  lying below  $P_{abc}$  as  $R_{ab}, T_{bc}$ , respectively. The degree one places of  $K(x)$ ,  $K(y)$  and  $K(z)$  lying below  $P_{abc}$  are  $(x = a)$ ,  $(y = b)$  and  $(z = c)$ , respectively. From the defining equations (1.38) and (1.39), we can deduce

$$\begin{aligned} z^{q^{n+1}} &= (y^{q^2} - y)^{q+1} \\ &= y^{q+1}((y^{q+1})^{q-1} - 1)^{q+1} \\ &= (x^q + x) \left( \frac{(x^q + x)^q}{x^q + x} - 1 \right)^{q+1} \\ &= \left( \frac{x^{q^2} - x}{x^q + x} \right)^{q+1} (x^q + x). \end{aligned}$$

So, we reach the following equation:

$$z^{q^{n+1}} = \left( \frac{x^{q^2} - x}{x^q + x} \right)^{q+1} (x^q + x). \quad (1.44)$$

The polynomial  $f(T) = T^{q^{n+1}} - \left( \frac{x^{q^2} - x}{x^q + x} \right)^{q+1} (x^q + x)$  is irreducible over  $K(x)$ . Hence  $\mathcal{C}_n = K(x, z)$ , and it is a Kummer extension of  $K(x)$  of degree  $q^n + 1$ . With the notation in Proposition 1.1.1, we have

$$\begin{aligned} r_{(x=\infty)} &= \gcd \left( q^n + 1, v_{(x=\infty)} \left( \left( \frac{x^{q^2} - x}{x^q + x} \right)^{q+1} (x^q + x) \right) \right) \\ &= \gcd(q^n + 1, -q^3) = 1. \end{aligned}$$

Therefore,  $e(P_\infty | (x = \infty)) = q^n + 1$ .

$a \in K, a^{q^2} - a = 0, a^q + a \neq 0 :$

$$\begin{aligned} r_{(x=a)} &= \gcd \left( q^n + 1, v_{(x=a)} \left( \left( \frac{x^{q^2} - x}{x^q + x} \right)^{q+1} (x^q + x) \right) \right) \\ &= \gcd(q^n + 1, q + 1) = q + 1. \end{aligned}$$

Therefore,  $e(P_{ab0}|(x = a)) = \frac{q^n + 1}{q + 1}$ .

$a \in K, a^q + a = 0 :$

$$\begin{aligned} r_{(x=a)} &= \gcd \left( q^n + 1, v_{(x=a)} \left( \left( \frac{x^{q^2} - x}{x^q + x} \right)^{q+1} (x^q + x) \right) \right) \\ &= \gcd(q^n + 1, 1) = 1. \end{aligned}$$

Therefore,  $e(P_{ab0}|(x = a)) = q^n + 1$ .

$a \in K, a^{q^2} - a \neq 0:$

$$\begin{aligned} r_{(x=a)} &= \gcd \left( q^n + 1, v_{(x=a)} \left( \left( \frac{x^{q^2} - x}{x^q + x} \right)^{q+1} (x^q + x) \right) \right) \\ &= \gcd(q^n + 1, 0) = q^n + 1. \end{aligned}$$

Therefore,  $e(P_{abc}|(x = a)) = 1$ .

Combining these observations with the ramification structure in  $\mathcal{H}/K(x)$  (cf. Example 1.2.1 and Remark 1.2.2), we conclude that the place  $R_\infty$  and the rational places  $R_{ab} \in \mathbb{P}_{\mathcal{H}}$  with  $a^{q^2} - a = 0$  (i.e.  $a \in \mathbb{F}_{q^2}$ ) are totally ramified in  $\mathcal{C}_n/\mathcal{H}$ . The other rational places in  $\mathcal{H}$  split completely in the extension  $\mathcal{C}_n/\mathcal{H}$ .

The extension  $\mathcal{C}_n/K(y)$  is Galois as the extensions  $\mathcal{H}/K(y)$  and  $\mathcal{X}_n/K(y)$  are both Galois (Artin-Schreier and Kummer extensions, respectively). In the extension  $\mathcal{X}_n/K(y)$ , we have

$$\begin{aligned} r_{(y=\infty)} &= \gcd \left( \frac{q^n + 1}{q + 1}, v_{(y=\infty)}(y^{q^2} - y) \right) \\ &= \gcd \left( \frac{q^n + 1}{q + 1}, -q^2 \right) = 1. \end{aligned}$$

Therefore,  $(T_\infty|(y = \infty)) = \frac{q^n + 1}{q + 1}$ .

$b \in K, b^{q^2} - b = 0 :$

$$\begin{aligned} r_{(y=b)} &= \gcd \left( \frac{q^n + 1}{q + 1}, v_{(y=b)}(y^{q^2} - y) \right) \\ &= \gcd \left( \frac{q^n + 1}{q + 1}, 1 \right) = 1. \end{aligned}$$

Therefore,  $e(T_{b0}|(y = b)) = \frac{q^n + 1}{q + 1}$ .

$b \in K, b^{q^2} - b \neq 0 :$

$$\begin{aligned} r_{(y=b)} &= \gcd\left(\frac{q^n + 1}{q + 1}, v_{(y=b)}(y^{q^2} - y)\right) \\ &= \gcd\left(\frac{q^n + 1}{q + 1}, 0\right) = q^n + 1. \end{aligned}$$

Therefore,  $e(T_{bc}|(y = b)) = 1$ .

In the extension  $\mathcal{C}_n/\mathcal{X}_n$ , ramification occurs only at  $T_\infty$  and it is a total ramification. The other rational places of  $\mathcal{X}_n$  split completely in  $\mathcal{C}_n$  (see [5, Theorem 2.6]). Hence, in the extension  $\mathcal{C}_n/K(y)$  ramification occurs at the places  $P_{ab0}$  with  $a \in \mathbb{F}_{q^2}$  and  $P_\infty$ . The ramification indices are

$$e(P_{ab0}|(y = b)) = \frac{q^n + 1}{q + 1} \quad e(P_\infty|(y = \infty)) = q \frac{(q^n + 1)}{q + 1}. \quad (1.45)$$

As far as the extension  $\mathcal{C}_n/K(z)$  is concerned, the extension  $\mathcal{X}_n/K(z)$  is an Artin-Schreier extension. For  $L \in \mathbb{P}_{K(z)}$ , we have

$$m_L = -1 \quad \text{for } L \neq (z = \infty) \quad \text{and} \quad m_{(z=\infty)} = \frac{q^n + 1}{q + 1}. \quad (1.46)$$

Therefore, the only ramified place in  $\mathcal{X}_n/K(z)$  is  $(z = \infty) \in \mathbb{P}_{K(z)}$ , and it is totally ramified (see [13, Proposition III.7.10]). As mentioned above, there is only one (total) ramification in  $\mathcal{C}_n/\mathcal{X}_n$  at the place  $T_\infty \in \mathbb{P}_{\mathcal{X}_n}$ . Hence, the only ramified place in  $\mathcal{C}_n/K(z)$  is  $(z = \infty)$ , which is totally ramified.

## CHAPTER 2

### THE AUTOMORPHISM GROUP OF THE GENERALIZED GK FUNCTION FIELD

In this chapter, we will describe the automorphism group of  $\mathcal{C}_n$  explicitly. For  $\mathcal{C}_3$ , the automorphism group was computed by Giulietti and Korchmáros in [8]. Recall that  $K$  stands for the finite field  $K = \mathbb{F}_{q^{2n}}$ , where  $n$  denotes an odd integer greater than or equal to 3. Throughout, we will also denote  $\mathcal{C}_n$  and  $\mathcal{X}_n$  by  $\mathcal{C}$  and  $\mathcal{X}$ , respectively, for simplicity.

#### 2.1 The Group $G(P_\infty)$

Let  $G$  denote the automorphism group of  $\mathcal{C}$ . In this section, we will determine the subgroup

$$G(P_\infty) = \{\sigma \in G \mid \sigma(P_\infty) = P_\infty\}, \quad (2.1)$$

where  $P_\infty$  is the unique pole of  $x, y, z$  in  $\mathbb{P}_{\mathcal{C}}$ . Recall that  $A$  denotes the automorphism group of the Hermitian function field, which is given in (1.31).

**Theorem 2.1.1.** *Every automorphism  $\sigma \in A(R_\infty)$  of  $\mathcal{H}$  can be extended to an automorphism  $\hat{\sigma} \in G(P_\infty)$  in exactly  $\frac{q^n+1}{q+1}$  ways, and the set*

$$\hat{A}(R_\infty) = \{\hat{\sigma} \in G \mid \hat{\sigma}|_{\mathcal{H}} \in A(R_\infty)\} \quad (2.2)$$

*is a subgroup of  $G(P_\infty)$  of order  $\frac{q^n+1}{q+1}q^3(q^2-1)$ .*

*Proof.* Recall that  $\sigma \in A(R_\infty)$  is of the form (cf. Eqn. 1.29)

$$\sigma(y) = ay + b \quad \sigma(x) = a^{q+1}x + ab^qy + c, \quad (2.3)$$



where  $a \in \mathbb{F}_{q^2}^*$ ,  $b \in \mathbb{F}_{q^2}$ ,  $c^q + c = b^{q+1}$ . We want to show that  $\sigma$  can be extended to an automorphism  $\hat{\sigma} : \mathcal{C} \rightarrow \mathcal{C}$ . We set

$$\hat{\sigma}(z) = dz \quad \text{with} \quad d^{\frac{q^n+1}{q+1}} = a, \quad (2.4)$$

where  $d$  is an element in the algebraic closure of  $\mathbb{F}_{q^2}$ . Since  $a \in \mathbb{F}_{q^2}^*$ , we have

$$d^{q^{2n}-1} = (d^{\frac{q^n+1}{q+1}})^{(q^n-1)(q+1)} = (a^{q^2-1})^{\frac{q^n-1}{q-1}} = 1. \quad (2.5)$$

This implies that  $d \in K$ . We now need show that  $\hat{\sigma}$  preserves the equations (1.38) and (1.39). As  $\hat{\sigma}|_{\mathcal{H}}$  is an automorphism of  $\mathcal{H}$ ,  $\hat{\sigma}$  preserves (1.38). Regarding Eqn. (1.39), we have

$$\hat{\sigma}(y^{q^2} - y) = (ay + b)^{q^2} - (ay + b) = a(y^{q^2} - y) = \hat{\sigma}(z^{\frac{q^n+1}{q+1}}) = (dz)^{\frac{q^n+1}{q+1}}. \quad (2.6)$$

Since we have  $d^{\frac{q^n+1}{q+1}} = a$ , Eqn. (2.6) turns into the original equation. Thus,  $\hat{\sigma}$  is an automorphism of  $\mathcal{C}$ . Moreover, by Lemma 1.1.1 we have  $\hat{\sigma} \in G(P_\infty)$  as  $P_\infty$  is totally ramified in  $\mathcal{C}/\mathcal{H}$ . Since  $|A(R_\infty)| = q^3(q^2 - 1)$  and each automorphism in  $A(R_\infty)$  can be extended in  $\frac{q^n+1}{q+1}$  different ways, the proof is finished.  $\square$

Our aim is to show that  $\hat{A}(R_\infty) = G(P_\infty)$ . The following lemma will be important for our proof.

**Lemma 2.1.1.**  *$\{1, y, \dots, y^{q^2-1}\}$  is an integral basis of  $\mathcal{X}/K(z)$  at the places  $L \in \mathbb{P}_{K(z)}$  with  $L \neq (z = \infty)$ , and  $\{1, x, \dots, x^{q-1}\}$  is an integral basis of  $\mathcal{C}/\mathcal{X}$  at the places  $T \in \mathbb{P}_{\mathcal{X}}$  with  $T \neq T_\infty$ .*

*Proof.* Let  $P \in \mathbb{P}_{\mathcal{C}}$  with  $P \neq P_\infty$ ,  $T \in \mathbb{P}_{\mathcal{X}}$  with  $P|T$  and  $L \in \mathbb{P}_{K(z)}$  with  $T|L$ . Since all places  $P \neq P_\infty$  are unramified in the extension  $\mathcal{C}/K(z)$  (cf. Section 1.3), we have

$$d(P|T) = d(T|L) = 0. \quad (2.7)$$

Let  $f(t) = t^{q^2} - t - z^{\frac{q^n+1}{q+1}}$  be the minimal polynomial of  $y$  over  $K(z)$ , and  $g(t) = t^q + t - y^{q+1}$  be the minimal polynomial of  $x$  over  $\mathcal{X}$ . Then, we have

$$d(P|T) = v_P(g'(x)) = 0 \quad \text{and} \quad d(T|L) = v_T(f'(y)) = 0. \quad (2.8)$$

Hence by [13, Theorem 3.5.10], we have that  $\{1, y, \dots, y^{q^2-1}\}$  is an integral basis of  $\mathcal{X}/K(z)$  at the place  $L$ , and  $\{1, x, \dots, x^{q-1}\}$  is an integral basis of  $\mathcal{C}/\mathcal{X}$  at the place  $T$ .  $\square$

Before passing to the next lemma, recall that the pole divisors of  $x$ ,  $y$  and  $z$  in  $\mathcal{C}$  are as follows

$$(x)_\infty = (q^n + 1)P_\infty, \quad (y)_\infty = \frac{q^n + 1}{q + 1}qP_\infty, \quad (z)_\infty = q^3P_\infty. \quad (2.9)$$

**Proposition 2.1.1.** *For any  $m \geq 0$ , the set*

$$\mathcal{B} = \left\{ x^i y^j z^k \mid i(q^n + 1) + j \left( \frac{q^n + 1}{q + 1} q \right) + kq^3 \leq m \text{ with} \right. \\ \left. 0 \leq i \leq q - 1, 0 \leq j \leq q^2 - 1 \text{ and } k \geq 0 \right\} \quad (2.10)$$

is a  $K$ -basis for  $\mathcal{L}(mP_\infty)$ . Moreover, the elements in  $\mathcal{B}$  have pairwise distinct pole orders at  $P_\infty$ .

*Proof.* All the elements in  $\mathcal{L}(mP_\infty)$  have either no pole or just a unique pole at  $P_\infty$  with pole order at most  $m$ . Let

$$\mathcal{L}_\infty = \bigcup_{m \geq 0} \mathcal{L}(mP_\infty) \quad (2.11)$$

be the set of elements of  $\mathcal{C}$  which do not have a pole outside  $P_\infty$ . Clearly,

$$\mathcal{L}_\infty = \bigcap_{P \in \mathbb{P}_{\mathcal{C}}, P \neq P_\infty} O_P = \bigcap_{T \in \mathbb{P}_{\mathcal{X}}, T \neq T_\infty} \left( \bigcap_{P \in \mathbb{P}_{\mathcal{C}}, P|T} O_P \right). \quad (2.12)$$

For every  $T \in \mathbb{P}_{\mathcal{X}}$  with  $T \neq T_\infty$ , one has

$$\bigcap_{P \in \mathbb{P}_{\mathcal{C}}, P|T} O_P = \bigoplus_{i=0}^{q-1} O_T x^i \quad (2.13)$$

by [13, Corollary 3.3.5] and Lemma 2.1.1. Therefore,

$$\bigcap_{P \in \mathbb{P}_{\mathcal{C}}, P \neq P_\infty} O_P = \bigoplus_{i=0}^{q-1} \left( \bigcap_{T \in \mathbb{P}_{\mathcal{X}}, T \neq T_\infty} O_T \right) x^i. \quad (2.14)$$

Likewise,

$$\bigcap_{T \in \mathbb{P}_{\mathcal{X}}, T \neq T_\infty} O_T = \bigcap_{L \in \mathbb{P}_{K(z)}, L \neq (z=\infty)} \left( \bigcap_{T \in \mathbb{P}_{\mathcal{X}}, T|L} O_T \right) = \bigoplus_{j=0}^{q^2-1} \left( \bigcap_{L \in \mathbb{P}_{K(z)}, L \neq (z=\infty)} O_L \right) y^j. \quad (2.15)$$

In the rational function field  $K(z)$ , the intersection

$$\bigcap_{L \in \mathbb{P}_{K(z)}, L \neq (z=\infty)} O_L \quad (2.16)$$

is equal to the polynomial ring  $K[z]$ . So, we have

$$\mathcal{L}_\infty = \bigcap_{P \in \mathbb{P}_C, P \neq P_\infty} O_P = \bigoplus_{i=0}^{q-1} \bigoplus_{j=0}^{q^2-1} \left( \bigcap_{L \in \mathbb{P}_{K(z)}, L \neq (z=\infty)} O_L \right) x^i y^j = \bigoplus_{i=0}^{q-1} \bigoplus_{j=0}^{q^2-1} K[z] x^i y^j. \quad (2.17)$$

Hence, every element  $w \in \mathcal{L}(mP_\infty)$  can be written in the form

$$w = \sum_{i,j,k} a_{ijk} x^i y^j z^k, \quad (2.18)$$

where  $a_{ijk} \in K$  and  $0 \leq i \leq q-1$ ,  $0 \leq j \leq q^2-1$ ,  $k \geq 0$ . It remains to show that the elements of the form  $x^i y^j z^k$  have pairwise distinct pole orders at  $P_\infty$ . For this, we need to prove the following statement for any  $i, j, k, i', j', k'$  with  $0 \leq i, i' \leq q-1$ ,  $0 \leq j, j' \leq q^2-1$  and  $k, k' \geq 0$ :

$$v_{P_\infty}(x^i y^j z^k) \neq v_{P_\infty}(x^{i'} y^{j'} z^{k'}) \quad \text{if} \quad (i, j, k) \neq (i', j', k'). \quad (2.19)$$

Equivalently,

$$i(q^n+1) + j \frac{q^n+1}{q+1} q + kq^3 \neq i'(q^n+1) + j' \frac{q^n+1}{q+1} q + k'q^3 \quad \text{if} \quad (i, j, k) \neq (i', j', k'). \quad (2.20)$$

Assume that  $0 \leq i, i' \leq q-1$ ,  $0 \leq j, j' \leq q^2-1$ ,  $k, k' \geq 0$  and that

$$i(q^n+1) + j \frac{q^n+1}{q+1} q + kq^3 = i'(q^n+1) + j' \frac{q^n+1}{q+1} q + k'q^3. \quad (2.21)$$

Eqn. (2.21) implies that  $i \equiv i' \pmod{q}$  and hence  $i = i'$ . Now, we have

$$j \frac{q^n+1}{q+1} q + kq^3 = j' \frac{q^n+1}{q+1} q + k'q^3, \quad (2.22)$$

which yields

$$j \frac{q^n+1}{q+1} + kq^2 = j' \frac{q^n+1}{q+1} + k'q^2. \quad (2.23)$$

It follows from Eqn. (2.23) that

$$j \frac{q^n+1}{q+1} \equiv j' \frac{q^n+1}{q+1} \pmod{q^2}. \quad (2.24)$$

This implies that  $j \equiv j' \pmod{q^2}$ , which means  $j = j'$ . Hence, we also have  $k = k'$ .  $\square$

**Corollary 2.1.1.** *For any  $n \geq 3$ , the pole numbers of  $P_\infty$  are*

$$\left\{ i(q^n+1) + j \frac{q^n+1}{q+1} q + kq^3 \mid i, j, k \in \mathbb{N} \text{ with } 0 \leq i < q, 0 \leq j < q^2, k \geq 0 \right\}. \quad (2.25)$$

**Corollary 2.1.2.** (i) The set of elements  $\{1, z\}$  forms a  $K$ -basis for  $\mathcal{L}(q^3P_\infty)$  for  $n \geq 5$ . For  $n = 3$ ,  $\{1, y, z\}$  is a basis for  $\mathcal{L}(q^3P_\infty)$ .

(ii) For  $n \geq 3$ , a  $K$ -basis for  $\mathcal{L}\left(\frac{q^n+1}{q+1}qP_\infty\right)$  is  $\{1, y, z, \dots, z^r\}$  with

$$rq^3 \leq \frac{q^n+1}{q+1}q < (r+1)q^3. \quad (2.26)$$

(iii) For  $n \geq 3$ , a  $K$ -basis for  $\mathcal{L}((q^n+1)P_\infty)$  is  $\{1, x, z, \dots, z^s, y, yz, \dots, yz^r\}$  with

$$rq^3 \leq \frac{q^n+1}{q+1} < (r+1)q^3 \quad \text{and} \quad sq^3 \leq q^n+1 < (s+1)q^3. \quad (2.27)$$

*Proof.* We will use Proposition 2.1.1.

(i) We want to find the elements  $x^i y^j z^k$  such that  $i(q^n+1) + j\frac{q^n+1}{q+1}q + kq^3 \leq q^3$ . We have  $i = 0$ . If  $k = 0$  and  $n > 3$  then  $j = 0$ , and if  $k = 0$  and  $n = 3$  then  $j = 0$  or  $j = 1$ . This gives the desired result.

(ii) For the inequality  $i(q^n+1) + j\frac{q^n+1}{q+1}q + kq^3 \leq \frac{q^n+1}{q+1}q$ , we have again  $i = 0$ . If  $j = 1$  then  $k = 0$ , and if  $j = 0$  then  $k$  can take the values  $1, 2, \dots, r$  with  $r$  as in Eqn. (2.26).

(iii) Regarding the inequality  $i(q^n+1) + j\frac{q^n+1}{q+1}q + kq^3 \leq q^n+1$ , we have  $i = 0$  or  $i = 1$ . If  $i = 1$  then  $j$  and  $k$  are both zero. If  $i = 0$  then  $j = 0$  or  $j = 1$ . If  $j = 0$  then  $k$  can be  $1, \dots, s$ , where  $s$  is as in Eqn. (2.27). If  $j = 1$  then we have  $kq^3 \leq \frac{q^n+1}{q+1}$  and hence  $k$  can be  $1, 2, \dots, r$  with  $r$  as in Eqn. (2.27). □

**Lemma 2.1.2.** Let  $F/K$  be a function field. For  $P \in \mathbb{P}_F$  and  $\sigma \in \text{Aut}(F/K)$  with  $\sigma(P) = P$ , we have  $\sigma(\mathcal{L}(mP)) = \mathcal{L}(mP)$  for any  $m \geq 0$ .

*Proof.* Since  $\sigma$  is an automorphism and  $\sigma(P) = P$ , we clearly have  $\sigma(Q) \neq P$  for any place  $Q \in \mathbb{P}_C$  that is different from  $P$ . Therefore, for  $a \in \mathcal{L}(mP)$  we have

$$v_Q(\sigma(a)) = v_{\sigma^{-1}(Q)}(a) \geq \begin{cases} -m & , \text{if } Q = P \\ 0 & , \text{if } Q \neq P. \end{cases}$$

Hence,  $\sigma(a) \in \mathcal{L}(mP)$  which implies that  $\sigma(\mathcal{L}(mP)) \subseteq \mathcal{L}(mP)$ . Since  $\sigma$  is a  $K$ -linear bijection, it preserves the dimension of  $\mathcal{L}(mP)$ . Hence,  $\sigma(\mathcal{L}(mP)) = \mathcal{L}(mP)$ . □

The following theorem is the main result of this section.

**Theorem 2.1.2.** For  $n \geq 3$ , the mapping

$$\begin{aligned}\psi : G(P_\infty) &\rightarrow A(R_\infty) \\ \hat{\sigma} &\mapsto \hat{\sigma}|_{\mathcal{H}}\end{aligned}$$

is an epimorphism and its kernel is  $\text{Gal}(\mathcal{C}/\mathcal{H})$ .

*Proof.* First, we will show that  $\psi$  maps  $G(P_\infty)$  to  $A(R_\infty)$ . Any automorphism  $\hat{\sigma} \in G(P_\infty)$  maps the  $\mathcal{L}$  spaces in Corollary 2.1.2 into themselves by Lemma 2.1.2. So,  $\hat{\sigma}(x) \in \mathcal{L}((q^n + 1)P_\infty)$ ,  $\hat{\sigma}(y) \in \mathcal{L}(q^{\frac{q^n+1}{q+1}}P_\infty)$  and  $\hat{\sigma}(z) \in \mathcal{L}(q^3P_\infty)$ . Since a basis for  $\mathcal{L}(q^3P_\infty)$  depends on the value of  $n$  (cf. Corollary 2.1.2), we have two cases:

**Case 1**  $n \geq 5$ : By Corollary 2.1.2 and Lemma 2.1.2, any  $\hat{\sigma} \in G(P_\infty)$  has to satisfy

$$\hat{\sigma}(z) = dz + e \quad \hat{\sigma}(y) = ay + P(z) \quad (2.28)$$

$$\hat{\sigma}(x) = hx + a_0y + a_1yz + \dots + a_r yz^r + B(z), \quad (2.29)$$

where  $a, d, e, h, a_0, \dots, a_r \in K$ , and  $q^3 \deg P(z) \leq \frac{q^n+1}{q+1}q$ ,  $q^3 r \leq \frac{q^n+1}{q+1}$ ,  $q^3 \deg B(z) \leq q^n + 1$ .

Note that  $x, y, z$  and their images under  $\hat{\sigma}$  must have the same pole orders at  $P_\infty$ . Therefore,  $a, d$  and  $h$  must be different from 0. If we plug (2.28) and (2.29) in the defining equations (1.38) and (1.39) of  $\mathcal{C}$ , we obtain the following:

$$(dz + e)^{\frac{q^n+1}{q+1}} = (ay)^{q^2} - ay + P(z)^{q^2} - P(z) \quad (2.30)$$

$$(hx)^q + (a_0y)^q + \dots + (a_r yz^r)^q + B(z)^q + hx + a_0y + \dots + a_r yz^r + B(z) = (ay + P(z))^{q+1} \quad (2.31)$$

Since  $\hat{\sigma}$  is an automorphism of  $\mathcal{C}$ , Eqns. (2.30) and (2.31) must yield the original Eqns. (1.38) and (1.39) up to a nonzero factor in  $K$ . So, we compare these equations. We first consider the term  $e(dz)^{\frac{q^n+1}{q+1}-1}$  on the left hand side of Eqn. (2.30). Since  $q^2 \deg P(z) < \frac{q^n+1}{q+1} - 1$  and  $q^2 \nmid \frac{q^n+1}{q+1} - 1$ , it is impossible to get a term in  $z$  of degree  $\frac{q^n+1}{q+1} - 1$  on the right hand side of the equation. So, we have  $e = 0$ . If  $P(z)^{q^2} - P(z) \neq 0$ , then the right hand side of (2.30) contains  $z$ -terms which do not exist on the left hand side. So,  $P(z)^{q^2} - P(z) = 0$  and hence  $P(z) = b \in \mathbb{F}_{q^2}$ . Therefore,

$$(dz)^{\frac{q^n+1}{q+1}} = (ay)^{q^2} - ay, \quad (2.32)$$

which implies that  $d^{\frac{q^n+1}{q+1}} = a^{q^2} = a$  by Eqn. (1.39).

Regarding Eqn. (2.31), since there is no term in Eqn. (1.38) containing the terms  $y^q z^{iq}$  for  $0 \leq i \leq r$  and  $iq < \frac{q^n+1}{q+1}$ , we have  $a_1 = \dots = a_r = 0$ . As Eqn. (1.38) does not contain any term containing  $z$  and  $\deg B(z) < \frac{q^n+1}{q+1}$ ,  $B(z)$  must be a constant polynomial i.e.  $B(z) = c$  for some  $c \in K$ . Note, in particular, that  $\hat{\sigma}(\mathcal{H}) \subseteq \mathcal{H}$  and hence  $\hat{\sigma}|_{\mathcal{H}}$  is an automorphism of  $\mathcal{H}$ . So, Eqn. (2.31) becomes

$$(hx)^q + (a_0y)^q + c^q + hx + a_0y + c = (ay+b)^{q+1} = (ay)^{q+1} + (ay)^q b + ab^q y + b^{q+1}. \quad (2.33)$$

This yields

$$c^q + c = b^{q+1}, \quad h^q = h = a^{q+1}, \quad a_0 = ab^q. \quad (2.34)$$

Therefore, any  $\hat{\sigma} \in G(P_\infty)$  is of the form

$$\hat{\sigma}(z) = dz \quad \hat{\sigma}(y) = ay + b \quad (2.35)$$

$$\hat{\sigma}(x) = a^{q+1}x + ab^q y + c, \quad (2.36)$$

where  $a \in \mathbb{F}_{q^2}^*$ ,  $b \in \mathbb{F}_{q^2}$ ,  $c^q + c = b^{q+1}$  and  $d^{\frac{q^n+1}{q+1}} = a$ . So, we have  $\psi(\hat{\sigma}) = \hat{\sigma}|_{\mathcal{H}} = \sigma \in A(R_\infty)$  for  $n \geq 5$ .

**Case 2**  $n = 3$ : We will use the same procedure.  $\hat{\sigma}(y), \hat{\sigma}(x)$  are of the same form as in Eqns. (2.28) and (2.29). For  $\hat{\sigma}(z)$ , we have

$$\hat{\sigma}(z) = dz + uy + e \quad \text{with} \quad d, u, e \in K, d \neq 0. \quad (2.37)$$

If we apply  $\hat{\sigma}$  to Eqn. (1.39), we get

$$(dz + uy + e)^{\frac{q^n+1}{q+1}} = (ay)^{q^2} - ay + P(z)^{q^2} - P(z). \quad (2.38)$$

If we consider the term  $(uy + e)(dz)^{\frac{q^n+1}{q+1}-1}$  on the left hand side of (2.38), we see that  $u = e = 0$  and  $P(z) = b \in \mathbb{F}_{q^2}$ . Then, we reduce to the case  $n \geq 5$  and the same argument can be given.

We have proved that  $\psi(\hat{\sigma}) \in A(R_\infty)$  for any  $n \geq 3$ .  $\psi$  is obviously a homomorphism, and it is onto by Theorem 2.1.1. The kernel of  $\psi$  consists of the extensions of the identity automorphism of  $\mathcal{H}$ , and these automorphisms are of the form

$$\sigma(z) = dz \quad \text{with} \quad d^{\frac{q^n+1}{q+1}} = 1. \quad (2.39)$$

The set such automorphisms form the Galois group of the Kummer extension  $\mathcal{C}/\mathcal{H}$  by Proposition 1.1.1. This completes the proof.  $\square$

## 2.2 $P_\infty$ is a Weierstrass Point of $\mathcal{C}$

In this section, we will show that  $P_\infty$  is a Weierstrass point of  $\mathcal{C}$ . We will also describe the places which have the same pole numbers as  $P_\infty$ . We start with the following Lemma.

**Lemma 2.2.1.** *The extension  $\mathcal{C}/K(z)$  is Galois for any  $n \geq 3$ . The Galois group of this extension consists of automorphisms of the form*

$$\hat{\sigma}(y) = y + b \quad \hat{\sigma}(x) = x + b^q y + c \quad \hat{\sigma}(z) = z, \quad (2.40)$$

where  $b \in \mathbb{F}_{q^2}$  and  $c^q + c = b^{q+1}$ .

*Proof.* It is enough to check that  $\hat{\sigma}$  preserves the defining equations (1.38) and (1.39) of  $\mathcal{C}$ . Note that  $\hat{\sigma}|_{\mathcal{H}} \in A(R_\infty)$  by (1.29). Thus,  $\hat{\sigma}$  preserves Eqn. (1.38). Regarding Eqn. (1.39), we have

$$\hat{\sigma}(y^{q^2} - y) = (y + b)^{q^2} - (y + b) = y^{q^2} - y = \hat{\sigma}(z^{\frac{q^n+1}{q+1}}) = z^{\frac{q^n+1}{q+1}}. \quad (2.41)$$

So,  $\hat{\sigma}$  is an automorphism of  $\mathcal{C}$ . The number of such automorphisms is  $q^3$ . As the degree of the extension  $\mathcal{C}/K(z)$  is also  $q^3$ ,  $\mathcal{C}/K(z)$  is Galois, and its automorphisms are described by (2.40).  $\square$

The following Lemma will be our main tool in determining the rational places which have the same pole numbers as  $P_\infty$ .

**Lemma 2.2.2.** *[15, Page 625] Let  $P$  be a rational place of  $\mathcal{C}$ . Then,  $k$  is a gap number for  $P$  if and only if there exists  $t \in \mathcal{L}(W)$  such that  $v_P(t) = k - 1$ , where  $W$  is a canonical divisor of  $\mathcal{C}$  whose support does not contain  $P$ .*

Now we need to have a canonical divisor.

**Lemma 2.2.3.**  *$(2g(\mathcal{C}) - 2)P_\infty$  is a canonical divisor of  $\mathcal{C}$ .*

*Proof.* We consider the extension  $\mathcal{C}/K(z)$ . By [13, Eqn. (4.37)], the divisor of the differential  $dz$  is

$$(dz) = -2(z)_\infty + \text{Diff}(\mathcal{C}/K(z)). \quad (2.42)$$

Since  $(dz)$  is canonical divisor, we have  $\deg(dz) = 2g(\mathcal{C}) - 2$ . We have observed in Chapter 1 that  $P_\infty$  is the only ramified place in  $\mathcal{C}/K(z)$ , and  $P_\infty$  is the only pole of  $z$ . Therefore, the support of the divisor  $(dz)$  only contains the rational place  $P_\infty$ . Hence,  $(dz) = (2g(\mathcal{C}) - 2)P_\infty$ .  $\square$

**Remark 2.2.1.** For  $\sigma \in \text{Aut}(F/K)$  and  $P \in \mathbb{P}_F$ ,  $P$  and  $\sigma(P)$  have the same pole numbers and the same degrees. Motivated by this, we would like to determine the rational places of  $\mathcal{C}$  which have the same pole numbers as  $P_\infty$ .

**Lemma 2.2.4.** *For  $n \geq 5$ ,  $P_\infty$  is the only degree one place of  $\mathcal{C}$  with the pole numbers given in (2.25).*

*Proof.* Consider any rational place  $P_{abc}$  of  $\mathcal{C}$  that is different from  $P_\infty$ . Our aim is to show that  $q^3$  is a gap number at  $P_{abc}$ . Since  $q^3$  is a pole number at  $P_\infty$ , our result will follow.

Since  $(2g(\mathcal{C}) - 2)P_\infty$  is a canonical divisor of  $\mathcal{C}$  and  $P_{abc}$  is not in its support, it is enough to find a function  $t \in \mathcal{L}((2g(\mathcal{C}) - 2)P_\infty)$  such that  $v_{P_{abc}}(t) = q^3 - 1$  (cf. Lemma 2.2.2). We know by our analysis in Section 1.3 that  $P_\infty$  is the only ramified place in  $\mathcal{C}/K(z)$ . Hence,

$$v_{P_{abc}}((z - c)^{q^3 - 1}) = (q^3 - 1)e(P_{abc}|(z = c)) = q^3 - 1, \quad (2.43)$$

where  $(x - c) \in \mathbb{P}_{K(z)}$  is the place lying below  $P_{abc}$ . It is clear that  $P_\infty$  is the only pole of  $(z - c)^{q^3 - 1}$  in  $\mathcal{C}$ . Moreover,

$$v_{P_\infty}((z - c)^{q^3 - 1}) = (q^3 - 1)e(P_\infty|(z = \infty)) = -(q^3 - 1)q^3 \quad (2.44)$$

where  $(z = \infty) \in \mathbb{P}_{K(z)}$  is the infinite place lying below  $P_\infty$ . For  $n \geq 5$ , we have

$$q^3(q^3 - 1) \leq 2g(\mathcal{C}) - 2 = (q - 1)(q^{n+1} + q^n - 2) - 2 \quad (2.45)$$

Hence  $(z - c)^{q^3 - 1} \in \mathcal{L}((2g(\mathcal{C}) - 2)P_\infty)$  and the proof is finished.  $\square$

Now, for  $n = 3$  we determine the rational places of  $\mathcal{C}$  that have the same pole numbers as  $P_\infty$ . We will need the following Lemma.

**Lemma 2.2.5.** *For  $n = 3$ , every automorphism of  $\mathcal{H}$  can be extended to  $\mathcal{C}$ .*



*Proof.* The automorphism group of  $\mathcal{H}$  over  $K$  is generated by the group  $A(R_\infty)$  and the involution automorphism  $w$  given by (1.30) (cf. Remark 1.2.3). We know by Theorem 2.1.1 that every automorphism  $\sigma \in A(R_\infty)$  can be extended to  $\mathcal{C}$  for any  $n \geq 3$ . So, for  $n = 3$  it is enough to show that the involution  $w$  can be extended to an automorphism  $\hat{w}$  of  $\mathcal{C}$ . For  $n = 3$ , we can extract from the defining equations (1.38) and (1.39) that

$$\begin{aligned}
z^{q^3+1} &= (y^{q^2} - y)^{q+1} \\
&= (y^{q^3} - y^q)(y^{q^2} - y) \\
&= (y^{q+1})^{q^2} - (y^{q+1})^{\frac{q^3+1}{q+1}} - (y^{q+1})^q + y^{q+1} \\
&= (x^q + x)^{q^2} - (x^q + x)^{\frac{q^3+1}{q+1}} - (x^q + x)^q + (x^q + x) \\
&= x^{q^3} + x - (x^q + x)^{\frac{q^3+1}{q+1}}.
\end{aligned}$$

Hence, we have  $\mathcal{C} = K(x, z)$  with

$$z^{q^3+1} = x^{q^3} + x - (x^q + x)^{\frac{q^3+1}{q+1}}. \quad (2.46)$$

We define the map  $\hat{w}$  which extends  $w$  by

$$\hat{w}(z) = \frac{z}{x}. \quad (2.47)$$

It is easy to see that  $\hat{w}$  preserves Eqn. (2.46):

$$\frac{z^{q^3+1}}{x^{q^3+1}} = \frac{x^{q^3} + x}{x^{q^3+1}} - \left( \frac{x^q + 1}{x^{q+1}} \right)^{\frac{q^3+1}{q+1}} = \frac{x^{q^3} + x - (x^q + x)^{\frac{q^3+1}{q+1}}}{x^{q^3+1}} \quad (2.48)$$

So,  $\hat{w}$  is a automorphism of  $\mathcal{C}$  with  $\hat{w}|_{\mathcal{H}} = w$ .  $\square$

**Lemma 2.2.6.** *For  $n = 3$ , the set of degree one places which have the same pole numbers as  $P_\infty$  is*

$$\mathbb{S} = \{P_{ab0} \mid a \in \mathbb{F}_{q^2}\} \cup \{P_\infty\}. \quad (2.49)$$

*Proof.* It follows from the defining equations of  $\mathcal{C}$  that the set of places of  $\mathcal{C}$  lying above  $(z = 0) \in \mathbb{P}_{K(z)}$  is  $\{P_{ab0} \mid a \in \mathbb{F}_{q^2}\}$  (see also Figures 1.3 and 1.4). Since the extension  $\mathcal{C}/K(z)$  is Galois (Lemma 2.2.1), these places have the same pole number distribution (cf. Remark 2.2.1) for  $n \geq 3$ . Moreover, for  $n = 3$  the elements  $z$  and  $\frac{z}{x}$

are prime elements of  $P_{000}$  and  $P_\infty$ , respectively. Since the involution automorphism  $\hat{w}$  of  $\mathcal{C}$  take  $z$  to  $\frac{z}{x}$ , we have

$$\hat{w}(P_{000}) = P_\infty. \quad (2.50)$$

Hence, by Remark 2.2.1, all the places in  $\mathbb{S}$  have the same pole numbers for  $n = 3$ . We want to show that no other rational place of  $\mathcal{C}$  has the same pole numbers.

Now, consider the rational places  $P_{abc}$  with  $a \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ . Note that all such places are unramified over  $\mathbb{F}_{q^6}(x)$ ,  $\mathbb{F}_{q^6}(y)$  and  $\mathbb{F}_{q^6}(z)$  (cf. Figure 1.5). We set  $\hat{x} = x - a$ ,  $\hat{y} = y - b$  and  $\hat{z} = z - c$  and rewrite Eqn. (1.39) as

$$(\hat{z} + c)^{\frac{q^3+1}{q+1}} = (\hat{y} + b)^{q^2} - (\hat{y} + b), \quad (2.51)$$

where  $c^{\frac{q^3+1}{q+1}} = b^{q^2} - b$ . Observe that we have

$$(\hat{z} + c)^{\frac{q^3+1}{q+1}} = (\hat{z}^q + c^q)^{q-1}(\hat{z} + c) = \hat{z}^{\frac{q^3+1}{q+1}} + \dots - \hat{z}^q c^{q^2-2q+1} + \hat{z} c^{\frac{q^3+1}{q+1}-1} + c^{\frac{q^3+1}{q+1}}, \quad (2.52)$$

where  $\hat{z}$ -terms are ordered with respect to their degrees. So, we can rewrite Eqn. 2.51 as

$$\hat{z} c^{\frac{q^3+1}{q+1}-1} + \hat{y} = -\hat{z}^{\frac{q^3+1}{q+1}} - \dots + \hat{z}^q c^{q^2-2q+1} + \hat{y}^{q^2}. \quad (2.53)$$

We set  $t := \hat{z} c^{\frac{q^3+1}{q+1}-1} + \hat{y}$ . Applying strict triangle inequality on the right side, we conclude

$$v_{P_{abc}}(t) = q. \quad (2.54)$$

We can replace the term  $x^q + x$  in (2.46) by  $y^{q^2+1}$  to obtain

$$x^{q^3} + x = y^{q^3+1} + z^{q^3+1}. \quad (2.55)$$

If we write the above equation in variables  $\hat{x}$ ,  $\hat{y}$ , and  $\hat{z}$ , we obtain

$$(\hat{x} + a)^{q^3} + (\hat{x} + a) = (\hat{y} + b)^{q^3+1} + (\hat{z} + c)^{q^3+1}, \quad (2.56)$$

where  $a^{q^3} + a = b^{q^3+1} + c^{q^3+1}$ . Hence, Eqn. (2.56) becomes

$$\hat{x} - b^{q^3} \hat{y} - c^{q^3} \hat{z} = -\hat{x}^{q^3} + b \hat{y}^{q^3} + \hat{y}^{q^3+1} + c \hat{z}^{q^3} + \hat{z}^{q^3+1}. \quad (2.57)$$

We set

$$u := \hat{x} - b^{q^3} \hat{y} - c^{q^3} \hat{z}. \quad (2.58)$$

We have  $v_{P_{abc}}(u) = v_{P_{abc}}(-\hat{x}^{q^3} + b\hat{y}^{q^3} + \hat{y}^{q^3+1} + c\hat{z}^{q^3} + \hat{z}^{q^3+1}) \geq q^3$  by triangle inequality. Since  $u$  has unique pole at  $P_\infty$  of order  $q^3 + 1$  (cf. Eqn. (2.9)), we have

$$v_{P_{abc}}(u) = q^3 \quad \text{or} \quad v_{P_{abc}}(u) = q^3 + 1. \quad (2.59)$$

Note that  $u \in \mathcal{L}((2g(\mathcal{C}) - 2)P_\infty)$  since

$$v_{P_\infty}(u) = -(q^3 + 1) \geq -q^5 + 2q^3 - q^2 + 2.$$

Hence if  $v_{P_{abc}}(u) = q^3$  then  $q^3 + 1$  is a gap number at  $P_{abc}$  (cf. Lemma 2.2.2). However  $q^3 + 1$  is a pole number for  $P_\infty$ . Now suppose  $v_{P_{abc}}(u) = q^3 + 1$ . We set

$$s := ut^{q^2-2q+1}\hat{x}^{q-2} = (\hat{x} - b^{q^3}\hat{y} - c^{q^3}\hat{z})(\hat{z}c^{\frac{q^3+1}{q+1}-1} + \hat{y})^{q^2-2q+1}\hat{x}^{q-2}. \quad (2.60)$$

Note that  $v_{P_\infty}(s) = -(q^2 - 2q + 1)q^3 - (q^3 + 1)(q - 1)$  by strict triangle inequality. Moreover,  $P_\infty$  is the only pole of  $s$ . Since

$$-(q^2-2q+1)q^3 - (q^3+1)(q-1) = -(q^5 - q^4 + q - 1) \geq -(2g(\mathcal{C}) - 2) = -(q^5 - 2q^3 + q^2 - 2) \quad (2.61)$$

holds for any  $q \geq 2$ , we have  $s \in \mathcal{L}(2g(\mathcal{C}) - 2)P_\infty$ . By (2.54), we have

$$\begin{aligned} v_{P_{abc}}(s) &= (q^3 + 1) + (q^2 - 2q + 1)q + (q - 2) \\ &= 2q^3 - 2q^2 + 2q - 1 \\ &= 2(q^3 - q^2 + q) - 1. \end{aligned}$$

Hence,  $2q^3 - 2q^2 + 2q$  is a gap number for  $P_{abc}$ . Since  $\frac{q^3+1}{q+1}q = q^3 - q^2 + q$  is a pole number at  $P_\infty$ , we conclude the proof.  $\square$

**Automorphism Group of  $\mathcal{C}$ :** As before  $G$  denotes  $\text{Aut}(\mathcal{C}/K)$ . As seen in the proof of Theorem 2.1.2, the subgroup  $G(P_\infty)$  of  $G$  consists of automorphisms of the form

$$\sigma(x) = a^{q+1}x + ab^qy + c \quad \sigma(y) = ay + b \quad \sigma(z) = dz, \quad (2.62)$$

where  $a \in \mathbb{F}_{q^2}^*$ ,  $b \in \mathbb{F}_{q^2}$ ,  $c^q + c = b^{q+1}$ ,  $d^{\frac{q^n+1}{q+1}} = a$ . We also know, by Lemma 2.2.5, that the elements in the automorphism group  $A = \langle A(R_\infty), w \rangle$  of  $\mathcal{H}$  can be extended to  $\mathcal{C}$  for  $n = 3$ . Let  $\hat{A}$  denote the set of all these extensions. The following is our main result.

**Theorem 2.2.1.** (i) For  $n \geq 5$ , we have  $G = G(P_\infty)$ .

(ii) For  $n = 3$ , we have  $G = \hat{A}$ .

*Proof.* (i) By Remark 2.2.1 and Lemma 2.2.4, any automorphism  $\sigma \in G$  must map  $P_\infty$  to itself. So,  $G = G(P_\infty)$ .

(ii) Consider the fixed fields of  $G$  and its subgroup  $Gal(\mathcal{C}/K(z))$  in  $\mathcal{C}/K$ , which are  $\mathcal{C}^G$  and  $K(z)$ , respectively. Places  $P_{ab0} \in \mathbb{P}_{\mathcal{C}}$  (with  $a \in \mathbb{F}_{q^2}$ ) lie over  $(z = 0) \in \mathbb{P}_{K(z)}$ . Moreover, The involution  $\hat{w}$  maps  $P_{000}$  to  $P_\infty$ . Since  $\mathcal{C}/\mathcal{C}^G$  is Galois, places in the set  $\mathcal{S} = \{P_{ab0} \mid a \in \mathbb{F}_{q^2}\} \cup \{P_\infty\}$  lie over some place  $Q \in \mathbb{P}_{\mathcal{C}^G}$ . Furthermore, there is no other place in  $\mathcal{C}$  which lie over  $Q$  by Lemma 2.2.6. Hence, we have

$$|G| = |G(P_\infty)|(q^3 + 1) = |\hat{A}| \quad (2.63)$$

This completes the proof.

□

# CHAPTER 3

## SOME SUBFIELDS OF $\mathcal{C}$

In this chapter, we will describe some subgroups of the automorphism group  $G$  of  $\mathcal{C}$  and find the genera of the fixed fields corresponding to these subgroups. For  $n \geq 5$ , the automorphism group of  $\mathcal{C}$  is exactly the group  $G(P_\infty)$  by Theorem 2.2.1. So, we will concentrate on the subgroups of  $G(P_\infty)$ . Note that a large class of subfields of  $\mathcal{C}$  for  $n = 3$  was found in [4].

### 3.1 Preliminaries

Let  $U$  be a subgroup of  $G(P_\infty)$ , and  $\mathcal{C}^U$  the fixed field corresponding to  $U$ . In this section, we will describe the computation of the genus of  $\mathcal{C}^U$ . We start with investigating the different exponents and ramification indices of the places in the extension  $\mathcal{C}/\mathcal{C}^{G(P_\infty)}$ . Consider, as before, the following set of places in  $\mathbb{P}_{\mathcal{C}}$ :

$$\mathbb{S} = \{P_{ab0} \mid a \in \mathbb{F}_{q^2}\} \cup \{P_\infty\}. \quad (3.1)$$

For the element

$$t = \frac{z^{q^{n-3}}}{x}, \quad (3.2)$$

we have

$$v_{P_\infty}(t) = -q^{n-3}q^3 - (-q^n - 1) = 1 \quad (3.3)$$

by (2.9). Thus,  $t$  is a prime element for  $P_\infty$ . If  $Q$  is the place lying below  $P_\infty$ , then by Theorem 1.1.1, we have

$$d(P_\infty|Q) = \sum_{id \neq \sigma \in G} v_{P_\infty}(\sigma(t) - t). \quad (3.4)$$

For the summands, we have

$$\begin{aligned}
v_{P_\infty}(\sigma(t) - t) &= v_{P_\infty} \left( \frac{(dz)^{q^{n-3}}}{a^{q+1}x + ab^qy + c} - \frac{z^{q^{n-3}}}{x} \right) \\
&= v_{P_\infty} \left( \frac{z^{q^{n-3}}(d^{q^{n-3}}x - a^{q+1}x - ab^qy - c)}{x(a^{q+1}x + ab^qy + c)} \right) \\
&= v_{P_\infty}(z^{q^{n-3}}) + v_{P_\infty}(d^{q^{n-3}}x - a^{q+1}x - ab^qy - c) - v_{P_\infty}(x) \\
&\quad - v_{P_\infty}(a^{q+1}x + ab^qy + c) \\
&= -q^n + v_{P_\infty}(d^{q^{n-3}}x - a^{q+1}x - ab^qy - c) + (q^n + 1) + (q^n + 1),
\end{aligned}$$

where  $a \in \mathbb{F}_{q^2}^*$ ,  $b \in \mathbb{F}_{q^2}$ ,  $c^q + c = b^{q+1}$ ,  $d^{\frac{q^n+1}{q+1}} = a$ . So, this value depends on  $v_{P_\infty} \left( x(d^{q^{n-3}} - a^{q+1}) - ab^qy - c \right)$ . If  $d^{q^{n-3}} \neq a^{q+1}$ , then the valuation is  $-(q^n + 1)$ . If  $d^{q^{n-3}} = a^{q+1}$ , then we also have  $d^{q^{n-3}} = d^{q^n+1}$ , which yields

$$d^{q^n - q^{n-3} + 1} = 1. \quad (3.5)$$

Note that  $q^n - q^{n-3} + 1 \nmid q^{2n} - 1 = |\mathbb{F}_{q^{2n}}^*|$ . Hence  $d = 1$ , in which case  $a = 1$  as well.

So, for  $a = d = 1$ , we have

$$v_{P_\infty}(d^{q^{n-3}}x - a^{q+1}x - ab^qy - c) = v_{P_\infty}(-ab^qy - c) = \begin{cases} -\frac{q^n+1}{q+1}q, & b \neq 0 \\ 0, & b = 0. \end{cases}$$

Hence,

$$v_{P_\infty}(\sigma(t) - t) = \begin{cases} \frac{q^n+1}{q+1} + 1, & a = d = 1, b \neq 0 \\ q^n + 2, & a = d = 1, b = 0 \\ 1, & \text{else.} \end{cases} \quad (3.6)$$

**Lemma 3.1.1.** *The places in  $\mathbb{S}$  are the only ramified places of  $\mathcal{C}$  in the extension  $\mathcal{C}/\mathcal{C}^{G(P_\infty)}$  with*

$$e(P_\infty) = (q^2 - 1)q^3 \frac{q^n + 1}{q + 1} \quad (3.7)$$

$$d(P_\infty) = \frac{(q^5 + q^2 - q - 1)(q^n + 1)}{q + 1} - 1 \quad (3.8)$$

$$e(P_{ab0}) = (q - 1)(q^n + 1), \quad d(P_{ab0}) = (q - 1)(q^n + 1) - 1. \quad (3.9)$$

*Proof.* Note that  $G(P_\infty)$  is the decomposition group of  $P_\infty$  in the extension  $\mathcal{C}/\mathcal{C}^{G(P_\infty)}$ .

Since  $P_\infty$  is rational we have  $f(P_\infty) = 1$  in  $\mathcal{C}/\mathcal{C}^{G(P_\infty)}$ . Hence, we have (cf. Eqn.

(1.11))

$$e(P_\infty) = |G(P_\infty)| = (q^2 - 1)q^3 \frac{q^n + 1}{q + 1}. \quad (3.10)$$

By (3.4) and (3.6), we have

$$\begin{aligned}
d(P_\infty) &= (q^2 - 1)q \left( \frac{q^n + 1}{q + 1} + 1 \right) + (q - 1)(q^n + 2) \\
&\quad + \left( (q^2 - 1)q^3 \frac{q^n + 1}{q + 1} - (q^3 - 1) - 1 \right) \\
&= \frac{q^n + 1}{q + 1} \left( (q^3 - q) + (q - 1)(q + 1) + (q^5 - q^3) \right) + (q^3 - q) + (q - 1) - q^3 \\
&= \frac{q^n + 1}{q + 1} (q^5 + q^2 - q - 1) - 1.
\end{aligned}$$

In the extension  $\mathcal{H}/\mathcal{H}^{A(R_\infty)}$ , the set of ramified places of  $\mathcal{H}$  apart from  $R_\infty$  is

$$\mathbb{T} = \{R_{ab} \mid a \in \mathbb{F}_{q^2}\} \quad (\text{see [7, Page 149]}). \quad (3.11)$$

Note that  $[\mathcal{H} : \mathcal{H}^{A(R_\infty)}] = A(R_\infty) = q^3(q^2 - 1)$ . There are  $q^3$  places of the form (3.11) in  $\mathcal{H}$  with  $f(R_{ab}) = 1$ . Hence,

$$q^3(q^2 - 1) = q^3 \cdot e(R_{ab})$$

and we have

$$e(R_{ab}) = q^2 - 1.$$

Recall that the set of all ramified rational places of  $\mathcal{C}$ , except for  $P_\infty$ , in  $\mathcal{C}/\mathcal{H}$  is  $\{P_{ab0} \mid a \in \mathbb{F}_{q^2}\}$ . The places of  $\mathcal{H}$  in  $\mathbb{T}$  are exactly the places lying below this set (see Figures 1.3 and 1.4).

Since

$$[\mathcal{C} : \mathcal{C}^{G(P_\infty)}] = |G(P_\infty)| = q^3(q^2 - 1) \frac{q^n + 1}{q + 1}$$

and

$$[\mathcal{C} : \mathcal{H}] \cdot [\mathcal{H} : \mathcal{H}^{A(R_\infty)}] = \frac{q^n + 1}{q + 1} \cdot q^3(q^2 - 1),$$

we have  $\mathcal{C}^{G(P_\infty)} = \mathcal{H}^{A(R_\infty)}$ . Hence,

$$e(P_{ab0}) = \frac{q^n + 1}{q + 1} (q^2 - 1). \quad (3.12)$$

Since the ramification is tame, we immediately obtain the different exponent. Using Eqn. (1.44), which defines  $\mathcal{C}$  over  $K(x)$ , we see that a nonrational place of  $\mathcal{C}$  does not ramify in  $\mathcal{C}/\mathcal{H}$ . By [7, Page 149], the places  $\{R_{ab} \mid a \in \mathbb{F}_{q^2}\}$  are the only ramified places in  $\mathcal{H}/\mathcal{H}^{A(R_\infty)}$ . Hence, a higher degree place in  $\mathcal{C}$  cannot ramify in  $\mathcal{C}/\mathcal{C}^{G(P_\infty)}$ .  $\square$

We will associate each automorphism in  $G(P_\infty)$  given by (2.62) with a quadruple  $[a, b, c, d]$ . Then

$$G(P_\infty) = \{[a, b, c, d] \mid a \in \mathbb{F}_{q^2}^*, b \in \mathbb{F}_{q^2}, c^q + c = b^{q+1}, d^{\frac{q^n+1}{q+1}} = a\}. \quad (3.13)$$

The group structure of  $G(P_\infty)$  is as follows:

$$[a_1, b_1, c_1, d_1] \cdot [a_2, b_2, c_2, d_2] = [a_1 a_2, a_2 b_1 + b_2, a_2^{q+1} c_1 + a_2 b_2^q b_1 + c_2, d_1 d_2] \quad (3.14)$$

$$id = [1, 0, 0, 1] \quad (3.15)$$

$$[a, b, c, d]^{-1} = [a^{-1}, -a^{-1}b, a^{-(q+1)}c^q, d^{-1}] \quad (3.16)$$

By Lemma 2.2.1, the subgroup  $Gal(\mathcal{C}/K(z))$  of  $G(P_\infty)$  has order  $q^3$ . Since  $G_1(P_\infty)$  is normal in  $G(P_\infty)$  with order relatively prime to  $q$  (cf. Lemma 1.1.3), we have  $|G_1(P_\infty)| = q^3$  as well. Uniqueness of  $G_1(P_\infty)$  implies that

$$G_1(P_\infty) = Gal(\mathcal{C}/K(z)) = \{[1, b, c, 1] \mid b \in \mathbb{F}_{q^2}, b^{q+1} = c^q + c\}. \quad (3.17)$$

Our next goal is to investigate  $\mathcal{C}/\mathcal{C}^U$  for a subgroup  $U$  of  $G(P_\infty)$ . If  $|U| = p^u m$  with  $p \nmid m$ ,  $U$  has a  $p$ -Sylow subgroup  $\tilde{U}$  of order  $p^u$ . Since  $G_1(P_\infty)$  is the unique  $p$ -Sylow subgroup of  $G(P_\infty)$ ,  $\tilde{U}$  is also contained in  $G_1(P_\infty)$ . Hence,

$$U \cap G_1(P_\infty) = \tilde{U}. \quad (3.18)$$

Moreover, if  $U$  has another  $p$ -Sylow subgroup  $U'$ , then by the same argument  $U'$  is contained in  $G_1(P_\infty)$ . But, this would imply that  $|U \cap G_1(P_\infty)| > p^u$ , which is a contradiction. We fix the following notation.

$$V_U = \{b \in \mathbb{F}_{q^2} \mid \text{there is } c \in \mathbb{F}_{q^2} \text{ such that } [1, b, c, 1] \in U\}.$$

$$W_U = \{c \in \mathbb{F}_{q^2} \mid [1, 0, c, 1] \in U\}.$$

$$\mathbb{T} = \{R_{ab} \in \mathbb{P}_{\mathcal{H}} \mid a \in \mathbb{F}_{q^2}\}$$

$$L = U \cap Gal(\mathcal{C}/\mathcal{H}).$$

$$J = \{\sigma \in A(R_\infty) \mid \sigma = \hat{\sigma}|_{\mathcal{H}} \text{ for some } \hat{\sigma} \in U\}.$$



Note that  $V_U$  is the image of the homomorphism

$$\begin{aligned} U \cap G_1(P_\infty) &\rightarrow K \\ [1, b, c, 1] &\mapsto b. \end{aligned}$$

Moreover,  $W_U$  is in one-to-one correspondence with the kernel of this homomorphism. Hence, we have

$$|U| = mp^u, |V_U| = p^v, |W_U| = p^w \text{ with } u = v + w \text{ for some } v \text{ and } w. \quad (3.19)$$

We now apply Hurwitz genus formula to the extension  $\mathcal{C}/\mathcal{C}^U$ . Since all ramified places of  $\mathcal{C}$  in the extension  $\mathcal{C}/\mathcal{C}^{G(P_\infty)}$  are in  $\mathbb{S}$ , we have

$$(q-1)(q^{n+1} + q^n - q^2) - 2 = mp^u(2g(\mathcal{C}^U) - 2) + d(P_\infty) + \sum_{P \in \mathbb{S}, P \neq P_\infty} d(P). \quad (3.20)$$

By (3.4) and (3.6), we have

$$\begin{aligned} d(P_\infty) &= \sum_{id \neq \hat{\sigma} \in U} v_{P_\infty}(\sigma(t) - t) \\ &= (p^w - 1)(q^n + 2) + (p^{v+w} - p^w) \left( \frac{q^n + 1}{q + 1} + 1 \right) + mp^u - p^u. \end{aligned} \quad (3.21)$$

Note that  $P_{ab0} \in \mathbb{S}$  is tamely ramified in  $\mathcal{C}/\mathcal{C}^U$ . Since  $f(P_{ab0}) = 1$ , we have

$$p \nmid e(P_{ab0}) = |G(P_{ab0})|.$$

Hence, by Lemma 1.1.3, we have

$$G_1(P_{ab0}) = G_2(P_{ab0}) = \cdots = \{id\}. \quad (3.22)$$

Hence,

$$\sum_{P \in \mathbb{S}, P \neq P_\infty} d(P) = \sum_{P \in \mathbb{S}, P \neq P_\infty} (|G(P)| - 1) = \sum_{id \neq \hat{\sigma} \in U} |\{P \in \mathbb{S} \mid P \neq P_\infty, \hat{\sigma}(P) = P\}|. \quad (3.23)$$

The following lemma describes how to calculate the expression in (3.23).

**Lemma 3.1.2.** *Let  $U$  be a subgroup of  $G(P_\infty)$  as above. Then we have*

$$\sum_{id \neq \hat{\sigma} \in U} |\{P \in \mathbb{S} \mid P \neq P_\infty, \hat{\sigma}(P) = P\}| = (|L| - 1)q^3 + |L| \sum_{id \neq \sigma \in J} |\{R \in \mathbb{T} \mid \sigma(R) = R\}|. \quad (3.24)$$

*Proof.* Since  $L$  is a subgroup of  $U$ , we can write  $U$  as a disjoint union of its cosets mod  $L$  as

$$U = L \cup \left( \bigcup_{i=1}^{r-1} A_i \right), \quad (3.25)$$

where  $r = \frac{|U|}{|L|} - 1$  and  $A_i = \hat{\sigma}_i L = \{\hat{\sigma}_i \mu \mid \mu \in L\}$  for some  $\hat{\sigma}_i \in U \setminus L$ . For  $P \in \mathbb{S}$  and  $\mu \in \text{Gal}(\mathcal{C}/\mathcal{H})$  we have  $\mu(P) = P$  since the places in  $\mathbb{S}$  are totally ramified in  $\mathcal{C}/\mathcal{H}$ . So, we have

$$\sum_{id \neq \hat{\sigma} \in L} |\{P \in \mathbb{S} \mid P \neq P_\infty, \hat{\sigma}(P) = P\}| = (|L| - 1)(|\mathbb{S} - 1|) = (|L| - 1)q^3. \quad (3.26)$$

Moreover, for  $\hat{\sigma} \in U \setminus L$  we have  $\hat{\sigma}\mu(P) = \hat{\sigma}(P) = P$  if and only if  $\hat{\sigma}|_{\mathcal{H}}(R) = R$ , where  $R \in \mathbb{P}_{\mathcal{H}}$  is the unique place lying below  $P$ . So, for each  $1 \leq i \leq r - 1$ , we have

$$\sum_{\hat{\sigma} \in A_i} |\{P \in \mathbb{S} \mid P \neq P_\infty, \hat{\sigma}(P) = P\}| = |L| \cdot |\{R \in \mathbb{T} \mid \hat{\sigma}_i|_{\mathcal{H}}(R) = R\}|. \quad (3.27)$$

This completes the proof. □

We also have (see [7, Theorem 4.4])

$$\sum_{id \neq \sigma \in J} |\{R \in \mathbb{T} \mid \sigma(R) = R\}| = \hat{m}p^u + d(qp^v - p^u) - qp^v, \quad (3.28)$$

where  $|J| = \hat{m}p^u$  for some  $\hat{m} \leq m$  and  $d = \gcd(\hat{m}, q + 1)$ .

**Some Subgroups of  $G(P_\infty)$ :** Recall that  $n \geq 5$  is an odd integer. We now determine some subgroups  $U$  of  $G(P_\infty)$ . In the literature [2, 7], certain subgroups of  $A(R_\infty)$  in the automorphism group of  $\mathcal{H}$  have been described. These subgroups consist of automorphisms

$$[a, b, c] \in A(R_\infty) \text{ with } a^\mu = 1 \quad (3.29)$$

for some  $\mu$  and possible extra conditions on  $b$  and  $c$ . Our aim is to extend such subgroups  $J$  of  $A(R_\infty)$  to a subgroup  $\hat{J}$  of  $G(P_\infty)$  in a way that

$$\hat{J} \cap \text{Gal}(\mathcal{C}/\mathcal{H}) = \{id\}. \quad (3.30)$$

Then, for a subgroup  $I$  of  $\text{Gal}(\mathcal{C}/\mathcal{H})$ , we will set

$$U := I \times \hat{J}. \quad (3.31)$$

In this case,  $U \cap \text{Gal}(\mathcal{C}/\mathcal{H}) \simeq I$ .

Consider a subgroup  $J \subseteq A(R_\infty)$  with  $\gcd\left(\mu, \frac{q^n+1}{q+1}\right) = 1$  in (3.29). We define

$$\hat{J} := \{[a, b, c, d] \mid d^{\frac{q^n+1}{q+1}} = a, d^\mu = 1\}. \quad (3.32)$$

Let  $R(\mu)$  be the set of  $\mu$ th roots of unity in  $\mathbb{F}_{q^2}$ . Then the homomorphism

$$\begin{aligned} R(\mu) &\rightarrow R(\mu) \\ \xi &\mapsto \xi^{\frac{q^n+1}{q+1}} \end{aligned}$$

is a bijection as  $\gcd\left(\mu, \frac{q^n+1}{q+1}\right) = 1$ . This implies that there is a unique  $d \in \mathbb{F}_{q^{2n}}$  with  $d^{\frac{q^n+1}{q+1}} = a$  and  $d^\mu = 1$ . Hence,  $|\hat{J}| = |J|$ . With our previous notation, we have  $|L| = |I|$  and  $|U| = |L||J|$ . This will be the setting in Examples 3.2.1 through 3.2.9 in the next section.

### 3.2 Examples

Note that  $\text{Gal}(\mathcal{C}/\mathcal{H})$  is a cyclic group of order  $\frac{q^n+1}{q+1}$ . Hence there exists a subgroup  $I$  of  $\text{Gal}(\mathcal{C}/\mathcal{H})$  of order  $\ell$ , for each divisor  $\ell$  of  $\frac{q^n+1}{q+1}$ . Throughout, we assume that  $q = p^k$ .

**Example 3.2.1.** Let  $p$  be an odd prime and  $v, w$  be integers  $0 \leq v \leq k-1$ ,  $0 \leq w \leq k$  such that  $\frac{p^{k-v}(p^{k-w}-1)}{2}$  is an integer. Then, by [7, Theorem 3.2] and its proof there exists a subgroup  $J$  of  $A(R_\infty)$  of order  $p^{v+w}$ . For  $\mathcal{C}/\mathcal{C}^U$ , we have by (3.21)

$$d(P_\infty) = (p^w - 1)(q^n + 2) + (p^{v+w} - p^w)\left(\frac{q^n + 1}{q + 1} + 1\right) + \ell p^{v+w} - p^{v+w}. \quad (3.33)$$

By Lemma 3.1.2 and Eqn. (3.28), we also have

$$\sum_{P \in \mathbb{S}, P \neq P_\infty} d(P) = (\ell - 1)q^3. \quad (3.34)$$

Now, we apply Hurwitz genus formula (cf. Eqn. (3.20)) to  $\mathcal{C}/\mathcal{C}^U$  and obtain

$$(q-1)(q^{n+1} + q^n - q^2) - 2 = (2g(\mathcal{C}^U) - 2)\ell p^{v+w} + d(P_\infty) + \sum_{P \in \mathbb{S}, P \neq P_\infty} d(P). \quad (3.35)$$

Then

$$q^{n+2} - q^n - q^3 + q^2 - 2 = 2g(\mathcal{C}^U)\ell p^{v+w} - \ell p^{v+w} + p^w + p^w q^n + p^{v+w} \frac{q^n + 1}{q + 1} - p^w \frac{q^n + 1}{q + 1} - q^n - 2 + \ell q^3 - q^3.$$

So, we have

$$\begin{aligned} 2g(\mathcal{C}^U)\ell p^{v+w} &= q^{n+2} + q^2 - p^w q^n - p^w - p^{v+w} \frac{q^n + 1}{q + 1} + p^w \frac{q^n + 1}{q + 1} + \ell q^3 + \ell p^{v+w} \\ &= q^2(q^n + 1) - p^w(q^n + 1) + \frac{q^n + 1}{q + 1}(p^w - p^{v+w}) + \ell(p^{v+w} - q^3) \\ &= \frac{q^n + 1}{q + 1}(q^2(q + 1) - p^w(q + 1) + p^w - p^{v+w}) + \ell(p^{v+w} - q^3) \\ &= \frac{q^n + 1}{q + 1}(q^3 + q^2 - p^{v+w} - p^w q) + \ell(p^{v+w} - q^3). \end{aligned}$$

Hence,

$$g(\mathcal{C}^U) = \frac{\frac{q^n+1}{q+1}(q^3 + q^2 - p^{v+w} - p^w q) + \ell(p^{v+w} - q^3)}{2\ell p^{v+w}}. \quad (3.36)$$

**Example 3.2.2.** For  $p = 2$  and for all  $v$  and  $w$  with  $0 \leq v \leq w < k$ , there exists a subgroup  $J$  of  $A(R_\infty)$  with order  $2^{v+w}$  by [7, Corollary 3.4.ii]. Calculations for  $g(\mathcal{C}^U)$  are the same as in Example 3.2.1. We replace  $p$  by 2 and obtain

$$g(\mathcal{C}^U) = \frac{\frac{q^n+1}{q+1}(q^3 + q^2 - 2^{v+w} - 2^w q) + \ell(2^{v+w} - q^3)}{\ell 2^{v+w+1}}. \quad (3.37)$$

**Example 3.2.3.** For  $p = 2$  and for all integers  $v, w$  satisfying

$$w \mid k, \quad w \mid v, \quad v \mid 2k, \quad 1 \leq v \leq k \quad \text{and} \quad \frac{2^v - 1}{2^w - 1} \mid (2^k + 1), \quad (3.38)$$

there is a subgroup  $J$  of  $A(R_\infty)$  of order  $2^{v'+w}$  for any  $v'$  with  $0 \leq v' \leq v$  (see [7, Corollary 3.4.i, Corollary 3.4.iii] and their proofs). In order to calculate  $g(\mathcal{C}^U)$ , it is sufficient to replace  $p$  and  $v$  in Example 3.2.1 by 2 and  $v'$ , respectively. We obtain

$$g(\mathcal{C}^U) = \frac{\frac{q^n+1}{q+1}(q^3 + q^2 - 2^{v'+w} - 2^w q) + \ell(2^{v'+w} - q^3)}{\ell 2^{v'+w+1}}. \quad (3.39)$$

**Example 3.2.4.** We assume that  $p \neq 2$ . Let  $s$  be the order of  $p$  in  $(\mathbb{Z}/m\mathbb{Z})^*$  and

$$r = \begin{cases} \text{order of } p \text{ in } (\mathbb{Z}/\frac{m}{2}\mathbb{Z})^* & \text{if } m \text{ is even} \\ s & \text{if } m \text{ is odd.} \end{cases}$$

Let  $m$  be a divisor of  $q - 1$ . Then, for every  $0 \leq v \leq k$  with  $s \mid v$ , and for every  $0 \leq w \leq k - 1$  with  $r \mid w$   $A(R_\infty)$  has a subgroup  $J$  of order  $mp^{v+w}$  by [2, Theorem 1]. We have

$$d(P_\infty) = (p^w - 1)(q^n + 2) + (p^{v+w} - p^w)\left(\frac{q^n + 1}{q + 1} + 1\right) + (p^{v+w} - p^w) + m\ell p^{v+w} - p^{v+w}. \quad (3.40)$$

and

$$\sum_{P \in \mathbb{S}, P \neq P_\infty} d(P) = (\ell - 1)q^3 + \ell(mp^{v+w} + d(qp^v - p^{v+w}) - qp^v), \quad (3.41)$$

where  $d = \gcd(m, q + 1)$ . Now, we apply Hurwitz genus formula to  $\mathcal{C}/\mathcal{C}^U$  and obtain

$$\begin{aligned} q^{n+2} - q^n - q^3 + q^2 - 2 &= (2g(\mathcal{C}^U) - 2)m\ell p^{v+w} + m\ell p^{v+w} + \ell(dqp^v - dp^{v+w} - qp^v) \\ &\quad + q^n p^w + 2p^w - q^n - 2 + \frac{q^n + 1}{q + 1}(p^{v+w} - p^w) + m\ell p^{v+w} \\ &\quad - p^{v+w}. \end{aligned}$$

We have

$$2g(\mathcal{C}^U)m\ell p^{v+w} = q^n(q^2 - p^w) + (q^2 - p^w) + \frac{q^n + 1}{q + 1}(p^w - p^{v+w}) - \ell(q^3 + dqp^v - dp^{v+w} - qp^v).$$

Hence,

$$g(\mathcal{C}^U) = \frac{(q^n + 1)(q^2 - p^w) + \left(\frac{q^n + 1}{q + 1}\right)(p^w - p^{v+w}) - \ell(q^3 + dqp^v - dp^{v+w} - qp^v)}{2m\ell p^{v+w}}. \quad (3.42)$$

**Example 3.2.5.** Let  $m \geq 1$ ,  $d \geq 1$  and  $0 \leq w \leq k$  be integers satisfying:

- (i)  $m \mid (q^2 - 1)$  and  $d = \gcd(m, q + 1)$
- (ii) Let  $s := \min\{r \geq 1 \mid p^r \equiv 1 \pmod{(m/d)}\}$  and assume that  $s$  divides  $w$ .

Then, there exists a subgroup  $J$  of  $A(R_\infty)$  of order  $mp^w$  by [7, Proposition 4.6] and its proof. This subgroup consists of the elements in the form  $[a, 0, c]$  with  $a^m = 1$ . Assume that  $\gcd(m, \frac{q^n + 1}{q + 1}) = 1$ . Computation of  $g(\mathcal{C}^U)$  is same as in Example 3.2.4 for  $v = 0$  i.e.,

$$d(P_\infty) = (p^w - 1)(q^n + 2) + m\ell p^w - p^w \quad (3.43)$$

and

$$\sum_{P \in \mathbb{S}, P \neq P_\infty} d(P) = (\ell - 1)q^3 + mp^w + dq - dp^w - q, \quad (3.44)$$

where  $d = \gcd(m, q + 1)$ . So, we have

$$g(\mathcal{C}^U) = \frac{(q^n + 1)(q^2 - p^w) - \ell(q^3 + dq - dp^w - q)}{2\ell m p^w}. \quad (3.45)$$

**Example 3.2.6.** We assume that  $p \neq 2$ . Let  $m$  be a divisor of  $(q^2 - 1)$  with  $m$  not dividing  $q - 1$ . Let  $s$  and  $r$  be the order of  $p$  in  $(\mathbb{Z}/m\mathbb{Z})^*$  and  $(\mathbb{Z}/\frac{m}{d}\mathbb{Z})^*$ , respectively. Then, by [2, Theorem 2] there exists a subgroup  $J$  of  $A(R_\infty)$  of order  $mp^{v+w}$  if the following conditions hold:

- (i)  $0 \leq v \leq k$ ,  $v \mid 2k$ ,  $v \nmid k$  and  $s \nmid v$
- (ii)  $\frac{v}{2} \leq w \leq k$  and  $r \mid w$ .

By the same calculations as in Example 3.2.4, we have

$$g(\mathcal{C}^U) = \frac{(q^n + 1)(q^2 - p^w) + \left(\frac{q^n + 1}{q + 1}\right)(p^w - p^{v+w}) - \ell(q^3 + dqp^v - dp^{v+w} - qp^v)}{2\ell mp^{v+w}}, \quad (3.46)$$

where  $d = \gcd(m, q + 1)$ .

**Example 3.2.7.** For  $p = 2$ , let  $s \mid k$  and  $0 \leq h \leq s$ . Then for each  $1 \leq v \leq k - 1$  with  $v = s + h$ , and for each  $s \leq w \leq k - 1$ , there exists a subgroup  $J$  of  $A(R_\infty)$  of order  $2^{v+w}$  when the value  $2^{k-v-1}(2^{k-w} - 1)$  is an integer ([2, Theorem 4]). We have

$$g(\mathcal{C}^U) = \frac{\frac{q^n + 1}{q + 1}(q^3 + q^2 - 2^{v+w} - 2^w q) + \ell(2^{v+w} - q^3)}{\ell 2^{v+w+1}}. \quad (3.47)$$

**Example 3.2.8.** Let  $k$  be even number such that 4 does not divide  $k$ . Let  $s$  be an odd integer with  $s \mid k$  and  $0 \leq h \leq s$ . Then, for each  $1 \leq v \leq k - 1$ , such that  $v = 2s + h$ , and for all  $2s \leq w \leq k - 1$  there exists a 2-subgroup  $J$  of  $A(R_\infty)$  of order  $2^{v+w}$  when  $2^{n-v-1}(2^{n-w} - 1)$  is an integer ([2, Theorem 5]). We have

$$g(\mathcal{C}^U) = \frac{\frac{q^n + 1}{q + 1}(q^3 + q^2 - 2^{v+w} - 2^w q) + \ell(2^{v+w} - q^3)}{\ell 2^{v+w+1}}. \quad (3.48)$$

**Example 3.2.9.** Let  $k = 2^e t$  with  $e, t \in \mathbb{N}$  and  $t \geq 3$  odd. For each divisor  $j$  of  $t$ , let  $h_j$  be the order of 2 in  $(\mathbb{Z}/t\mathbb{Z})^*$  and  $r_j = \frac{\Phi(j)}{h_j}$  where  $\Phi$  is the Euler function. Then for all  $1 \leq w \leq k - 2$  such that  $w = 2^e [1 + \sum_{i \neq 1} l_i h_i]$  with  $0 \leq l_i \leq r_i$ , there exists a 2-subgroup of  $A(R_\infty)$  of order  $p^{v+w}$  with  $v = w + 1$  ([2, Theorem 6]). Then by the same calculations as in example 3.2.1 for  $p = 2$  and  $v = w + 1$ , we have

$$g(\mathcal{C}^U) = \frac{\frac{q^n + 1}{q + 1}(q^3 + q^2 - 2^{2w+1} - 2^w q) + \ell(2^{2w+1} - q^3)}{\ell 2^{2w+2}}. \quad (3.49)$$

**Remark 3.2.1.** (i) For  $n = 3$ , genera of the subfields that we described in these examples coincide with the genera of the subfields corresponding to the subgroups of  $G(P_\infty)$  that were found in [4].

(ii) Our examples yield some new genera for the set  $M(q^2)$  (cf. Eqn. (1.24)) which are different from those obtained in [2], [4] and [7]. Below, we list some of new genera for  $q = 3^5, 2^{10}, 3^9$ . All of these numbers are obtained from Example 3.2.1.

$$q = 3^5 : 301, 963$$

$$q = 2^{10} : 7656, 3572, 1530, 714, 1735, 1506, 702, 300, 140, 341, 743, 156, 72, 77, 35.$$

$$q = 3^9 : 11235, 78723, 19680, 24601, 2115, 528, 661, 144, 2808, 3511, 4131, 1032, \\ 1291, 181, 291, 99, 31, 24.$$

# Bibliography

- [1] Abdon, M., Bezerra, J., Quoos, L., “Further examples of maximal curves”, J. Pure Appl. Algebra, vol. 213, no. 6, 1192-1196, 2009.
- [2] Abdon, M., Quoos, L., “On the genera of subfields of the Hermitian function field”, Finite Fields Appl., vol. 10, no. 3, 271-284, 2004.
- [3] Duursma, I., Mak, K.-H., “On maximal curves which are not Galois subcovers of the Hermitian Curve”, arXiv:1012.2068v3.
- [4] Fanali, S., Giulietti, M., “Quotient curves of the GK Curve”, arXiv:0909.2582v1.
- [5] Garcia, A., Güneri, C., Stichtenoth, H., “A generalization of the Giulietti-Korchmáros maximal curve”, Adv. Geom., vol. 10, no. 3, 427-434, 2010.
- [6] Garcia, A., Stichtenoth, H., “A maximal curve which is not a Galois subcover of the Hermitian curve”, Bull. Braz. Math. Soc. (N.S.), vol. 37, no. 1, 139-152, 2006.
- [7] Garcia, A., Stichtenoth, H., Xing, C.-P., “On subfields of the Hermitian function field”, Compositio Math., vol. 120, no. 2, 137-170, 2000.
- [8] Giulietti, M., Korchmáros, G., “A new family of maximal curves over a finite field”, Math. Ann., vol. 343, no. 1, 229-245, 2009.
- [9] Hirschfeld, J.W.P., Korchmáros, G., Torres, F., *Algebraic Curves over a Finite Field*, Princeton University Press, 2008.
- [10] Lachaud, G., “Sommes d ’Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis”, C.R. Acad. Sci. Paris Sér.I Math, vol. 305, no. 16, 729-732, 1987.



- [11] Leopoldt, H-W. “Über die Automorphismengruppe des Fermatkörpers”, J. Number Theory, vol. 56, no. 2, 256-282, 1996.
- [12] Rück, H.G., Stichtenoth, H., “Characterization of Hermitian function fields over finite fields”, J. Reine Angew. Math., vol. 457, 185-188, 1994.
- [13] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 2009.
- [14] Stichtenoth, H., “Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik I”, Arch. Math., vol. 24, 524-544, 1973.
- [15] Stichtenoth, H., “Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik II”, Arch. Math., vol. 24, 615-631, 1973.