CONTRIBUTIONS TO THE THEORY OF FUNCTION FIELDS IN POSITIVE CHARACTERISTIC

by
Burçin Güneş

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

Sabancı University
2019

Contributions to the Theory of Function Fields in Positive Characteristic

APPROVED BY

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

Assoc. Prof. Dr. Kağan Kurşungöz .....

Prof. Dr. Özgür Gürbüz .....

Prof. Dr. Massimo Giulietti .....

Assoc. Prof. Dr. Ekin Özman .....

DATE OF APPROVAL: July 19, 2019

to my beloved family

Contributions to the theory of function fields in positive characteristic

Burçin Güneş

Mathematics, PhD Dissertation, 2019

Thesis Supervisor: Prof. Dr. Cem Güneri
Thesis Co-supervisor: Asst. Prof. Nurdagül Anbar Meidl

Keywords: automorphism group, function field, Galois extension, Hermitian function field, Hurwitz's genus formula, nilpotent subgroup, maximal curve, positive characteristic

Abstract

In this thesis, we consider two problems related to the theory of function fields in positive characteristic.

In the first part, we study the automorphisms of a function field of genus $g \geq 2$ over an algebraically closed field of characteristic $p > 0$. We show that for any nilpotent subgroup G of the automorphism group, the order of G is bounded by $16(g-1)$ when G is not a p-group and by $\frac{4p}{(p-1)^2}g^2$ when G is a p-group. Also, there are examples of function fields attaining these bounds; therefore, the bounds we obtained cannot be improved.

In the second part, we focus on maximal function fields over finite fields having large automorphism groups. More precisely, we consider maximal function fields over the finite field $\mathbb{F}_{p^4}$ whose automorphism groups have order exceeding the Hurwitz's bound. We determine some conditions under which the maximal function field is Galois covered by the Hermitian function field.

Pozitif karakteristikteki Fonksiyon Cisimleri Teorisine Katkılar

Burçin Güneş

Matematik, Doktora Tezi, 2019

Tez Danışmanı: Prof. Dr. Cem Güneri
Tez Eş Danışmanı: Dr. Öğr. Üyesi. Nurdagül Anbar Meidl

Anahtar Kelimeler: fonksiyon cismi, Galois genişlemesi, Hermitsel fonksiyon cismi, Hurwitz cins formülü, maksimal eğri, otomorfizma grubu, pozitif karakteristik, sıfırkuvvetli altgrup

Özet

Bu tezde pozitif karakteristikteki fonksiyon cisimleri teorisine ilişkin iki problem ele alınmıştır.

Birinci bölümde, karakteristiği $p > 0$ olan cebirsel kapalı bir cisim üzerinde tanımlı olan ve cinsi g'nin 2'den büyük olduğu fonksiyon cisiminin otomorfizmaları çalışılmıştır. Otomorfizma grubunun herhangi bir sıfırkuvvetli altgrubu G için G'nin mertebesinin p'nin bir kuvveti olmadığı durumda bu mertebenin $16(g-1)$ ile sınırlı olduğu ve p'nin bir kuvveti olduğu durumda ise $\frac{4p}{(p-1)^2}g^2$ ile sınırlı olduğu gösterilmiştir. Ayrıca, bu sınırları sağlayan fonksiyon cisimleri örnekleri verilmiştir; böylelikle, elde edilen sınırların geliştirilemeyeceği gösterilmiştir.

İkinci bölümde, sonlu cisimler üzerine geniş otomorfizma grubu olan maksimal fonksiyon cisimlerine odaklanılmıştır. Daha açık olarak, $\mathbb{F}_{p^4}$ sonlu cismi üzerinde tanımlı ve otomorfizma grubunun mertebesi Hurwitz sınırını geçen maksimal fonksiyon cisimleri ele alınmıştır. Bazı koşullar altında Hermitsel fonksiyon cisminin bu maksimal fonksiyon cisminin Galois genişlemesi olduğu gösterilmiştir.

Acknowledgments

First and foremost, I owe my deepest gratitude to Prof. Henning Stichtenoth for his support, guidance, patience and for sharing his immense knowledge with me. I am also thankful for his valuable comments, which helped me shape this thesis' final form.

I would like to extend my sincere gratitude to my thesis supervisor Prof. Cem Güneri for his guidance and support.

I am profoundly thankful to my co-advisor Dr. Nurdagül Anbar Meidl who helped me carry my research to the next level with her endless energy, precious support and guidance.

I am thankful to all my jury members Prof. Kağan Kurşungöz, Prof. Özgür Gürbüz, Prof. Ekin Özman, Prof. Massimo Giulietti, including the former committee member Prof. Alev Topuzoğlu.

My genuine appreciation goes to the members of the Department of Mathematics of Sabancı University for providing a friendly atmosphere and stimulating environment. I am also thankful to the administrative team of Graduate School of Engineering and Natural Sciences of Sabancı University for all their help.

I feel more than lucky for having spent nine months of my Ph.D. study in Perugia. I am grateful to the members of the research group "Galois geometries and their applications" for their hospitality. I also thank Massimo Giulietti, Gabor Korchmáros, Daniele Bartoli and Maria Montanucci for encouraging and enlightening discussions. A special thanks to Prof. Massimo Giulietti for facilitating every means before and during my stay; I am humbled by his generosity.

I was supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) during my stay in Italy under the program 2214-A – International Doctoral Research Fellowship Program; thereby, I would like to thank TÜBİTAK for their support.

Last but not least, I am deeply grateful to my parents, whose love and support are with me in whatever I pursue. I would like to thank my sister, my best friend Burcu, for always encouraging me to do better. A heart-felt thank you to my dearest friends Canan, Derya, Dilek, Elif, Hazal, Özge, Türkü for their continuous support, care and patience they showed me throughout this emotional roller coaster of a Ph.D. journey.

Contents

Introduction

Many deep results on the automorphism group of a function field (of one variable) have been obtained over the course of the last decades due to demand from applications such as coding theory and cryptography. In particular, there has been a lot of research on the automorphism groups of function fields in positive characteristic, see [3, 4, 14, 23, 27] and references therein.

In this thesis, we consider two problems in this topic:

In the first problem, for a given function field, we study the relation between the size of its automorphism group and its genus. Let F/K be a function field of genus g, where K is an algebraically closed field. We denote by G, the automorphism group $\mathrm{Aut}(F/K)$ of F over K. If F/K is of genus 0 or 1, then G is an infinite group. However, for $g \geq 2$, it is a well-known fact that G is finite. This result is proved by Hurwitz [20] for $K = \mathbb{C}$ and by Schmid [33] for K of positive characteristic. In his paper, Hurwitz also showed that $|G| \leq 84(g-1)$, which is called Hurwitz's bound. This bound is sharp, i.e., there exists a function field of characteristic zero of arbitrarily high genus whose automorphism group has order $84(g-1)$, see [28]. In positive characteristic p, Roquette [31] showed that the Hurwitz's bound also holds if p does not divide $|G|$. We remark that Hurwitz's bound does not hold in general. In the positive characteristic, the best known bound is

$$|G| \leq 16g^4$$

with one exception: the Hermitian function field. This result is due to Stichtenoth [34, 35].

There are better bounds for the order of special subgroups of automorphism groups. When $K = \mathbb{C}$ and G is a nilpotent subgroup, Zomorrodian proved in [38] that

$$|G| \leq 16(g-1).$$

He also showed that if the equality holds, then $g-1$ is a power of 2; and conversely, if $g-1$ is a power of 2, then there is at least one function field of genus g with an

automorphism group of order $16(g-1)$. In the case that G is abelian, Nakajima [29] showed that $|G| \leq 4(g+1)$.

In the first part of this thesis, we give a similar bound for the order of the nilpotent subgroups of the automorphism group of a function field in positive characteristic. More precisely, our main result is as follows:

Theorem. *Let K be an algebraically closed field of characteristic $p > 0$ and F/K be a function field of genus $g \geq 2$. Suppose that G is a nilpotent subgroup of $\mathrm{Aut}(F/K)$. Then the following holds.*

(a) If G is not a p-group, then we have

$$|G| \leq 16(g-1).$$

Moreover, if $|G| = 16(g-1)$, then $g-1$ is a power of 2.

(b) If G is a p-group, then we have $|G| \leq \dfrac{4p}{(p-1)^2} g^2$.

We remark that Montanucci and Korchmáros proved independently that if G is a d-subgroup of $\mathrm{Aut}(F/K)$, where $d \neq p$, then $|G| \leq 9(g-1)$. They also showed that the equality can only be obtained for $d = 3$, see [22]. Our result agrees with their result and gives a linear bound in a more general setup, see Theorem 2.2.5 (Case (a)) and Theorem 2.2.6 (Case (b)-(iv)).

The second problem in the study of function fields over finite fields is the classification of maximal function fields.

The most well-known example of a maximal function field over the finite field $\mathbb{F}_q$, $q = \ell^2$ for some prime power ℓ, is the Hermitian function field. It has genus $\ell(\ell-1)/2$, which is the largest possible genus among all maximal function fields defined over the same finite field, see [21]. Moreover, Rück and Stichtenoth [32] showed that the Hermitian function field is the only $\mathbb{F}_q$-maximal function field of genus $\ell(\ell-1)/2$, up to isomorphism.

It is a nontrivial task to show that a function field is maximal. On the other hand, any function field covered by a maximal function field is also maximal, see [25, Propositon 6]. This result is attributed to Serre, and it is one of the main tools to obtain new genera for maximal function fields by considering the fixed fields of the subgroups of its automorphism group.

For a long time, all known maximal function fields were Galois covered by the Hermitian function field. However, Giulietti and Korchmáros gave an example of a maximal function field F for $q = \ell^6$, where $\ell > 2$ is a prime power, such that the Hermitian function field is not a Galois extension of F, see [12]. They also determined the automorphism group of F, whose order exceeds Hurwitz's bound $84(g-1)$.

Until recently, Giulietti and Korchmáros function field and some of its subfields were the only known examples of maximal function fields over $\mathbb{F}_{\ell^6}$ that are not Galois covered by the Hermitian function field. In [4], Beelen and Montanucci constructed a new family of maximal function fields $\mathcal{C}_n$ over $\mathbb{F}_{\ell^{2n}}$ for odd $n \geq 5$ and determined the full automorphism group and its order, which is $\ell(\ell^2-1)(\ell^n+1)$. They also showed that for $\ell \geq 3$, the Hermitian function field is not a Galois extension of $\mathcal{C}_n$.

It is natural to ask whether there exist other function fields that are not Galois covered, also when $q = p^2$ and $q = p^4$, where p is the characteristic of the constant field. The first open case $q = p^2$ is addressed in [2]. The authors proved that a $\mathbb{F}_{p^2}$-maximal function field F of genus at least 2, whose automorphism group has order exceeding the Hurwitz's bound, is Galois covered by the Hermitian function field.

In the second part of this thesis, we study the case $q = p^4$, i.e., maximal function fields over finite fields $\mathbb{F}_{p^4}$. This is a joint work with Daniele Bartoli and Maria Montanucci.

Our main result is as follows:

Theorem. *Let $F/\mathbb{F}_{p^4}$ be a maximal function field of genus $g \geq 2$. Suppose that G is a subgroup of the $\mathbb{F}_{p^4}$-automorphism group such that $|G| > 84(g-1)$. Then we have the following results:*

(a) G cannot admit exactly two short orbits, which are both wild.

(b) If G has only one short orbit, which is wild, then F is Galois covered by the Hermitian function field.

(c) G cannot admit exactly three short orbits, exactly two of which are tame.

The present thesis is organized as follows: In the first chapter, we introduce some basic definitions and fundamental facts about function fields and related topics which will be used in the following chapters. In the second chapter, we investigate the relation between the order of nilpotent automorphisms of function fields and its genus. Moreover, we present examples which show that the bounds are sharp. In the last chapter, we study maximal function fields with large automorphism groups. More precisely, we determine some of the conditions under which the maximal function field is Galois covered by the Hermitian function field.

1

Preliminaries

In this chapter we will introduce some preliminaries on algebraic function fields including extensions of algebraic function fields, Hilbert's ramification theory that will be used in the later sections. For the proofs and further details, we refer to [36].

1.1 Basic Concepts of Function Fields

Definition 1.1.1. *Let K be a field. An algebraic function field over K is a field extension of K such that there exists an element $x \in F$ with x is transcendental over K and $[F : K(x)]$ is finite. The full constant field of F is the subfield defined by*

$$\tilde{K} = \{\alpha \in F \ : \ \alpha \text{ is algebraic over } K\}.$$

$\tilde{K}$ is algebraically closed in F and F is also a function field over $\tilde{K}$.

Throughout F/K will denote a function field such that K is the full constant field.

Definition 1.1.2. *We say that a subring $\mathcal{O} \subseteq F$ is a valuation ring of F/K if the following properties hold.*

(i) $K \subsetneq \mathcal{O} \subsetneq F$.

(ii) For every $z \in F$, we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

A valuation ring $\mathcal{O}$ of F/K is a local ring with its unique maximal ideal $P = \mathcal{O} \backslash \mathcal{O}^{\times}$, where $\mathcal{O}^{\times} = \{z \in \mathcal{O} \ : \ \text{There is an element } w \in \mathcal{O} \text{ with } zw = 1\}$. The unique maximal ideal P is a principal ideal of $\mathcal{O}$ and if $P = t\mathcal{O}$, then each $0 \neq z \in F$ has a unique representation of the form $z = t^m u$ for some $m \in \mathbb{Z}$ and $u \in \mathcal{O}^{\times}$. Also, $\mathcal{O}$ is a principal ideal domain. More precisely, if $P = t\mathcal{O}$ and $\{0\} \neq I \subseteq \mathcal{O}$ is an ideal, then $I = t^n\mathcal{O}$ for some $n \in \mathbb{N}$.

Such a ring with these properties is called a *discrete valuation ring (DVR).*

Definition 1.1.3. *The unique maximal ideal P of some valuation ring $\mathcal{O}$ of F/K is called a place of F and any generator of P is called a prime element for P. We denote the set of all places of F by $\mathbb{P}_F$.*

Given a place P, the valuation ring $\mathcal{O}$ corresponding to P is uniquely determined by P, namely $\mathcal{O} = \{z \in F \ : \ z^{-1} \notin P\}$. Therefore, we write $\mathcal{O}_P := \mathcal{O}$.

Definition 1.1.4. *Let $P \in \mathbb{P}_F$ and t be a prime element for P. For $z \in F^\times$, write $z = t^m u$ with $m \in \mathbb{Z}$, $u \in \mathcal{O}_P^\times$. We associate P with a map*

$$v_P : F \to \mathbb{Z} \cup \{\infty\}$$

defined as follows: $v_P(z) = m$ and $v_P(0) = \infty$. v_P is called the discrete valuation of F associated with P.

This definition does not depend on the choice of the prime element t. Moreover, v_P has the following properties:

(i) $v_P(xy) = v_P(x) + v_P(y)$ for all $x, y \in F$.

(ii) $v_P(x + y) \geq \min\{v_P(x), v_P(y)\}$ for all $x, y \in F$.

(iii) If $v_P(x) \neq v_P(y)$, then $v_P(x + y) = \min\{v_P(x), v_P(y)\}$.

(iv) $v_P(a) = 0$ for all $a \in K^\times$.

Theorem 1.1.5. *[36, Theorem 1.1.13] Let F/K be a function field.*

(a) If $P \in \mathbb{P}_F$ and v_P is the discrete valuation of F associated with P, we have

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \ : \ v_P(z) \geq 0\}, \\ \mathcal{O}_P^\times &= \{z \in F \ : \ v_P(z) = 0\}, \\ P &= \{z \in F \ : \ v_P(z) > 0\}. \end{aligned}$$

(b) An element $x \in F$ is prime for P if and only if $v_P(x) = 1$.

Definition 1.1.6. *The residue class field of F at a place P is the field $F_P := \mathcal{O}_P/P$.*

Since $K \subseteq \mathcal{O}_P$ and $K \cap P = \{0\}$, K can be embedded in F_P; therefore, the following definition makes sense. The *degree of P* is defined as the degree of the field extension F_P over K, i.e., $\deg P = [F_P : K]$. A place of degree one is called a rational place. Note that if K is algebraically closed, then all places of F are rational. If $P \in \mathbb{P}_F$ and $0 \neq x \in P$, we have

$$\deg P \leq [F : K(x)] < \infty.$$

In particular, the degree of a place is always finite.

Definition 1.1.7. *Let $z \in F$ and $P \in \mathbb{P}_F$. If $v_P(z) = m > 0$, we say that P is a zero of z of order m; if $v_P(z) = -m < 0$, we say that P is a pole of z of order m.*

Remark 1.1.8. Let $z \in F$ be transcendental over K. Then z has at least one zero and one pole. In particular, $\mathbb{P}_F \neq \emptyset$. In fact, every function field has infinitely many places. On the other hand, a nonzero element has only finitely many zeros and poles.

Example 1.1.9. An important example of an algebraic function field is the rational function field, that is, $F = K(x)$ for some $x \in F$ which is transcendental over K. For an irreducible monic polynomial $p(x) \in K[x]$, we have a valuation ring

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \ : \ f, g \in K[x],\ p(x) \nmid g(x) \right\}.$$

Then

$$\mathcal{O}_{p(x)}^{\times} = \left\{ \frac{f(x)}{g(x)} \ : \ f, g \in K[x],\ p(x) \nmid f(x),\ p(x) \nmid g(x) \right\}.$$

Hence, the place associated to $\mathcal{O}_{p(x)}$ is

$$P_{p(x)} := \mathcal{O}_{p(x)} \setminus \mathcal{O}_{p(x)}^{\times} = \left\{ \frac{f(x)}{g(x)} \ : \ f, g \in K[x],\ p(x) | f(x),\ p(x) \nmid g(x) \right\}. \tag{1.1}$$

We denote by $(x = a)$, the place P_{x-a}. It is the zero of $x - a$.

Another valuation ring of $K(x)$ is given by

$$\mathcal{O}_{\infty} := \left\{ \frac{f(x)}{g(x)} \ : \ f, g \in K[x],\ \deg f(x) \leq \deg g(x) \right\},$$

whose associated place is

$$P_{\infty} := \left\{ \frac{f(x)}{g(x)} \ : \ f, g \in K[x],\ \deg f(x) < \deg g(x) \right\}. \tag{1.2}$$

We denote the place P_{∞} by $(x = \infty)$. It is called the *infinite place* of $K(x)$ and it is the only pole of x.

Remark 1.1.10. The places $P_{p(x)}$ and P_{∞}, defined by (1.1) and (1.2), give rise to all the places of $K(x)/K$.

Definition 1.1.11. *A divisor D of F is an element of the free abelian group* $\mathrm{Div}(F)$ *(written additively) generated by the places of F/K, i.e., a divisor is a formal sum*

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ with } \ n_P \in \mathbb{Z}, \ \ n_P = 0 \text{ for all but finitely many } P \in \mathbb{P}_F.$$

The support of D is defined as

$$\text{supp}D := \{P \in \mathbb{P}_F \ : \ n_P \neq 0\}.$$

The addition in $\text{Div}(F)$ is coefficientwise, i.e., if $D = \sum_{P \in \mathbb{P}_F} n_P P$ and $D' = \sum_{P \in \mathbb{P}_F} m_P P$ are two divisors of F then

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + m_P)P.$$

The zero element of the divisor group $\text{Div}(F)$ is the divisor

$$0 := \sum_{P \in \mathbb{P}_F} r_P P, \text{ with all } r_P = 0.$$

For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \text{Div}(F)$ we define $\upsilon_Q(D) := n_Q$, therefore

$$\text{supp}D = \{P \in \mathbb{P}_F \ : \ \upsilon_P(D) \neq 0\} \textit{ and } D = \sum_{P \in \text{supp}D} \upsilon_P(D)P.$$

A partial ordering on Div(F) is defined by

$$D_1 \leq D_2 \quad :\Leftrightarrow \quad \upsilon_P(D_1) \leq \upsilon_P(D_2) \textit{ for all } P \in \mathbb{P}_F.$$

If $D_1 \leq D_2$ and $D_1 \neq D_2$, we will also write $D_1 < D_2$. A divisor $D \geq 0$ is called positive (or effective). The degree of a divisor is defined as

$$\deg D := \sum_{P \in \mathbb{P}_F} \upsilon_P(D) \cdot \deg P,$$

and this yields a homomorphism $\deg : \text{Div}(F) \to \mathbb{Z}$.

Definition 1.1.12. *Let $0 \neq z \in F$. Let Z and N denote the set of its zeros and poles, respectively. Then we define*

$$\begin{aligned} (z)_0 &:= \sum_{P \in Z} \upsilon_P(z)P, \\ (z)_\infty &:= \sum_{P \in N} (-\upsilon_P(z))P, \\ (z) &:= (z)_0 - (z)_\infty; \end{aligned}$$

which are called the zero divisor, the pole divisor and the principal divisor of z, respectively.

The number of zeros of z is equal to the number of poles of z, both counted with

multiplicity; in particular, $\deg(z)_0 = \deg(z)_\infty = [F : K(z)]$ ([36, Theorem 1.4.11]). Therefore, (z) has degree zero.

The set of principal divisors of F form a subgroup

$$\mathrm{Princ}(F) := \{(z) \ : \ z \in F^\times\}$$

of $\mathrm{Div}(F)$. The divisor class group of F is the quotient group

$$\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F).$$

The corresponding equivalence relation on $\mathrm{Div}(F)$ is given by

$$D_1 \sim D_2 \quad \Leftrightarrow \quad [D_1] = [D_2] \in \mathrm{Cl}(F).$$

Definition 1.1.13. *For a divisor $A \in \mathrm{Div}(F)$, the Riemann-Roch space associated to A (or $\mathscr{L}$-space of A) is the following vector space over K:*

$$\mathscr{L}(A) := \{z \in F \ : \ (z) \geq -A\} \cup \{0\}.$$

The dimension of $\mathscr{L}(A)$ over K is denoted by $\ell(A)$.

Note that an element $x \in F$ is in the Riemann-Roch space associated to a divisor A if and only if $\upsilon_P(x) \geq -\upsilon_P(A)$ for all $P \in \mathbb{P}_F$.

Below we collect some useful properties of Riemann-Roch spaces (see [36, Section 1.4]):

Proposition 1.1.14. *Let $A, B \in \mathrm{Div}(F)$. Then the following holds.*

(a) $\mathscr{L}(A) \neq \{0\}$ if and only if there is a positive divisor $B \sim A$.

(b) If $A \sim B$, then $\mathscr{L}(A) \cong \mathscr{L}(B)$.

(c) If $\deg A < 0$, then $\mathscr{L}(A) = \{0\}$.

(d) If $A \leq B$, then $\mathscr{L}(A) \subseteq \mathscr{L}(B)$ and $\dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \deg(B) - \deg(A)$.

Note that, for a positive divisor A, we have $\ell(A) \leq \deg A + 1$ by Proposition 1.1.14 (d). Thus, for each divisor $A \in \mathrm{Div}(F)$, the Riemann-Roch space associated to A is a finite dimensional vector space over K.

Theorem 1.1.15 (Riemann-Roch Theorem)**.** *Given a function field F/K, there exist an integer g and a divisor $W \in \mathrm{Div}(F)$ such that for all divisors $A \in \mathrm{Div}(F)$ we have*

$$\ell(A) = \deg A + 1 - g + \ell(W - A).$$

Moreover, g and W are uniquely determined by F in the following sense: If g_0 and $W_0 \in \mathrm{Div}(F)$ are such that for all divisors $A \in \mathrm{Div}(F)$,

$$\ell(A) = \deg A + 1 - g_0 + \ell(W_0 - A)$$

then $g = g_0$ and $W \sim W_0$.

Hence, the following definition makes sense.

Definition 1.1.16. *The integer g in Theorem 1.1.15 is called the genus of F/K. The divisor W in Theorem 1.1.15 is called a canonical divisor of F/K.*

Corollary 1.1.17. *The genus of a function field F/K is a nonnegative integer.*

Remark 1.1.18. The rational function field $K(x)$ has genus zero.

1.2 Extensions of Function Fields

Let F/K and F'/K' be function fields where K, K' are the full constant fields. We say that F'/K' is an algebraic extension of F/K if $F' \supseteq F$ and $K' \supseteq K$ with F'/F is algebraic.

We consider algebraic extensions of functions fields and study the relation between the places of F and F'.

Definition 1.2.1. *A place $P' \in \mathbb{P}_{F'}$ is said to lie over $P \in \mathbb{P}_F$ if $P \subseteq P'$. We say that P' is an extension of P or that P lies under P', and we write $P'|P$.*

Suppose that $P \in \mathbb{P}_F$ (resp. $P' \in \mathbb{P}_{F'}$) and $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) is the corresponding valuation ring, v_P (resp. $v_{P'}$) the corresponding discrete valuation. The following are equivalent:

(i) $P'|P$.

(ii) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

(iii) There exists an integer $e \geq 1$ such that $v_{P'}(x) = e \cdot v_P(x)$ for all $x \, in F$.

Moreover, if $P'|P$, then

$$P = P' \cap F \quad \textit{and} \quad \mathcal{O} = \mathcal{O}_{P'} \cap F.$$

For this reason, P is also called the restriction of P' to F.

The integer $e(P'|P) := e$ with $v_{P'}(x) = e \cdot v_P(x)$ for all $x \in F$ is called the *ramification index* of P' over P. We say that $P'|P$ is ramified if $e(P'|P) > 1$, and $P'|P$ is unramified if $e(P'|P) = 1$. If the characteristic p of K divides we call $P'|P$ is

wildly ramified; otherwise it is called *tamely ramified*. Moreover, we call F'/F a *tame extension* if any ramified place is tamely ramified.

For a place $P' \in \mathbb{P}_{F'}$ lying over $P \in \mathbb{P}_F$, the facts that $P' \subseteq P$ and $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$ imply that there is an embedding of F_P into $F'_{P'}$ given by $x(P) \mapsto x(P')$ for all $x \in \mathcal{O}_P$. That is, $F'_{P'}$ is an extension field of F_P. The extension degree $[F'_{P'} : F_P]$ is called the *relative degree* of $P'|P$ and denoted by $f(P'|P)$.

The next proposition shows the existence of extensions of places in algebraic extensions of function fields.

Proposition 1.2.2. *Let F'/K' be an algebraic extensions of F/K.*

(a) For each place $P' \in \mathbb{P}_{F'}$ there is a unique place $P \in \mathbb{P}_F$ such that $P'|P$.

(b) Given $P \in \mathbb{P}_F$, there exists at least one, but only finitely many extensions $P' \in \mathbb{P}_{F'}$.

Theorem 1.2.3 (Fundamental Equality)**.** *Let F'/K' be a finite extension of F/K, let P be a place of F/K and let $P'_1, ..., P'_m$ be all the places of F'/K' lying over P. Then we have the following equality*

$$\sum_{i=1}^{m} e(P'_i|P) f(P'_i|P) = [F' : F].$$

Corollary 1.2.4. *Let F'/K' be a finite extension of F/K and $P \in \mathbb{P}_F$. Then we have:*

(a) $|\{P' \in \mathbb{P}_{F'} \ : \ P' \text{ lies over } P\}| \leq [F' : F]$.

(b) If $P' \in \mathbb{P}_F$ lies over P, then $e(P'|P) \leq [F' : F]$ and $f(P'|P) \leq [F' : F]$.

Definition 1.2.5. *Let F'/K' be an extension of F/K of degree $[F' : F] = n$ and $P \in \mathbb{P}_F$. We say that*

(i) P splits completely in F'/F if there are exactly n distinct places of $\mathbb{P}_{F'}$ lying over P.

(ii) P is totally ramified in F'/F if there exists a place $P' \in \mathbb{P}_{F'}$ lying over P with ramification index $e(P'|P) = n$.

For every divisor of F, we can find a divisor of F' as follows:

Definition 1.2.6. *(i) Let $P \in \mathbb{P}_F$, then* $\mathrm{Con}_{F'/F}(P) := \sum_{\substack{P' \in \mathbb{P}_{F'} \\ P'|P}} e(P'|P) \cdot P' \in \mathrm{Div}(F')$.

(ii) For $A = \sum n_P \cdot P \in \mathrm{Div}(F)$, $\mathrm{Con}_{F'/F}(A) := \sum n_P \, \mathrm{Con}_{F'/F}(P) \in \mathrm{Div}(F')$.

In particular, for a canonical divisor of F/K we can find a divisor in F'/K'. This divisor may not be a canonical divisor of F'/K' itself. However, $\mathrm{Con}_{F'/F}(W)+\mathrm{Diff}(F'/F)$ gives rise to a canonical divisor of F'/K', where W is a canonical divisor of F/K and

$$\mathrm{Diff}(F'/F) = \sum_{P\in\mathbb{P}_F} \sum_{\substack{P'\in\mathbb{P}_{F'} \\ P'|P}} d(P'|P)\cdot P',$$

see [36, Theorem 3.4.6]. Here $d(P'|P)$ is the different exponent of P' over P, whose definition can be found in [36, Definition 3.4.3].

Corollary 1.2.7 (Hurwitz's genus formula)**.** *Suppose that F/K is a function field with full constant field K, F'/K' is a function field with full constant field K' and F'/F is finite separable. Let $g := g(F)$ and $g' := g(F')$. Then*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg(\mathrm{Diff}(F'/F)).$$

Therefore, we need methods to compute $\mathrm{Diff}(F'/F)$ to calculate $g(F')$.

Lemma 1.2.8 (Transitivity of the Different)**.** *If $F'' \supseteq F' \supseteq F$ are finite separable extensions, then the following hold:*

(a) $\mathrm{Diff}(F''/F) = \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)) + \mathrm{Diff}(F''/F')$

(b) $d(P''|P) = e(P''|P')\cdot d(P'|P) + d(P''|P')$*, if P'' (resp. P', P) are places of F'' (resp. F', F) with $P'' \supseteq P' \supseteq P$.*

Consider a finite separable extension F'/F where F/K and F'/K' are algebraic function fields with constant fields K and K', respectively.

The following theorem states the relationship between $e(P'|P)$ and $d(P'|P)$.

Theorem 1.2.9 (Dedekind's Different Theorem)**.** *We have for all $P'|P$*

(a) $d(P'|P) \geq e(P'|P) - 1$.

(b) $d(P'|P) = e(P'|P) - 1$ *if and only if* $\mathrm{char}\, K$ *does not divide* $e(P'|P)$.

1.2.1 Galois Extensions of Function Fields

Given a field extension M/L,

$$\mathrm{Aut}(M/L) := \{\sigma : M \to M \mid \sigma \text{ is an isomorphism of } M \text{ and } \sigma_{\restriction L} = id_L\}.$$

We say that M/L is Galois if and only if $[M : L] < \infty$ and $|\mathrm{Aut}(M/L)| = [M : L]$ and denote the automorphism group $\mathrm{Aut}(M/L)$ by $\mathrm{Gal}(M/L)$.

From now on, we assume that K is a perfect field. We say that F'/K' is a Galois extension of F/K if F'/K' is an algebraic extension of F/K and F'/F is Galois.

Suppose that we have two function fields F'/K' and F/K with F'/K' is an algebraic extension of F/K. Fix a place $P \in \mathbb{P}_F$. Let $Q \in \mathbb{P}_{F'}$ with $Q|P$. Consider the image of Q under an automorphism σ of F'/F, i.e., consider

$$\sigma(Q) := \{\sigma(x) \ : \ x \in Q\}.$$

Clearly, $\sigma(Q)$ is the unique maximal ideal of the valuation ring $\sigma(\mathcal{O}_Q)$, therefore $\sigma(Q)$ is a place of F' with $v_{\sigma(Q)}(y) = v_Q(\sigma^{-1}(y))$ for all $y \in F'$. Moreover, $\sigma(Q)$ lies over P, $e(\sigma(Q)|P) = e(Q|P)$ and $f(\sigma(Q)|P) = f(Q|P)$.

If additionally F'/F is a Galois extension of function fields, set $G := \mathrm{Gal}(F'/F)$. Then G acts on the set of all places lying over P. Moreover, this action is transitive. In other words, if $Q_1, Q_2 \in \mathbb{P}_{F'}$ with $Q_1|P$ and $Q_2|P$, then there exists a $\sigma \in G$ such that $Q_2 = \sigma(Q_1)$, see [36, Theorem 3.7.1].

Corollary 1.2.10. *Suppose that F'/F is a Galois extension of function fields. Let $Q_1, \ldots, Q_m$ be all extensions of a place $P \in \mathbb{P}_F$ to F'. Then we have:*

(a) $e(Q_i|P) = e(Q_j|P)$ and $f(Q_i|P) = f(Q_j|P)$ for all $i, j \in \{1, \ldots, m\}$. Therefore, we can define $e(P) := e(Q_i|P)$ and $f(P) = f(Q_i|P)$.

(b) $e(P)f(P)m = [F' : F]$.

(c) $d(Q_i|P) = d(Q_j|P)$ for all $i, j \in \{1, \ldots, m\}$. We define $d(P) := d(Q_i|P)$.

In the case of K is algebraically closed, we mainly use the Orbit-Stabilizer Theorem to decide the type of the ramification. Let F, F' be function fields over K, where K is algebraically closed and let F'/F be a Galois extension with $G = \mathrm{Aut}(F'/F)$. For a place $Q \in \mathbb{P}_{F'}$, we define

$$G(Q) := \{\sigma(Q) \ : \ \sigma \in G\},$$
$$G_Q := \{\sigma \in G \ : \ \sigma(Q) = Q\}.$$

$G(Q)$ is called *orbit of* Q and G_Q is called *stabilizer of* Q in $\mathrm{Aut}(F'/F)$. The orbit is said to be *short* if $|G_Q| > 1$. Otherwise, it is called *long*. A short orbit $G(Q)$ is called *tame* (resp. *wild*) if $p \nmid |G_Q|$ (resp. $p \mid |G_Q|$).

Lemma 1.2.11. *[19, Lemma 11.41] Let G be a finite subgroup of $\mathrm{Aut}(F/K)$. Then two places of F lie over the same place of F^G if and only if they are in the same orbit under the action of G. That is, there is a one-to-one correspondence between places of F^G and G-orbits of places of F.*

Theorem 1.2.12. *[19, Theorem 11.42] Let Q be a place of F lying over a place P of F^G. If $n = |G|$ and $m = |G_Q|$, then the number of distinct places lying over P is n/m and the ramification index of each of them is $e(P) = m$.*

Remark 1.2.13. If the orbit of Q is long, then Q is unramified in F/F^G. If G has no short orbits, the extension F/F^G is unramified. In particular, G has a finite number of short orbits.

We finish this section with two special types of Galois extensions, namely Kummer and Artin-Schreier extensions.

Proposition 1.2.14. *[36, Proposition 3.7.3] Let F/K be an algebraic function field where K contains a primitive n-th root of unity (with $n > 1$ and n relatively prime to the characteristic of K). Suppose that $u \in F$ is an element satisfying*

$$u \neq w^d \text{ for all } w \in F \quad \text{and} \quad d|n, \quad d > 1 \ .$$

Let $F' = F(y)$ with $y^n = u$. Such an extension F'/F is said to be a Kummer extension of F. We have:

(a) The polynomial $\phi(T) = T^n - u$ is the minimal polynomial of y over F (in particular, it is irreducible over F).

The extension F'/F is Galois of degree $[F' : F] = n$; its Galois group is cyclic, and the automorphisms of F'/F are given by $\sigma(y) = \zeta y$, where $\zeta \in K$ is an n-th root of unity.

(b) Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ be an extension of P. Then

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

where

$$r_P := \gcd(n, v_P(u)) > 0 \tag{1.3}$$

is the greatest common divisor of n and $v_P(u)$.

(c) If K' denotes the constant field of F' and g (resp. g') the genus of F/K (resp. F'/K'), then

$$g' = 1 + \frac{n}{[K' : K]}\left(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\left(1 - \frac{r_P}{n}\right)\deg P\right),$$

where r_P is defined by Equation (1.3).

Proposition 1.2.15. *[36, Proposition 3.7.8] Let F/K be an algebraic function field of characteristic $p > 0$. Suppose that $u \in F$ is an element which satisfies the following condition:*

$$u \neq w^p - w \text{ for all } w \in F. \tag{1.4}$$

Let $F' = F(y)$ with $y^p - y = u$. Such an extension F'/F is called an Artin-Schreier extension of F. For $P \in \mathbb{P}_F$ we define the integer m_P by

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

(Observe that m_P is well-defined by [36, Lemma 3.7.7.]). We then have:

(a) F'/F is a cyclic Galois extension of degree p. The automorphisms of F'/F are given by $\sigma(y) = y + \nu$, with $\nu = 0, 1, ..., p - 1$.

(b) P is unramified in F'/F if and only if $m_P = -1$.

(c) P is totally ramified in F'/F if and only if $m_P > 0$. Denote by P' the unique place of F' lying over P. Then the different exponent $d(P'|P)$ is given by

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

(d) If at least one place $Q \in \mathbb{P}_F$ satisfies $m_Q > 0$, then K is algebraically closed in F' and

$$g' = p \cdot g + \frac{p-1}{2}\Big(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg P \Big),$$

where g' (resp. g) is the genus of F'/K (resp. F/K).

Definition 1.2.16. *Let F'/F be a Galois extension of function fields. Suppose that $P_1, \ldots, P_r$ are all the places of $\mathbb{P}_F$, which are ramified in F, with ramification indices $e_1, \ldots, e_r$ and different exponents $d_1, \ldots, d_r$, respectively. We can without loss of generality assume that $e_1 \leq \ldots \leq e_r$. In this case, we say that F is of type $(e_1, e_2, \ldots, e_r)$.*

We will later analyze the types that function fields with nilpotent automorphism groups can have.

Remark 1.2.17. Let F'/F be a Galois extension of function fields and $G = \mathrm{Gal}(F'/F)$. Suppose that $P_1, \ldots, P_r$ are all the places of $\mathbb{P}_F$, which are ramified in F, with ramification indices $e_1, \ldots, e_r$ and different exponents $d_1, \ldots, d_r$, respectively. Then by

Corollary 1.2.10, the different divisor $\mathrm{Diff}(F'/F)$ of F'/F is given by

$$\begin{aligned}\mathrm{Diff}(F'/F) &= \sum_{i=1}^{r} \sum_{\substack{Q\in\mathbb{P}_{F'}\\ Q|P_i}} d_i Q = \sum_{i=1}^{r} d_i \sum_{\substack{Q\in\mathbb{P}_{F'}\\ Q|P_i}} Q \\ &= \sum_{i=1}^{r} \frac{d_i}{e_i} \sum_{\substack{Q\in\mathbb{P}_{F'}\\ Q|P_i}} e_i Q = \sum_{i=1}^{r} \frac{d_i}{e_i} \mathrm{Con}_{F'/F}(P_i).\end{aligned}$$

Hence, by the Fundamental Equality (see Theorem 1.2.3), we have

$$\deg\left(\mathrm{Diff}(F'/F)\right) = |G| \cdot \left(\sum_{i=1}^{r} \frac{d_i}{e_i} \deg P_i\right). \tag{1.5}$$

Then Hurwitz's genus formula and Equation (1.5) yield the following formula.

$$\begin{aligned}2g(F') - 2 &= |G|(2g(F) - 2) + \deg\left(\mathrm{Diff}(F'/F)\right) \\ &= |G|\left(2g(F) - 2 + \sum_{i=1}^{r} \frac{d_i}{e_i} \deg P_i\right)\end{aligned} \tag{1.6}$$

The Equation (1.6) will be often used to estimate the order of the Galois group G.

Another tool that is often used in the study of automorphisms of function fields is the higher ramification groups.

Definition 1.2.18. *Let F'/F be a Galois extension of algebraic function fields with Galois group $G = \mathrm{Gal}(F'/F)$. Consider a place $P \in \mathbb{P}_F$ and an extension Q of P in $\mathbb{P}_{F'}$. For every $i \geq -1$ we define the i-th ramification group of $Q|P$ by*

$$G^{(i)}(Q|P) := \{\sigma \in G : v_Q(\sigma(z) - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_Q\}.$$

Clearly, $G^{(i)}(Q|P)$ is a subgroup of G. For abbreviation we write $G_Q^{(i)} := G^{(i)}(Q|P)$.

Proposition 1.2.19. *With the above notations we have:*

(a) $|G_Q^{(0)}| = e(Q|P)$.

(b) $G_Q^{(-1)} \supseteq G_Q^{(0)} \supseteq \cdots \supseteq G_Q^{(i)} \supseteq G_Q^{(i+1)} \supseteq \cdots$ *and* $G_Q^{(m)} = \{id\}$ *for m sufficiently large.*

(c) Let $\sigma \in G_Q^{(0)}$, $i \geq 0$ and let t be a Q-prime element, i.e., $v_Q(t) = 1$. Then

$$\sigma \in G_Q^{(i)} \Leftrightarrow v_Q(\sigma(t) - t) \geq i + 1.$$

(d) If $\mathrm{char}\, F = 0$, *then $G_Q^{(i)} = \{id\}$ for all $i \geq 1$, and $G_Q^{(0)}$ is cyclic.*

(e) If $\operatorname{char} F = p > 0$*, then* $G_Q^{(1)}$ *is a normal subgroup of* $G_Q^{(0)}$*. The order of* $G_Q^{(1)}$ *is a power of* p*, and the factor group* $G_Q^{(0)}/G_Q^{(1)}$ *is cyclic of order relatively prime to* p*.*

(f) If $\operatorname{char} F = p > 0$*, then* $G_Q^{(i+1)}$ *is a normal subgroup of* $G_Q^{(i)}$ *(for all* $i \geq 1$*), and* $G_Q^{(i)}/G_Q^{(i+1)}$ *is isomorphic to an additive subgroup of the residue class field* F'_Q*. Hence* $G_Q^{(i)}/G_Q^{(i+1)}$ *is an elementary abelian* p*-group of exponent* p*.*

Theorem 1.2.20 (Hilbert's Different Formula)**.** *Consider a Galois extension* F'/F *of algebraic function fields, a place* $P \in \mathbb{P}_F$ *and a place* $P' \in \mathbb{P}_{F'}$ *lying over* P*. Then the different exponent* $d(P'|P)$ *is*

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

We remark that since $G^{(i)}(P'|P) = \{id\}$ *for large* i*, the above sum is finite.*

Remark 1.2.21. Note that if $P' \in \mathbb{P}_{F'}$ is wild with ramification index $e(P'|P) = p^a E$ for some integer $a \geq 1$, $E \geq 1$ with $(p, E) = 1$, then by Hilbert's Different Formula, we have

$$d(P'|P) \geq e(P'|P) - 1 + (p^a - 1).$$

In particular, if $e(P'|P) = p^a$ for some integer $a \geq 1$, we have $d(P'|P) \geq 2(p^a - 1)$.

1.3 Group and Field Theory

1.3.1 Nilpotent Groups

Let G be a group (finite or infinite). We define the following subgroups of G inductively.

(i) $Z_0(G) = \{id\}, Z_1(G) = Z(G)$,

(ii) For $i \geq 1$, $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

(i.e., $Z_{i+1}(G)$ is the preimage in G of the center of $G/Z_i(G)$ under the canonical projection $G \to G/Z_i(G)$). Therefore, we obtain a chain of subgroups

$$1 = Z_0(G) < Z_1(G) < Z_2(G) < \ldots,$$

which is called the upper central series of G.

Definition 1.3.1. *A group* G *is called nilpotent if* $Z_n(G) = G$ *for some* $n \in \mathbb{Z}$ *and the smallest such* n *is called the nilpotency class of* G*.*

Some examples of nilpotent groups are as follows: abelian groups, finite p-groups. Note also that every subgroup and every quotient of a nilpotent group are nilpotent.

The following theorem is a well-known characterization of finite nilpotent groups.

Theorem 1.3.2. *[5, Theorem 3, Section 6.1] Let G be a finite group, let $p_1, p_2, \ldots, p_s$ be different primes dividing its order, let P_i be a Sylow p_i-subgroup of G for $1 \leq i \leq s$. Then the following are equivalent:*

(1) G is nilpotent.

(2) If $H < G$, then $H < N_G(H)$, i.e., every proper subgroup of G is a proper subgroup of its normalizer in G.

(3) $P_i \trianglelefteq G$ for $1 \leq i \leq s$, i.e., every Sylow subgroup is normal in G.

(4) $G \simeq P_1 \times P_2 \times \ldots \times P_s$.

The following lemma will be one of our main tools to give an upper bound for the order of a nilpotent subgroup of the automorphism group of a function filed.

Lemma 1.3.3. *If G is a finite nilpotent group, then G has a normal subgroup of each order dividing $|G|$.*

Proof. Since G is the direct product of its Sylow p-subgroups, it is enough to show that the statements is true for a p-group. Let G be a group of order p^n. We will proceed by induction on n. If $n = 1$ there is nothing to prove. Thus, let $n > 1$. We first show that the center $Z(G)$ of G is not trivial. Since G acts on itself by conjugation, the sum of the orders of its conjugacy classes gives the order of G. That is, we have the following equality.

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|$$

where $g_1, \ldots, g_k$ are representatives of distinct conjugacy classes of G not contained in $Z(G)$. Since $C_G(g_i) \neq G$ for $i = 1, \ldots, k$, p divides $|G : C_G(g_i)|$. Then $|Z(G)|$ is also divisible by p. Hence, $Z(G)$ is not trivial. Then let $x \in Z(G)$ be an element of order p and N be the subgroup of G generated by x. Since $N \leq Z(G)$, N is normal in G. Therefore, G/N is a group of order p^{n-1}. Hence, G/N has a normal subgroup of order p^b for every $b = 1, \ldots, n-1$. Then the preimages of these normal subgroups give arise to normal subgroups of G. of order p^i for $i = 1, \ldots, n$.

Now, if p, q are distinct primes dividing $|G|$, an element of order p and an element of order q commute. Therefore, for every divisor m of $|G|$, G has a normal subgroup of order m.

□

1.3.2 Galois Theory

Consider a Galois extension L/K with Galois group $G = \mathrm{Gal}(L/K)$. Let

$$\mathcal{U} := \{H \subseteq G \ : \ H \textit{ is a subgroup of } G\}$$

and

$$\mathcal{F} := \{E \subseteq L \ : \ E \textit{ is an intermediate field of } \ L/K\}.$$

For a subgroup H of G we define the fixed field of H by

$$L^H := \{c \in L \ : \ \sigma(c) = c \textit{ for all } \sigma \in H\}.$$

Thus we have a mapping

$$\begin{aligned} \phi : \mathcal{U} &\longrightarrow \mathcal{F} \\ H &\longmapsto L^H. \end{aligned}$$

Conversely, for an intermediate field E of L/K the extension L/E is Galois; thus, we have the mapping

$$\begin{aligned} \psi : \mathcal{F} &\longrightarrow \mathcal{U} \\ E &\longmapsto \mathrm{Gal}(L/E). \end{aligned}$$

The main results of Galois theory is collected below.

Theorem 1.3.4 (Fundamental theorem of Galois Theory)**.** *Let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$.*

(1) The maps ϕ and ψ are inverse to each other. Therefore, there is a one-to-one correspondence between $\mathcal{U}$ and $\mathcal{F}$ (Galois correspondence).

(2) For $U \in \mathcal{U}$, we have $[L : L^U] = |U|$ and $[L^U : K] = [G : U]$.

(3) For $U \in \mathcal{U}$, we have $U = \mathrm{Gal}(L/L^U)$.

(4) For $E \in \mathcal{F}$, we have $E = L^U$ with $U = \mathrm{Gal}(L/E)$.

(5) Suppose that E_1, E_2 are intermediate fields of L/K corresponding to the subgroups H_1, H_2 of G, respectively. Then $E_1 \subseteq E_2$ if and only if $H_2 \subseteq H_1$.

(6) A subgroup $U \leq G$ is normal in G if and only if the extension L^U/K is Galois. If this is the case,

$$\mathrm{Gal}(L^U/K) \cong G/U.$$

2

Automorphisms of Function Fields

2.1 Background

Throughout this chapter K is an algebraically closed field of characteristic $p > 0$ and F/K is an algebraic function field of one variable with constant field K.

Firstly, we recall the action of K-automorphisms on the set of places of F.
Let $\sigma \in \mathrm{Aut}(F/K)$ and $P \in \mathbb{P}_F$. The image $\sigma(P)$ of P is also a place of F. The action of K-automorphisms on $\mathbb{P}_F$ is given by

$$\sigma \cdot P := \sigma(P).$$

This action extends naturally to $\mathrm{Div}(F)$ as follows: Let $D \in \mathrm{Div}(F)$ with $D = \sum n_P P$. Then

$$\sigma \cdot D := \sum n_P \sigma(P).$$

In particular, σ acts on the set of positive divisors. Moreover, for any nonzero element $z \in F$, we have

$$v_{\sigma(P)}(z) = v_P(\sigma^{-1}(z)). \tag{2.1}$$

As a consequence, we obtain $\sigma \cdot (z) = (\sigma^{-1}(z))$, where (z) is the principal divisor of z. More precisely,

$$\sigma \cdot (z)_0 = (\sigma^{-1}(z))_0 \quad \text{and} \quad \sigma \cdot (z)_\infty = (\sigma^{-1}(z))_\infty. \tag{2.2}$$

Therefore, if $A, B \in \mathrm{Div}(F)$ with $A \sim B$, then $\sigma(A) \sim \sigma(B)$.

Lemma 2.1.1. *Let $\sigma \in \mathrm{Aut}(F/K)$. If $\sigma \cdot (z) = (z)$ for every nonzero element z of F, then σ is the identity automorphism of F.*

Proof. It is enough to show that $\sigma(z) = z$ for any $z \in F \setminus K$. By our assumption, we have

$$(\sigma \cdot (z)) = (z)$$

since $\sigma^{-1} \cdot (z) = (z)$. Therefore, $\left(\frac{\sigma(z)}{z}\right) = 0$, i.e., $\sigma(z) = cz$ for some nonzero $c \in K$. Replacing z by $z+1$, there exists a nonzero element $c' \in K$ such that

$$c'(z+1) = \sigma(z+1) = \sigma(z) + \sigma(1) = cz + 1.$$

Thus, $(c-c')z = c' - 1$. Since $z \in F \setminus K$, this is possible only if $c = c' = 1$. Hence $\sigma(z) = z$. □

Corollary 2.1.2. *If $\sigma \in \mathrm{Aut}(F/K)$ and σ fixes every place of F, then σ is the identity automorphism of F.*

Lemma 2.1.3. *The only automorphism of F/K fixing more than $2g+2$ places is the identity.*

Proof. Let $\sigma \in \mathrm{Aut}(F/K)$. Assume that $Q, Q_1, \ldots, Q_{2g+2}$ are all distinct places of F that are fixed by σ. By the Riemann-Roch Theorem, there are $x, z \in F$ such that $(x)_\infty = 2gQ$ and $(z)_\infty = (2g+1)Q$. Since the degrees $[F : K(x)] = 2g$ and $[F : K(z)] = 2g+1$ are relatively prime, we get $K(x,z) = F$. Note that $x - \sigma(x)$ and $z - \sigma(z)$ have at least $2g+2$ zeros (namely, $Q_1, \ldots, Q_{2g+2}$), but their pole divisor has degree at most $2g+1$ because Q is their only pole. We conclude that $\sigma(x) = x$ and $\sigma(z) = z$, then σ is the identity. □

2.1.1 Examples of Automorphism Groups of Function Fields

Example 2.1.4. Let $F = K(x)$ be the rational function field. The K-automorphism group of F has the following properties.

(a) Let $\sigma \in \mathrm{Aut}(K(x)/K)$ and $f(x) \in K[x]$. Write $f(x) = a_n x^n + \ldots + a_1 x + a_0$. Then

$$\begin{aligned}\sigma(f(x)) &= \sigma(a_n x^n + \ldots + a_1 x + a_0) = \sigma(a_n)\sigma(x^n) + \ldots + \sigma(a_1)\sigma(x) + \sigma(a_0) \\ &= a_n \sigma(x)^n + \ldots + a_1 \sigma(x) + a_0 = f(\sigma(x)).\end{aligned}$$

Also, if $\frac{f(x)}{g(x)} \in K(x)$, then $\sigma\left(\frac{f(x)}{g(x)}\right) = \frac{f(\sigma(x))}{g(\sigma(x))}$. Therefore, $\sigma(K(x)) = K(\sigma(x))$.

Now, let $z = \sigma(x) \in K(x) \setminus K$. Since $K(x) = K(z)$, we have $\sigma(x) = z = \frac{ax+b}{cx+d}$ for some $a, b, c, d \in K$ with $ad - bc \neq 0$.

Conversely, given $a, b, c, d \in K$ with $ad - bc \neq 0$, there is a unique automorphism $\sigma \in \mathrm{Aut}(K(x)/K)$ with $\sigma(x) = \frac{ax+b}{cx+d}$.

For $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, K)$, denote by σ_A, the automorphism $K(x)/K$ with $\sigma_A = \frac{ax+b}{cx+d}$. The map $A \mapsto \sigma_A$ is a homomorphism from $\mathrm{GL}(2, K)$ onto

$\mathrm{Aut}(K(x)/K)$. Its kernel is the set of diagonal matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ with $a \in K^\times$; hence,

$$\mathrm{Aut}(K(x)/K) \simeq \mathrm{GL}(2,K)/K^\times = \mathrm{PGL}(2,K).$$

In particular, $\mathrm{Aut}(K(x)/K)$ is infinite as K is infinite.

(b) By Lemma 2.1.3, we conclude that the identity of $\mathrm{Aut}(F/K)$ is the only K-automorphism fixing at least three places of F.

(c) Let $\sigma \in \mathrm{Aut}(K(x)/K)$. Then there are $a, b, c, d \in K$ with $ad - bc \neq 0$ such that $\sigma(x) = \dfrac{ax+b}{cx+d}$. If $c \neq 0$ or $c = 0$ but $a \neq d$, then the equation $aT + b = T(cT + d)$ has a solution α in K; therefore, the place $(x = \alpha)$ is fixed by σ. If $c = 0$ and $a = d$, then P_∞, the pole of x, is fixed by σ. Hence, every automorphism $\sigma \in \mathrm{Aut}(K(x)/K)$ fixes a place $P \in \mathbb{P}_{K(x)}$.

(d) Suppose $\sigma \in \mathrm{Aut}(K(x)/K)$ and $p \nmid \mathrm{ord}(\sigma)$. We consider the extension $K(x)/K(x)^\sigma$, which is of degree $\mathrm{ord}(\sigma)$; hence, $K(x)/K(x)^\sigma$ is a tame extension. Therefore, by applying Hurwitz's genus formula with respect to $K(x)/K(x)^\sigma$, we obtain exactly two tamely ramified places in $K(x)^\sigma$. Hence, σ fixes exactly two places.

(e) Suppose $\sigma \in \mathrm{Aut}(K(x)/K)$ and $p | \mathrm{ord}(\sigma)$. Then by classification of subgroups (see [19, Theorem A.8]) of $\mathrm{PGL}(2,K)$, we conclude that $\mathrm{ord}(\sigma) = p$. By applying Hurwitz's genus formula with respect to $K(x)/K(x)^\sigma$, we conclude that σ has exactly one fixed place. In fact, if the fixed place is a pole of x, the map σ is $\sigma(x) = cx + b$ for some $c, b \in K \setminus \{0\}$. Then the fact $\mathrm{ord}(\sigma) = p$ implies that $c^p = 1$, i.e., $c = 1$.

Example 2.1.5. Let E be an elliptic function field. Then the automorphism group of E/K has the following properties.

(a) We will show that $\mathrm{Aut}(E/K)$ is infinite. To this end, we fix a place $P_0 \in \mathbb{P}_E$. Let

$$\mathrm{Div}^0(E) = \{A \in \mathrm{Div}(E) \ : \ \deg A = 0\}.$$

Clearly, $\mathrm{Princ}(E) \leq \mathrm{Div}^0(E) \leq \mathrm{Div}(E)$. The factor $\mathrm{Jac}(E) := \mathrm{Div}^0(E)/\mathrm{Princ}(E)$ is called the Jacobian of E. There is a bijection Φ between $\mathbb{P}_E$ and $\mathrm{Jac}(E)$ given as follows:

$$\begin{aligned} \Phi : \ \mathbb{P}_E &\to \mathrm{Jac}(E) \\ P &\mapsto [P - P_0]. \end{aligned}$$

Then we can carry the group structure of $\mathrm{Jac}(E)$ to the set $\mathbb{P}_E$ via Φ as follows: for $P, Q \in \mathbb{P}_E$

$$P \oplus Q := \Phi^{-1}(\Phi(P) + \Phi(Q)).$$

$(P_E, \oplus)$ is an abelian group, and the zero element of the group $\mathbb{P}_E$ is the place P_0. Moreover,

$$P \oplus Q = R \Leftrightarrow P + Q \sim R + P_0.$$

For $P \in \mathbb{P}_E$, it follows from Riemann-Roch that $\ell(P + P_0) = 2$; hence, there exists an element $x \in E$ whose pole divisor is $(x)_\infty = P + P_0$. Then $[E : K(x)] = \deg(x)_\infty = 2$. Now, if $x_1, x_2 \in \mathscr{L}(P + P_0)$ such that $(x_1)_\infty = P + P_0 = (x_2)_\infty$, then $\left(\frac{x_1}{x_2}\right)_\infty = 0$. Therefore, $\left(\frac{x_1}{x_2}\right)_0 = \left(\frac{x_1}{x_2}\right) = 0$, i.e., $x_1 = cx_2$ for some $c \in K$. Hence, the following automorphisms are well-defined. Let

$$\sigma_P := \textit{the nontrivial automorphism of } E/K(x) \qquad \textit{and}$$
$$\tau_P := \sigma_P \circ \sigma_{P_0}.$$

Note that the definition of σ_P and τ_P depend on the choice of the place P_0. On the other hand, for $P \neq Q$, we have $\sigma_P \neq \sigma_Q$. Indeed, suppose $\sigma_P = \sigma_Q$. Then there are $z_1 \in \mathscr{L}(P + P_0) \setminus K$ and $z_2 \in \mathscr{L}(Q + P_0) \setminus K$ such that $K(z_1) = K(z_2)$. Therefore, $z_1 = \dfrac{az_2 + b}{cz_2 + d}$ for some $a, b, c, d \in K$ with $ad - bc \neq 0$. Thus, $P + P_0 = (z_1)_\infty = \left(\dfrac{az_2 + b}{cz_2 + d}\right)_\infty$. We investigate in three cases:

- Suppose that $c = 0$. Then $(z_1)_\infty = (\tilde{a}z_2 + \tilde{b})_\infty$ where $\tilde{a} = \dfrac{a}{d}, \tilde{b} = \dfrac{b}{d}$ with $\tilde{a} \neq 0$. Since $(z_2)_\infty = (\tilde{a}z_2 + \tilde{b})_\infty = Q + P_0$, we have $P + P_0 = Q + P_0$. Hence, $P = Q$.
- Suppose that $a = 0$. Then $(z_1)_\infty = \left(\dfrac{1}{\tilde{c}z_2 + \tilde{d}}\right)_\infty$ where $\tilde{c} = \dfrac{c}{b}, \tilde{d} = \dfrac{d}{b}$ with $\tilde{c} \neq 0$. Since $P + P_0 = (z_1)_\infty = (\tilde{a}z_2 + \tilde{b})_\infty = Q + P_0$, we have P_0 is a zero of $(\tilde{c}z_2 + \tilde{d})$, a contradiction.
- Suppose that $a, c \neq 0$. Then $(z_1)_\infty = \left(\dfrac{az_2 + b}{cz_2 + d}\right)_\infty$. Therefore, P_0 is a pole of $\frac{az_2+b}{cz_2+d}$. However, since $(z_2)_\infty = Q + P_0$, we have $v_{P_0}(az_2 + b) = v_{P_0}(cz_2 + d) = -1$. Thus, $v_{P_0}(az_2 + bcz_2 + d) = 0$, a contradiction.

Hence, we conclude that if $\sigma_P = \sigma_Q$, then $z_1 = az_2 + b$ and $P = Q$. Therefore, we also have $\tau_P \neq \tau_Q$ for $P \neq Q$. Since there are infinitely many places of E, we conclude that $\mathrm{Aut}(E/K)$ is an infinite group.

(b) For all $P, Q \in \mathbb{P}_E$, we have $\sigma_P(Q) \oplus Q = P$ and $\tau_P(Q) = P \oplus Q$. Hence, τ_P is called a *translation automorphism*. Now, the map $P \to \tau_P$ gives a group monomorphism

from $\mathbb{P}_E$ into $\mathrm{Aut}(E/K)$. Its image $T := \{\tau_P \ : \ P \in \mathbb{P}_E\} \subseteq \mathrm{Aut}(E/K)$ is isomorphic to the divisor classes $\mathrm{Jac}(E)$; hence, an infinite abelian subgroup of $\mathrm{Aut}(E/K)$. T is called the *translation group of* E/K. The translation group T is independent of the choice of the place P_0; T is a normal subgroup of $\mathrm{Aut}(E/K)$, and the factor group $\mathrm{Aut}(E/K)/T$ is finite.

Example 2.1.6. Let q be a power of the characteristic p of K. Let $\mathcal{H}$ be the Hermitian function field, that is, $\mathcal{H} = K(x, y)$ with

$$y^q + y = x^{q+1}.$$

We will consider $\mathcal{H}$ as an extension of $K(x)$ and calculate the genus of $\mathcal{H}$. For further details, see [35, Satz 1].

We first show that $\mathcal{H}/K(x)$ is of degree q. Since y satisfies the equation $T^q + T = x^{q+1}$, clearly, we have $[\mathcal{H} : K(x)] \leq q$. Conversely, let P_∞ be the pole of x in $K(x)$ and $Q_\infty \in \mathbb{P}_\mathcal{H}$ with $Q_\infty | P_\infty$. Let v_∞ be the valuation with respect to Q_∞. Then

$$v_\infty(x^{q+1}) = v_\infty(y^q + y) = v_\infty(y^q) = q \cdot v_\infty(y).$$

On the other hand, $v_\infty(x^{q+1}) = (q+1) \cdot v_\infty(x) = -(q+1)e(Q_\infty|P_\infty)$. Thus, $q | [\mathcal{H} : K(x)]$, which demonstrates $[\mathcal{H} : K(x)] = q$. Moreover, Q_∞ is totally ramified.

Next, we will show that $\mathcal{H}/K(x)$ is Galois. Note that the irreducible equation for y over $K(x)$ is

$$\varphi(T) = T^q + T - x^{q+1}.$$

Also, if $\gamma \in K$ such that $\gamma^q + \gamma = 0$, then $y + \gamma$ is also a root of $\varphi(T)$ because

$$\varphi(y + \gamma) = (y + \gamma)^q + (y + \gamma) - x^{q+1} = y^q + \gamma^q + y + \gamma - x^{q+1} = 0.$$

Since $T^q + T$ is separable, $\varphi(T)$ splits completely into linear factors over $\mathcal{H}$. In other words, $\mathcal{H}/K(x)$ is Galois.

Let $G := \mathrm{Gal}(\mathcal{H}/K(x))$. Now, we will show that all places $P \in \mathbb{P}_{K(x)} \setminus \{P_\infty\}$ are unramified in $\mathcal{H}/K(x)$. Let $P \in \mathbb{P}_{K(x)} \setminus \{P_\infty\}$. Notice that the coefficients of the minimal polynomial φ of y over $K[x]$ lies in $\mathcal{O}_P$. Therefore, from [36, Theorem 3.5.10 (a)], for all $Q|P$, we obtain $0 \leq d(Q|P) \leq v_P(\varphi'(y)) = v_P(1) = 0$, i.e., $e(Q|P) = 1$.

We will now calculate the higher ramification groups $G^{(i)}(Q_\infty|P_\infty)$. Clearly, $t := \dfrac{x}{y}$ is a prime element for Q_∞. Also,

$$\begin{aligned} v_\infty(\sigma t - t) &= v_\infty\left(\frac{x}{\sigma(y)} - \frac{x}{y}\right) = v_\infty(x) + v_\infty\left(\frac{1}{y+\gamma} - \frac{1}{y}\right) \\ &= -q + 2(q+1) = q + 2. \end{aligned}$$

Thus, for $\sigma \in G$ with $\sigma(y) = y + \gamma$ and $\gamma \neq 0$, $\sigma \in G^{(i)}(Q_\infty|P_\infty)$ if and only if $q + 2 \geq i + 1$. Therefore, the higher ramification groups $G^{(i)}(Q_\infty|P_\infty)$ are

$$G^{(i)}(Q_\infty|P_\infty) = \begin{cases} G, & \text{for } 0 \leq i \leq q+1, \\ \{id\}, & \text{for } i \geq q+2 \end{cases}$$

and, by Hilbert's Different Formula, we have

$$d(Q_\infty|P_\infty) = (q+2)(q-1).$$

Then by Hurwitz's genus formula we get

$$g := g(\mathcal{H}) = \frac{q(q-1)}{2}.$$

The automorphism group of the Hermitian Function Field:

By [15, Proposition 3.8, Theorem 3.10], we know that any automorphism of $\mathcal{H}$ is actually defined over $\mathbb{F}_{q^2}$. The automorphism group $\mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})$ is known [34, 35] and it is described as follows:

For each pair $(d, e) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ with $e^q + e = d^{q+1}$ the map $\sigma : \mathcal{H} \to \mathcal{H}$ given by $\sigma_{d,e}(x) = x + d$ and $\sigma_{d,e}(y) = y + d^q x + e$ defines an automorphism in $\mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})$. These automorphisms form a subgroup $V \subseteq \mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})$ of order q^3.

Also, for each element $c \in \mathbb{F}_{q^2}^\times$ there is an automorphism $\tau \in \mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})$ with $\tau_c(x) = cx$ and $\tau_c(y) = c^{q+1}y$. These automorphisms form a cyclic subgroup $W \subseteq \mathrm{Aut}(\mathcal{H}/K)$, which is of order $q^2 - 1$.

Now, let $U \subseteq \mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})$ be the group which is generated by V and W. Since $V \cap W = \{\mathrm{id}\}$, we obtain $|U| = q^3(q^2 - 1)$. Moreover, if $\sigma_{d,e} \in V$ and $\tau_c \in W$, then

$$\begin{aligned} \tau_c^{-1}\sigma_{d,e}\tau_c(x) &= \tau_c^{-1}\sigma_{d,e}(cx) = \tau_c^{-1}(c\sigma_{d,e}(x)) \\ &= \tau_c^{-1}(c(x+d)) = x + cd, \\ \tau_c^{-1}\sigma_{d,e}\tau_c(y) &= \tau_c^{-1}\sigma_{d,e}(c^{q+1}y) = \tau_c^{-1}(c^{q+1}\sigma_{d,e}(y)) \\ &= \tau_c^{-1}(c^{q+1}(y + d^q x + e)) = y + (cd)^q x + c^{q+1}e, \end{aligned}$$

and $(cd)^{q+1} = c^{q+1}d^{q+1} = c^{q^2-1}c^{q+1}d^{q+1} = c^{q^2+q}d^{q+1} = (c^{q+1}e)^q + (c^{q+1}e)$. Hence, if $\sigma_{d,e} \in V$ and $\tau_c \in W$, then we also obtain $\tau_c^{-1}\sigma_{d,e}\tau_c \in V$. This shows that V is normal in U. Also, since $\sigma_{d,e}$ and τ_c both stabilize Q_∞, every $\rho \in U$ stabilizes Q_∞, i.e., $\rho(Q_\infty) = \rho(Q_\infty)$.

We remark that for $\alpha \in \mathbb{F}_{q^2}$, the place $(x = \alpha)$ of $K(x)$ splits completely into places

of degree one in $\mathcal{H}/\mathbb{F}_{q^2}$. Therefore, the number $N(\mathcal{H}/\mathbb{F}_{q^2})$ of rational places in $\mathcal{H}$ is

$$N(\mathcal{H}/\mathbb{F}_{q^2}) = 1 + q^2 \cdot q = 1 + q^3.$$

Note that U acts transitively on the set

$$S := \{Q \ : \ Q \textit{ is a rational place of } \mathcal{H}/\mathbb{F}_{q^2} \ \textit{ and } \ Q \neq Q_\infty\}.$$

In fact every automorphism $\lambda \in \mathrm{Aut}(\mathcal{H}/K)$ with $\lambda(Q_\infty) = Q_\infty$ lies in U as the elements $1, x, y$ form a K-basis of $\mathscr{L}((q+1)Q_\infty)$, in particular, $\lambda(\mathscr{L}((q+1)Q_\infty)) = \mathscr{L}((q+1)Q_\infty)$.

There is an automorphism $\mu \in \mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})$ with $\mu(x) = x/y$ and $\mu(y) = 1/y$. This automorphism maps the place Q_∞ to the common zero of x and y. Hence, the group which is generated by U and μ acts transitively on the set of all rational places of $\mathcal{H}/\mathbb{F}_{q^2}$. This implies that $\mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})$ is generated by U and μ. By Orbit-Stabilizer Theorem,

$$|\mathrm{Aut}(\mathcal{H}/K)| = |\mathrm{Aut}(\mathcal{H}/\mathbb{F}_{q^2})| = q^3(q^3+1)(q^2-1) > 16g^4 > 84(g-1).$$

2.1.2 Preliminary Results

Let K be an algebraically closed field and let F/K be a function field of genus $g = g(F) \geq 2$ with constant field K. For a subgroup G of the automorphism group $\mathrm{Aut}(F/K)$, we denote the fixed field of G by F_0 and genus of F_0 by g_0 . Clearly, F/F_0 is Galois with the Galois group $\mathrm{Gal}(F/F_0) = G$.

Lemma 2.1.7. *If $g_0 \geq 1$, then $|G| \leq 4(g-1)$.*

Proof. If $g_0 \geq 2$, then by Equation (1.6), we have $2g - 2 \geq 2|G|$, i.e., $|G| \leq g - 1$. If $g_0 = 1$, then by Equation (1.6),

$$2g - 2 = |G| \left(\sum_{P \in \mathbb{P}_{F_0}} \frac{d(P)}{e(P)} \right).$$

Since $g \geq 2$, there exists a place $P \in \mathbb{P}_{F_0}$, which is ramified in F. Thus,

$$2g - 2 \geq |G| \left(\frac{e(P)-1}{e(P)} \right).$$

Hence $|G| \leq 4(g-1)$ as $e(P) \geq 2$. □

In the following lemma we consider the sequence of extensions $F_0 \subset F_1 \subset F$ such that F/F_0 and F_1/F_0 are Galois extensions with Galois groups G and G_1, respectively.

Lemma 2.1.8. *If $g_1 = g(F_1) \geq 2$, then* $\dfrac{|G|}{g-1} \leq \dfrac{|G_1|}{g_1 - 1}$.

Proof. Note that F/F_1 is an extension of degree $[G : G_1]$. Then the desired inequality comes from Hurwitz's genus formula as follows:

$$\begin{aligned} 2g-2 &= [F:F_1](2g_1-2) + \deg\left(\mathrm{Diff}(F/F_1)\right) \\ &\geq \frac{|G|}{|G_1|}(2g_1-2). \end{aligned}$$

□

2.2 Nilpotent Subgroups of Automorphisms of Function Fields

From now on, we assume that G is a nilpotent subgroup of the automorphism group $\mathrm{Aut}(F/K)$. Our aim is to give an upper bound for $|G|$ in terms of g. Let $F_0 = F^G$. Recall that by Lemma 2.1.7, we will always assume $g(F_0) = 0$. Assume that F is of type $(e_1, \ldots, e_r)$, i.e., $P_1, \ldots, P_r$ are all the places of $\mathbb{P}_{F_0}$, which are ramified in F with ramification indices $e_1 \leq \ldots \leq e_r$, respectively. Set $N = |G|$.

Lemma 2.2.1. *Let ℓ be a prime number. Then $\ell | N$ if and only if $\ell | e_i$ for some $i \in \{1, \ldots, r\}$.*

Proof. Suppose first that $\ell | e_i$ for some $i \in \{1, \ldots, r\}$. Since $e_i | N$, we have $\ell | N$. Suppose that $\ell \nmid e_i$ for any $i = 1, \ldots, r$ and $\ell | N$. Since G is nilpotent, there is a subgroup $H \lhd G$ such that $[G : H] = \ell$. Let $F_1 = F^H$. Note that F_1/F_0 is an unramified extension of degree ℓ, by Corollary 1.2.10-(b). Then by Equation (1.6) we obtain

$$2g(F_1) - 2 = \ell(-2+0) = -2\ell,$$

so that $g(F_1) = -\ell + 1 < 0$, which is impossible. □

Lemma 2.2.2. *Suppose that ℓ is a prime number which divides exactly one of $e_1, \ldots, e_r$. Then $\ell = \mathrm{char}(K)$.*

Proof. Let H be a subgroup of G such that $[G : H] = \ell$ and $F_1 = F^H$. Then there is only one place of F_0, which is ramified in F_1/F_0, say P_1. Suppose that P_1 is tamely ramified; equivalently, $\ell \neq \mathrm{char}(K)$. Then by Equation (1.6) we have

$$2g(F_1) - 2 = \ell\left(-2 + \frac{d_1}{e_1}\right) = \ell\left(-2 + \frac{\ell-1}{\ell}\right) = -\ell - 1 < 0.$$

This implies that $g(F_1) = 0$; hence, $-\ell - 1 = 2g(F_1) - 2 = -2$, which gives a contradiction. □

The next lemma gives a better lower bound on the different exponent than Remark 1.2.21 when there exists a unique wild ramification.

Lemma 2.2.3. *Let K be an algebraically closed field of characteristic $p > 0$ and F/K be a function field of genus $g \geq 2$. Suppose that G is a nilpotent subgroup of the automorphism group $\mathrm{Aut}(F/K)$ and $F_0 := F^G$ is rational. Suppose also that there exists a unique wildly ramified place of F_0, say P, with ramification index $e(P) = p^a n$ for some integers $a \geq 1$ and $n \geq 1$ where $(p, n) = 1$. Then we have*

(i) $|G| = p^a N_1$ for some integer $N_1 \geq 1$ with $\gcd(p, N_1) = 1$, i.e., $G_P^{(1)}$ is the Sylow p-subgroup of G.

(ii) $d(P) \geq (e(P) - 1) + n(p^a - 1)$.

Proof. By Lemma 2.2.1, we know that $|G| = p^t N_1$ for some $t \geq a$, where N_1 is a positive integer with $n|N_1$ and $\gcd(p, N_1) = 1$. Let H be a normal subgroup of G of index $[G : H] = p^t$ and F_1 be the fixed field of H.

(i) Note that F_1/F_0 is a Galois p-extension of degree p^t. That is, P is the only ramified in F_1/F_0 with ramification index p^a. Then by Deuring–Shafarevic formula for p-Galois extensions ([1, Corollary 2.2.]), we have

$$\gamma(F_1) - 1 = p^t(\gamma(F_0) - 1) + p^t - a(p^a - 1) = -p^{t-a}.$$

As $\gamma(F_1) \geq 0$, this is possible if and only if $t = a$ and $\gamma(F_1) = 0$, which is the desired result.

(ii) Let P' (resp., P'') be a place of F_1 (resp., of F) lying over P (resp., over P'). Note that, by Corollary 1.2.8, we have

$$d(P) = d(P''|P) = e(P''|P')d(P'|P) + d(P''|P') = nd(P'|P) + (n - 1).$$

By Remark 1.2.21, we have $d(P'|P) \geq 2(p^a - 1)$; hence,

$$d(P) \geq 2n(p^a - 1) + (n - 1) = (np^a - 1) + n(p^a - 1).$$

Then the fact that $e(P) = np^a$ gives the desired result.

□

Lemma 2.2.4. *Suppose that the number of ramified places of F_0 is greater than or equal to 5, i.e., $r \geq 5$. Then we have $N \leq 4(g - 1)$.*

Proof. By Equation (1.6) we get

$$2g - 2 = N\left(-2 + \sum_{i=1}^{r} \frac{d_i}{e_i} \right) \geq N\left(-2 + 5 \cdot \frac{1}{2} \right) = \frac{N}{2}.$$

Therefore, we obtain $N \leq 4(g - 1)$. □

From now on, we investigate the cases for which the number of ramified places of F_0 in F/F_0 less than or equal to 4. We recall that F_0 is the fixed field of G and of genus 0. We denote the number of ramified places of F_0 in F/F_0 by r.

2.2.1 Case I: $r = 4$

In this subsection, we consider F of type (e_1, e_2, e_3, e_4). That is, there are 4 ramified places of F_0, say P_1, P_2, P_3, P_4, with ramification indices e_1, e_2, e_3, e_4, respectively, such that $e_1 \leq e_2 \leq e_3 \leq e_4$.

Theorem 2.2.5. *Let F/K be a function field and G be a nilpotent subgroup of $\mathrm{Aut}(F/K)$ of order N. If $F^G = F_0$ is rational and there are exactly 4 ramified places of F_0 in F/F_0, then $N \leq 8(g-1)$.*

Case (a): Suppose that $e_2 \geq 3$. We will show that $N \leq 4(g-1)$.
By Equation (1.6), we have

$$2g-2 = N\bigg(-2+\sum_{i=1}^{4}\frac{d_i}{e_i}\bigg) \geq N\bigg(-2+\frac{1}{2}+3\cdot\frac{2}{3}\bigg) = \frac{N}{2}.$$

Therefore, $N \leq 4(g-1)$.

Case (b): Suppose that $e_2 = 2$. We will show that $N \leq 8(g-1)$.
In this case, we have $e_1 = e_2 = 2$. Similarly, by Equation (1.6) if $e_3 \geq 4$, then we again have $N \leq 4(g-1)$. Hence, we suppose that $e_3 < 4$.
We first suppose that $e_3 = 3$. If $e_4 \geq 6$, then

$$2g-2 \geq N\bigg(-2+2\cdot\frac{1}{2}+\frac{2}{3}+\frac{5}{6}\bigg) = \frac{N}{2},$$

implying $N \leq 4(g-1)$.
The case $e_4 = 5$ is impossible by Lemma 2.2.2. That is, F is either of type $(2,2,3,4)$ or of type $(2,2,3,3)$.

(i) Assume that F is of type $(2,2,3,4)$. We will show $N < 2(g-1)$.
In this case, by Lemma 2.2.2, $\mathrm{char}(K) = 3$ and by Lemma 2.2.3-(i) $N = 2^a 3$ with $a \geq 2$. Let H be a normal subgroup of G of index $[G:H] = 2^a$, and $F_1 = F^H$, i.e., F_1/F_0 is a Galois extension of degree 2^a. Then P_1, P_2, P_4 are tamely ramified and P_3 is unramified in F_1/F_0. Thus, by Equation (1.6), we have

$$2g(F_1)-2 = 2^a\bigg(-2+\frac{1}{2}+\frac{1}{2}+\frac{3}{4}\bigg) < 0.$$

That is, $g(F_1) = 0$; hence, $2g(F_1) - 2 = -2 = 2^a \cdot (-\frac{1}{4})$. This implies that $a = 3$. Note that there are 8 places lying over P_3 and each of them is wildly ramified in F/F_1. Applying Hurwitz's genus formula with respect to the extension F/F_1, we obtain

$$2g - 2 \geq 3\bigg(-2 + 8 \cdot \frac{2(3-1)}{3} \bigg) = 3\bigg(-2 + \frac{32}{3} \bigg) > 8 \cdot 3 = N,$$

i.e., we have $N < 2(g-1)$.

(ii) Assume that F is of type $(2, 2, 3, 3)$. We will show that $N \leq 6(g-1)$.
Similarly, by Lemma 2.2.1, $N = 2^a 3^b$ where $a, b \in \mathbb{N}$ with $a, b \geq 1$. We will analyze the cases separately.

(1) Assume that $\mathrm{char}(K) = 2$.
Let H be a normal subgroup of G of index $[G : H] = 3^b$ and $F_1 = F^H$. Then P_1, P_2 are unramified and P_3, P_4 are tamely ramified in F_1/F_0 . Thus, by Equation (1.6), we have

$$2g(F_1) - 2 = 3^b\bigg(-2 + \frac{2}{3} + \frac{2}{3} \bigg) = 3^b \cdot \frac{-2}{3} < 0.$$

That is, $g(F_1) = 0$; hence, $b = 1$ and $N = 3 \cdot 2^a$. Note that there are 6 places of F_1 lying over P_1, P_2. Moreover, each of them is ramified in F/F_1 with a different exponent $\geq 2(2-1)$. Then applying Equation (1.6) to the extension F/F_1, we see that

$$2g - 2 \geq 2^a\bigg(-2 + 6 \cdot \frac{2(2-1)}{2} \bigg) = 4 \cdot 2^a > 3 \cdot 2^a = N,$$

i.e., $N < 2(g-1)$.

(2) Assume that $\mathrm{char}(K) = 3$.
Let H be a normal subgroup of G of index $[G : H] = 2^a$ and $F_1 = F^H$; so that F_1/F_0 is a Galois extension of degree 2^a. Then P_1, P_2 are tamely ramified and P_3, P_4 are unramified in F_1/F_0. Thus, by Equation (1.6), we have

$$2g(F_1) - 2 = 2^a\bigg(-2 + 2 \cdot \frac{1}{2} \bigg) = -2^a < 0.$$

That is, $g(F_1) = 0$; hence, $a = 1$ and $N = 2 \cdot 3^b$. Note that there are 4 places of F_1 lying over P_3, P_4. Moreover, each of them is ramified in F/F_1 with a different exponent $\geq 2(3-1)$. Then applying Equation (1.6) to the extension F/F_1, we see that

$$2g - 2 \geq 3^b\bigg(-2 + 4 \cdot \frac{2(3-1)}{3} \bigg) = \frac{10}{3} \cdot 3^b > 2 \cdot 3^b = N,$$

i.e., $N < 2(g-1)$.

(3) Assume that $\mathrm{char}(K) \neq 2, 3$.

We will show that $N = 6$ and $g = 2$, i.e, $N = 6(g-1)$.
Let H_1, H_2 be a normal subgroups of G of index $[G : H_1] = 2^a$ and $[G : H_2] = 3^b$. We set $F_1 = F^{H_1}$ and $F_2 = F^{H_2}$; so that F_1/F_0 and F_2/F_0 are Galois extensions of degree 2^a and 3^b, respectively. Then P_1, P_2 are tamely ramified and P_3, P_4 are unramified in F_1/F_0. Similarly, P_1, P_2 are unramified and P_3, P_4 are tamely ramified in F_2/F_0. Moreover, F is the compositum of F_1 and F_2. Thus, by Equation (1.6), we have

$$2g(F_1) - 2 = 2^a\left(-2 + \frac{1}{2} + \frac{1}{2}\right) = -2^a < 0.$$

That is, $g(F_1) = 0$; hence, $a = 1$ and $N = 2 \cdot 3^b$.

Now, we consider the extension F_2/F_0. By Equation (1.6) we have

$$2g(F_2) - 2 = 3^b\left(-2 + \frac{2}{3} + \frac{2}{3}\right) = 3^b \cdot \frac{-2}{3} < 0.$$

That is, $g(F_2) = 0$; hence, $b = 1$. In particular, we have $N = 6$ and by Equation (1.6), we obtain that $g = 2$, since

$$2g - 2 = 6\left(-2 + 2 \cdot \frac{1}{2} + 2 \cdot \frac{2}{3}\right) = 2.$$

Note that in this case G is cyclic group of order 6 and $N \leq 6(g-1)$.

Now, we consider the case $e_3 = 2$.
Write $e_4 = 2^s m$ where $s \geq 0$ and m is an odd integer, i.e., F is of type $(2, 2, 2, 2^s m)$. We investigate into two cases.

(1) Assume that $m > 1$. We will show that $N < 3(g-1)$.
Note that m cannot have more than one prime divisor by Lemma 2.2.2. That is, $m = p^t$ for some prime number $p > 2$, $t \geq 1$. Hence, $p = \mathrm{char}(K)$ and $N = 2^a p^b$ for some integers a, b with $a \geq \max\{1, s\}$, $b \geq t$. Note that there is a unique wild ramification, we get $b = t$ by Lemma 2.2.3–(i). Let H be a normal subgroup of G of index $[G : H] = p^t$ and $F_1 = F^H$ so that F_1/F_0 is a Galois extension of degree p^t. Since P_1, P_2, P_3 split in F_1/F_0, i.e., there are $3p^b$ places tamely ramified in F/F_1 ramified with ramification indices 2. Then by applying Equation (1.6) for F/F_1 we obtain the following equalities.

$$\begin{aligned} 2g - 2 &= 2^a\left(2g(F_1) - 2 + 3p^t \cdot \frac{1}{2}\right) \\ &= 2^a(2g(F_1) - 2) + 2^{a-1} \cdot 3 \cdot p^t \\ &\geq p^t \cdot 2^a + 2^{a-1}(p^t - 4) \\ &= N + 2^{a-1}(p^t - 4). \end{aligned} \tag{2.3}$$

If $p^t \neq 3$, then $p^t > 4$. Therefore, by Equation (2.3) we have $N < 2(g-1)$. Suppose $p^t = 3$, then $N = 3 \cdot 2^a$. Thus, by Equation (2.3), we obtain

$$2g - 2 \geq N + 2^{a-1}(3-4) = 2^a \cdot 3 - 2^{a-1} = N - \frac{N}{6},$$

which implies $N \leq \frac{12}{5}(g-1) < 3(g-1)$.

(2) Assume that $m = 1$. We will show that $N \leq 8(g-1)$.
That is, F is of type $(2, 2, 2, 2^s)$. Then $s \geq 1$ and $N = 2^a$ for some integer $a \geq s$. If $\mathrm{char}(K) = 2$, then $N \leq g - 1$. Suppose that $\mathrm{char}(K) > 2$. Then P_1, P_2, P_3, P_4 are all tamely ramified in F/F_0; hence, by Equation (1.6) we have

$$2g - 2 = N\left(-2 + 3 \cdot \frac{1}{2} + \frac{2^s - 1}{2^s}\right).$$

Therefore $s \geq 2$ since $g \geq 2$ and $N = \frac{2^{s+1}}{2^{s-1} - 1}(g-1) \leq 8(g-1)$.

The above calculations gives the desired result stated in Theorem 2.2.5.

2.2.2 Case II. $r = 3$

In this subsection, we consider F of type (e_1, e_2, e_3). That is, there are 3 ramified places of F_0, say P_1, P_2, P_3, with ramification indices e_1, e_2, e_3, respectively, such that $e_1 \leq e_2 \leq e_3$.

Theorem 2.2.6. *Let F/K be a function field and G be a nilpotent subgroup of $\mathrm{Aut}(F/K)$ of order N. If $F^G = F_0$ is rational and there are exactly 3 ramified places of F_0 in F/F_0, then $N \leq 16(g-1)$.*

Case (a): Assume that $e_1 \geq 4$. We will show that $N \leq 8(g-1)$.
By Equation (1.6), we obtain

$$2g - 2 \geq N\left(-2 + 3 \cdot \frac{3}{4}\right) = \frac{N}{4}.$$

Therefore, $N \leq 8(g-1)$.
Case (b): Suppose that $e_1 = 3$. We will show that $N \leq 9(g-1)$.

(i) Assume that $e_2 \geq 6$.
By Equation (1.6) we have

$$2g - 2 \geq N\left(-2 + \frac{2}{3} + 2 \cdot \frac{5}{6}\right) = \frac{N}{3}.$$

Therefore, $N \leq 6(g-1)$.

(ii) Assume now that $e_2 = 5$.
Thus, F is of type $(3, 5, e_3)$. By Lemma 2.2.2, e_3 can have at most one prime divisor $p \neq 3, 5$. We write $e_3 = 3^a 5^b p^c$ for some prime number $p \neq 3, 5$ and $a, b, c \geq 0$. Then $N = 3^k 5^l p^m$ for some $k \geq \max\{1, a\}$, $l \geq \max\{1, b\}$ and $m \geq c$. If $c > 0$, then both a and b are positive and $\operatorname{char} K = p$. Moreover, as P_3 is the unique wildly ramified place, by Lemma 2.2.3 (i), $N = 3^k 5^l p^c$. Now, let H be a normal subgroup of G of index $[G : H] = 3^k$ and F_1 be the fixed field of H; so that F_1/F_0 is an extension of degree 3^k and P_1, P_3 are the only ramified places of F_0 in F_1/F_0. Applying Hurwitz's genus formula with respect to F_1/F_0, we get

$$2g(F_1) - 2 = 3^k \left(-2 + \frac{2}{3} + \frac{3^a - 1}{3^a} \right) < 0.$$

Therefore, $g(F_1) = 0$ and $k = 1$. Similarly, we can show that $l = 1$. Hence, $e_3 = 15p^c$. Thus, by Equation (1.6) and Lemma 2.2.3 (ii), we obtain

$$\begin{aligned} 2g - 2 &\geq N \left(-2 + \frac{2}{3} + \frac{4}{5} + \frac{(15p^c - 1) + 15(p^c - 1)}{15p^c} \right) \\ &\geq N \left(\frac{2}{3} + \frac{4}{5} - \frac{8}{15} \right) = \frac{14N}{15} > \frac{2N}{3}, \end{aligned}$$

i.e., $N < 3(g-1)$.

Now, suppose that $c = 0$. If $a = 0$ (resp. $b = 0$), then $\operatorname{char} K = 3$ (resp. $\operatorname{char} K = 5$) and $b = 1$ (resp. $a = 1$). Thus, there is a unique wild ramification; hence,

$$2g - 2 \geq N \left(-2 + \frac{2(3-1)}{3} + 2 \cdot \frac{4}{5} \right) > \frac{2N}{3}$$

$\left(\text{resp. } 2g - 2 \geq N \left(-2 + 2\frac{2}{3} + \frac{2(5-1)}{5}\right) > \frac{2N}{3}\right)$. Hence, $N < 3(g-1)$.
If $a, b > 0$, then $e_3 \geq 15$. Then we have

$$2g - 2 \geq N \left(-2 + \frac{2}{3} + \frac{4}{5} + \frac{14}{15}) \right) = \frac{2N}{5};$$

hence, we obtain $N \leq 5(g-1)$.

(iii) Assume that $e_2 = 4$.
Then F is of type $(3, 4, e_3)$. By Lemma 2.2.2, e_3 can have at most one prime divisor $p \neq 2, 3$. We write $e_3 = 2^a 3^b p^c$ for some prime $p \neq 2, 3$ and $a, b, c \geq 0$. Then $N = 2^k 3^l p^m$ for some $k \geq \max\{2, a\}$, $l \geq \max\{1, b\}$ and $m \geq c$. If $c > 0$, then both a and b are positive. Then $\operatorname{char} K = p$. Moreover, as P_3 is the unique wildly ramified place, by Lemma 2.2.3 (i), $N = 2^k 3^l p^c$.

Now, let H be a normal subgroup of G of index $[G:H] = 3^l$ and F_1 be the fixed field of H, i.e., F_1/F_0 is a Galois extension of degree 3^l. Then only P_1 and P_3 are ramified in F_1/F_0. Applying Hurwitz's genus formula with respect to F_1/F_0 we get

$$2g(F_1) - 2 = 3^l\bigg(-2 + \frac{2}{3} + \frac{3^b - 1}{3^b}\bigg) < 0.$$

Thus, $g(F_1) = 0$ and $b = l = 1$. Similarly, we can show that $a = k = 2$. Hence, $e_3 = 12p^c$. Thus, by Equation (1.6) and Lemma 2.2.3 (ii), we get

$$\begin{aligned} 2g - 2 &\geq N\bigg(-2 + \frac{2}{3} + \frac{3}{4} + \frac{(12p^c - 1) + 12(p^c - 1)}{12p^c}\bigg) \\ &= N\bigg(\frac{2}{3} + \frac{3}{4} - \frac{13}{12p^c}\bigg) \geq N\bigg(\frac{2}{3} + \frac{3}{4} - \frac{13}{60}\bigg) > N, \end{aligned}$$

i.e., $N < 2(g-1)$.

Now, suppose that $c = 0$. If $a = 0$ (resp. $b = 0$), then $\operatorname{char} K = 2$ (resp. $\operatorname{char} K = 3$) and $b = 2$ (resp. $a = 1$). Thus, there is a unique wild ramification; hence,

$$2g - 2 \geq N\bigg(-2 + 2 \cdot \frac{2}{3} + \frac{2(4-1)}{4}\bigg) = \frac{5N}{6}.$$

$\Big($resp. $2g - 2 \geq N\left(-2 + 2 \cdot \frac{3}{4} + \frac{2(3-1)}{4}\right) = \frac{5N}{6}\Big)$. Therefore, $N < 3(g-1)$.

Suppose now that $a, b > 0$. Then $e_3 \geq 6$. Moreover, if $\operatorname{char} K \neq 2, 3$, then we have $a = k = 2$ and $b = l = 1$, i.e $e_3 = 12$. Therefore,

$$2g - 2 = N\bigg(-2 + \frac{2}{3} + \frac{3}{4} + \frac{11}{12}\bigg) = \frac{N}{3},$$

i.e., $N \leq 6(g-1)$.

If $\operatorname{char} K = 2$ (resp. $\operatorname{char} K = 3$), then we again have $b = l = 1$ (resp. $a = k = 2$) and there are two wildly ramified places P_2, P_3 (resp. P_1, P_3). Therefore, by Equation (1.6) and Lemma 2.2.3 (ii), we have

$$\begin{aligned} 2g - 2 &\geq N\bigg(-2 + \frac{2}{3} + \frac{2(4-1)}{4} + \frac{(3 \cdot 2^a - 1) + (2^a - 1)}{3 \cdot 2^a}\bigg) \\ &\geq N\bigg(\frac{3}{2} - \frac{2}{6}\bigg) > N \end{aligned}$$

$\Big($resp. $2g - 2 \geq N\left(-2 + \frac{2(3-1)}{3} + \frac{3}{4} + \frac{(4 \cdot 3^b - 1) + (3^b - 1)}{4 \cdot 3^b}\right) \geq N\left(\frac{4}{3} - \frac{1}{6}\right) > N\Big)$. Therefore $N < 2(g-1)$.

(iv) Assume that $e_2 = 3$.

Then F is of type of the form $(3, 3, e_3)$. By Lemma 2.2.2, e_3 can have at most one prime divisor $p \neq 3$. We write $e_3 = 3^a p^b$ for some $a, b \geq 0$ with $e_3 \geq 3$.

Then $N = 3^k p^l$ for some $k \geq \max\{1, a\}$ and $l \geq b$. If $b > 0$, then $\operatorname{char} K = p$. Then P_3 is the unique wildly ramified place. Hence, by Lemma 2.2.3, $d(P_3) \geq (3^a p^b - 1) + 3^a(p^b - 1)$ and $N = 3^k p^b$. Applying Hurwitz's genus formula with respect to F/F_0, we get

$$2g - 2 \geq N\bigg(-2 + 2 \cdot \frac{2}{3} + \frac{(3^a p^b - 1) + 3^a(p^b - 1)}{3^a p^b}\bigg) \geq \frac{2N}{3}.$$

Hence, $N \leq 3(g-1)$.
Now, suppose that $b = 0$. If $a = 1$, then $\operatorname{char} K = 3$; otherwise $g = 1$. That is, all places are wildly ramified; hence,

$$2g - 2 \geq N\bigg(-2 + 3 \cdot \frac{2(3-1)}{3}\bigg) \geq 2N.$$

Hence, $N \leq g - 1$.
If $a > 1$, then

$$2g - 2 \geq N\bigg(-2 + 2 \cdot \frac{3-1}{3} + \frac{3^a - 1}{3^a}\bigg) \geq \frac{2N}{9},$$

i.e., $N \leq 9(g-1)$.

Case (c): Suppose that $e_1 = 2$. We will show that $N \leq 16(g-1)$.
Let F be of the form $(2, e_2, e_3)$. We investigate under two cases according to characteristic of K.

(i) $\operatorname{char} K = 2$: In this case P_1 is wildly ramified, i.e., $d_1 \geq 2$; hence, by Equation (1.6), we have

$$2g - 2 \geq N\bigg(-1 + \frac{d_2}{e_2} + \frac{d_3}{e_3}\bigg).$$

If $e_2 \geq 3$, then

$$2g - 2 \geq N\bigg(-1 + 2 \cdot \frac{2}{3}\bigg) \geq \frac{N}{3},$$

i.e., we have $N \leq 6(g-1)$.
Assume that $e_2 = 2$. Then P_2 is also wildly ramified, i.e., $d_2 \geq 2$, and we get

$$2g - 2 \geq N\bigg(-2 + 2 \cdot \frac{2(2-1)}{2} + \frac{2}{3}\bigg) = \frac{2N}{3},$$

i.e., $N \leq 3(g-1)$.

(ii) $\operatorname{char}(K) > 2$:

(1) If $e_2 \geq 6$, then we have

$$2g-2 \geq N\bigg(-2+\frac{1}{2}+2\cdot\frac{5}{6}\bigg)=\frac{N}{6}.$$

Therefore, $N \leq 12(g-1)$.

(2) If $e_2 = 5$, then F is of type $(2,5,e_3)$. Then by Lemma 2.2.2, e_3 can have at most one prime divisor $p \neq 2,5$. We write $e_3 = 2^a 5^b p^c$ for some prime $p \neq 2,5$ and $a,b,c \geq 0$. Then $N = 2^k 5^l p^m$ for some $k \geq \max\{1,a\}$, $l \geq \{1,b\}$ and $m \geq c$. Let H be a normal subgroup of G of index $[G:H] = 2^k$ and F_1 be the fixed field of H, i.e F_1/F_0 is a Galois extension degree 2^k. Note that $2|e_3$ because otherwise $\operatorname{char} K = 2$. Then only P_1 and P_3 are ramified (tamely) in F_1/F_0. Applying Hurwitz's genus formula with respect to F_1/F_0, we get

$$2g(F_1)-2 = 2^k\bigg(-2+\frac{1}{2}+\frac{2^a-1}{2^a}\bigg) < 0.$$

Thus, $g(F_1) = 0$ and $a = k = 1$.
If $c > 0$, then $\operatorname{char} K = p$. Similarly as above, we get $b = l = 1$. Hence, $e_3 = 10p^c$. Then P_3 is the unique wildly ramified place. Therefore, by Lemma 2.2.3, $d(P_3) \geq (10p^c-1)+10(p^c-1)$ and $N = 10p^c$. Thus,

$$\begin{aligned} 2g-2 &\geq N\bigg(-2+\frac{1}{2}+\frac{4}{5}+\frac{(10p^c-1)+10(p^c-1)}{10p^c}\bigg) \\ &\geq \frac{14N}{15} > \frac{2N}{3}, \end{aligned}$$

i.e., $N < 3(g-1)$.
Now, suppose that $c = 0$. If $b = 0$, then $e_3 = 2$, which is impossible as $e_3 \geq 5$. Thus, $b > 0$; hence, $e_3 \geq 10$. Therefore,

$$2g-2 \geq N(-2+\frac{1}{2}+\frac{4}{5}+\frac{9}{10}) = \frac{N}{5},$$

i.e., $N \leq 10(g-1)$.

(3) If $e_2 = 4$, then F is of type $(2,4,e_3)$. Then by Lemma 2.2.2, e_3 can have at most one prime divisor $p \neq 2$. We write $e_3 = 2^a p^b$ for some prime number $p \neq 2$ and $a,b \geq 0$ with $e_3 \geq 4$. Then $N = 2^k p^l$ for some $k \geq \max\{1,a\}$ and $l \geq b$. If $b > 0$, then $\operatorname{char} K = p$ and applying Hurwitz's genus formula with respect to F/F_0, we get

$$2g-2 = N\bigg(-2+\frac{1}{2}+\frac{3}{4}+\frac{(2^a p^b-1)+(p^b-1)}{2^a p^b}\bigg) \geq \frac{N}{4}.$$

Thus, $N \leq 8(g-1)$.

Now, suppose that $b = 0$. Since $\operatorname{char} K \neq 2$, by Equation 1.6 we have

$$2g - 2 = N\bigg(-2 + \frac{1}{2} + \frac{3}{4} + \frac{2^a - 1}{2^a}\bigg) = N\bigg(\frac{1}{4} - \frac{1}{2^a}\bigg).$$

Since LHS of the above equality is greater than or equal to 2, we get $a \geq 3$. Hence, $2g - 2 \geq \dfrac{N}{8}$, i.e., $N \leq 16(g-1)$.

(4) If $e_2 = 3$, then F is of type $(2, 3, e_3)$. Then by Lemma 2.2.2, e_3 can have at most one prime divisor $p \neq 2, 3$. We write $e_3 = 2^a 3^b p^c$ for some prime number $p \neq 2, 3$ and $a, b, c \geq 0$ with $e_3 \geq 3$. Then $N = 2^k 3^l p^m$ for some $k \geq \max\{1, a\}$, $l \geq \{1, b\}$ and $m \geq c$. Let H be a normal subgroup of G of index $[G : H] = 2^k$ and F_1 be the fixed field of H, i.e., F_1/F_0 is a Galois extension of degree 2^k. Then only P_1 and P_3 can be ramified in F_1/F_0. Applying Hurwitz's genus formula with respect to F_1/F_0, we get

$$2g(F_1) - 2 = 2^k\bigg(-2 + \frac{1}{2} + \frac{2^a - 1}{2^a}\bigg) < 0.$$

Thus, $g(F_1) = 0$ and $a = k = 1$.

If $c > 0$, then $\operatorname{char} K = p$. Similarly as above, we get $b = l = 1$. Hence, $e_3 = 6p^c$. Then P_3 is the unique wildly ramified place. Therefore, by Lemma 2.2.3, $d(P_3) \geq (6p^c - 1) + 6(p^c - 1)$ and $N = 6p^c$. Then we get

$$2g - 2 \geq N\bigg(-2 + \frac{1}{2} + \frac{2}{3} + \frac{(6p^c - 1) + 6(p^c - 1)}{6p^c}\bigg) > \frac{2N}{3},$$

i.e., $N < 3(g-1)$.

Now, suppose that $c = 0$. If $b = 0$, then $e_3 = 2$, which is impossible as $e_3 \geq 3$. Then $b > 0$. Suppose that $\operatorname{char}(K) \neq 3$. Let H_1 be a normal subgroup of G of index $[G : H_1] = 3^b$ and $F_2 = F^{H_1}$ so that F_2/F_0 is a Galois extension of degree 3^b. Then applying Equation (1.6) to F_2/F_0, we observe that $b = 1$, i.e., F is of type $(2, 3, 6)$. Since F/F_0 is a tame extension, we have

$$2g - 2 = N\bigg(-2 + \frac{1}{2} + \frac{2}{3} + \frac{5}{6}\bigg) = 0,$$

which gives a contradiction as $g \geq 2$.

Therefore, we conclude that $\operatorname{char}(K) = 3$, i.e., P_2, P_3 are wildly ramified with different exponents $d_2 \geq 2(3-1)$ and $d_3 \geq 5 + 2(3-1)$. Then by Equation

(1.6), we have

$$2g-2 \geq N\bigg(-2+\frac{1}{2}+\frac{2(3-1)}{3}+\frac{5+2(3-1)}{6}\bigg)=\frac{4N}{3}>N,$$

i.e., we have $N<2(g-1)$.

(5) If $e_2=2$, then F is of type $(2,2,e_3)$. Then by Lemma 2.2.2, e_3 can have at most one prime divisor $p\neq 2$. We write $e_3=2^a p^b$ for some prime number $p\neq 2$ and $a,b\geq 0$ with $e_3\geq 2$. Then $N=2^k p^l$ for some $k\geq \max\{1,a\}$ and $l\geq b$. Suppose first that $b=0$. Since $\operatorname{char} K\neq 2$, we get

$$2g-2=N\bigg(-2+\frac{1}{2}+\frac{1}{2}+\frac{2^a-1}{2^a}\bigg)<0,$$

which is not possible as $g\geq 2$. Therefore, $b>0$. Then $\operatorname{char} K=p$. Applying Hurwitz's genus formula with respect to F/F_0 and using Lemma 2.2.3-(ii), we get

$$\begin{aligned}2g-2&=N\bigg(-2+\frac{1}{2}+\frac{1}{2}+\frac{(2^a p^b-1)+2^a(p^b-1)}{2^a p^b}\bigg)\\&=N\frac{2^a p^b-2^a-1}{2^a p^b}\geq N\bigg(1-\frac{2^a+1}{3\cdot 2^a}\bigg)\geq\frac{N}{3}.\end{aligned}$$

Hence, $N\leq 6(g-1)$.

The above calculations gives the desired result stated in Theorem 2.2.6.

2.2.3 Case III. $r=2$

In this subsection we investigate F of the form (e_1,e_2). That is, there are 2 ramified places of F_0, say P_1,P_2, with ramification indices e_1,e_2, respectively, such that $e_1\leq e_2$.

Theorem 2.2.7. *Let F/K be a function field and G be a nilpotent subgroup of $\operatorname{Aut}(F/K)$ of order N. If $F^G=F_0$ is rational and there are exactly 2 ramified places of F_0 in F/F_0, then $N\leq 10(g-1)$.*

Let $p=\operatorname{char}(K)$. Say $e_1=p^a n$, $e_2=p^b m$ for some nonnegative integers a,b and $\gcd(p,n)=\gcd(p,m)=1$. Note that a,b cannot be both zero; otherwise F/F_0 is tame; hence, by Equation (1.6), we have

$$2\leq 2g-2=N\bigg(-2+\frac{e_1-1}{e_1}+\frac{e_2-1}{e_2}\bigg)<0,$$

which is a contradiction.

Case (a): Suppose that G is a p-group.
In this case, P_1 and P_2 are wildly ramified with different exponents $d_1 \geq 2(p^a - 1)$ and $d_2 \geq 2(p^b - 1)$, respectively. Then by Equation (1.6) we have

$$2g - 2 \geq N\left(-2 + \frac{2(p^a - 1)}{p^a} + \frac{2(p^b - 1)}{p^b}\right) = N\left(2 - \frac{2}{p^a} - \frac{2}{p^b}\right).$$

If $p^a = p^b = 2$ is not the case, then we have

$$2g - 2 \geq N\left(2 - 1 - \frac{2}{4}\right) = \frac{N}{2},$$

i.e., we have $N \leq 4(g - 1)$.
If $p^a = p^b = 2$, then the case $d_1 = d_2 = 2$ cannot hold; otherwise, we would have $g = 1$. We without loss of generality suppose that $d_2 \geq 3$. Then we get

$$2g - 2 \geq N\left(-2 + 1 + \frac{3}{2}\right) = \frac{N}{2},$$

i.e., we have $N \leq 4(g - 1)$.

Case (b): Assume that G is not a p-group.
Let $|G| = N = p^t \cdot N_1$, where $t \geq \max\{a, b\}$ and $N_1 > 1$ is an integer with $\gcd(p, N_1) = 1$. Let H be a normal subgroup of G of index $[G : H] = N_1$. Set $F_1 = F^H$ and $g_1 = g(F_1)$. Note that F_1/F_0 is a tame Galois extension of degree N_1. By Equation (1.6), we conclude that $g_1 = 0$, and P_1, P_2 are both totally ramified in F_1/F_0. In particular, we conclude that $n = m = N_1$, i.e., F is of the type $(p^a N_1, p^b N_1)$.

(i) Suppose that F is of the type $(N_1, N_1 p^b)$.
Then there is only one wildly ramified place of F_0, namely, P_2; hence, by Lemma 2.2.3, we have $|G| = N_1 p^b$ and $d_2 \geq (N_1 p^b - 1) + N_1(p^b - 1)$. Then by Equation (1.6) we get

$$\begin{aligned} 2g - 2 &\geq N\left(-2 + \frac{N_1 - 1}{N_1} + \frac{(N_1 p^b - 1) + N_1(p^b - 1)}{N_1 p^b}\right) \\ &= N\left(1 - \frac{1}{N_1} - \frac{1}{N_1 p^b} - \frac{1}{p^b}\right). \end{aligned}$$

(1) Suppose $p^b \geq 5$.
Then by the facts that $p^b \geq 5$ and $N_1 \geq 2$ we have

$$2g - 2 \geq N\left(1 - \frac{1}{N_1} - \frac{1}{N_1 p^b} - \frac{1}{p^b}\right) \geq \frac{N}{5},$$

i.e., we have $N \leq 10(g - 1)$.

(2) Suppose $p^b = 4$. Then F is of the type $(N_1, 4N_1)$. Note that $\mathrm{char}(K) = 2$ and $N_1 \geq 3$. Then by Lemma 2.2.3 (ii) and Equation (1.6), we get

$$\begin{aligned} 2g-2 &\geq N\left(-2 + \frac{N_1 - 1}{N_1} + \frac{(4N_1 - 1) + N_1(4-1)}{4N_1} \right) \\ &= N\left(\frac{3}{4} - \frac{5}{4N_1} \right) \geq \frac{N}{3}, \end{aligned}$$

i.e., we have $N \leq 6(g-1)$.

(3) If $p^b = 3$, then F is of the type $(N_1, 3N_1)$. Note that $\mathrm{char}(K) = 3$ and $N_1 \geq 2$. By Lemma 2.2.3 (ii) and Equation (1.6), we get

$$\begin{aligned} 2g-2 &\geq N\left(-2 + \frac{N_1 - 1}{N_1} + \frac{(3N_1 - 1) + N_1(3-1)}{3N_1} \right) \\ &= N\left(\frac{2}{3} - \frac{4}{3N_1} \right). \end{aligned}$$

Suppose $N_1 > 2$, i.e., $N_1 \geq 4$. Then we have $2g - 2 \geq N/3$, i.e., we have $N \leq 6(g-1)$.

Now, we consider the case that F is of the type $(2, 6)$. Hence, we have $N = 6$. Applying Hurwitz's genus formula with respect to F/F_1, we obtain

$$2g - 2 \geq 3(-2 + 2(3-1)) = 6 = N.$$

Therefore, $N \leq 2(g-1)$.

(4) If $p^b = 2$, then $N \leq 10(g-1)$.
That is, F is of type $(N_1, 2N_1)$. Note that $\mathrm{char}(K) = 2$ and $N_1 \geq 3$. Then by Lemma 2.2.3 (ii) and Equation (1.6), we get

$$\begin{aligned} 2g-2 &\geq N\left(-2 + \frac{N_1 - 1}{N_1} + \frac{(2N_1 - 1) + N_1(2-1)}{2N_1} \right) \\ &= N\left(\frac{1}{2} - \frac{3}{2N_1} \right). \end{aligned} \tag{2.4}$$

If $N_1 \neq 3$, then $N_1 \geq 5$. In this case, by Equation (2.4), we get $2g-2 \geq N/5$, i.e., $N \leq 10(g-1)$.

Now, we consider the case that F is of the type $(3, 6)$. Then $N = 6$. Let H be a normal subgroup of G of index 2 and $F_2 = F^H$, i.e., F_2/F_0 is a Galois extension of degree 2. Let Q_2 be the unique place of F_2 lying over P_2 and $\tilde{Q}_2$

be the place of F lying over Q_2. Then by Lemma 1.2.8, we have

$$\begin{aligned} d(\tilde{Q}_2|P_2) &= e(\tilde{Q}_2|Q_2) \cdot d(Q_2|P_2) + d(\tilde{Q}_2|Q_2) \\ &= 3 \cdot d(Q_2|P_2) + 2. \end{aligned} \tag{2.5}$$

By Equations (1.6) and (2.5), we have

$$\begin{aligned} 2g-2 &= N\left(-2+\frac{2}{3}+\frac{d(\tilde{Q}_2|P_2)}{6}\right) \\ &= N\left(-\frac{4}{3}+\frac{3\cdot d(Q_2|P_2)+2}{6}\right) \\ &= N\left(-1+\frac{d(Q_2|P_2)}{2}\right). \end{aligned}$$

This implies that $d(Q_2|P_2) \geq 3$, since $2g-2 \geq 2$. Therefore,

$$2g-2 = N\left(-1+\frac{d(Q_2|P_2)}{2}\right) \geq \frac{N}{2},$$

i.e., $N \leq 4(g-1)$.

(ii) Suppose that F is of type (N_1p^a, N_1p^b).
Now, let H_1 be a normal subgroup of G with $[G:H_1] = p^t$ and $F_2 = F^{H_1}$, i.e., F/F_2 is an extension of degree p^t. Then applying Equation (1.6) to F_2/F_0, we have

$$2g(F_2)-2 = p^t\left(-2+\frac{d(P_1)}{p^a}+\frac{d(P_2)}{p^b}\right). \tag{2.6}$$

Note that we have $d(P_1) \geq 2(p^a-1)$ and $d(P_2) \geq 2(p^b-1)$ by Remark 1.2.21. Suppose first that $p^a = 2 = p^b$ is not the case. Then we get

$$\begin{aligned} 2g(F_2)-2 &= p^t\left(-2+\frac{d(P_1)}{p^a}+\frac{d(Q_2)}{p^b}\right) \\ &\geq p^t\left(-2+\frac{2(p^a-1)}{p^a}+\frac{2(p^b-1)}{p^b}\right) \\ &= p^t\left(2-\frac{2}{p^a}-\frac{2}{p^b}\right) \geq \frac{2p^t}{3}. \end{aligned}$$

Therefore,

$$p^t \leq 3(g(F_2)-1). \tag{2.7}$$

Moreover, since $\frac{2p^t}{3} > 0$, $g(F_2)$ is at least 2. Therefore, by Lemma 2.1.8, we also have $N \leq 3(g-1)$.

Suppose now that $p^a = p^b = 2$. In particular, $\mathrm{char}(K) = 2$. We will calculate

Diff(F/F_0) in two different ways using transitivity of different. For $i = 1, 2$, let $d_i, \tilde{d}_i$ be the different exponents of P_i in the extensions F_2/F_0 and F_1/F_0, respectively. Then by Lemma 1.2.8, we have

$$N_1 d_i + (N_1 - 1) = 2(N_1 - 1) + \tilde{d}_i,$$

i.e., $\tilde{d}_i = N_1(d_i - 1) + 1$. Then applying Equation (1.6) with respect to F/F_1, we get

$$\begin{aligned} 2g - 2 &= 2^t \left(-2 + \frac{\tilde{d}_1}{2} + \frac{\tilde{d}_2}{2} \right) \\ &= 2^t \left(-2 + \frac{N_1(d_1 - 1) + 1}{2} + \frac{N_1(d_2 - 1) + 1}{2} \right) \\ &= 2^t N_1 \left(\frac{-1}{N_1} + \frac{d_1 - 1}{2} + \frac{d_2 - 1}{2} \right) \\ &\geq N \left(\frac{-1}{3} + 1 \right) = \frac{2N}{3} \end{aligned}$$

where the last inequality comes from the facts that $d_1, d_2 \geq 2$ and $N_1 \geq 3$. Thus, we obtain $N \leq 3(g - 1)$.

The above calculations gives the desired result stated in Theorem 2.2.7.

2.2.4 Case IV. $r = 1$

Theorem 2.2.8. *Let F/K be a function field and G be a nilpotent subgroup of* Aut(F/K) *of order N. If $F^G = F_0$ is rational and there is a unique place P of F_0, which is ramified in F/F_0, then $N \leq \frac{4p}{(p-1)^2} g^2$.*

Proof. Note that P is wildly ramified. Let $p = \mathrm{char}(K)$. Then $e(P) = p^a n$ for some positive integer n with $\gcd(p, n) = 1$. Say $|G| = p^t N_1$ for some integers $t \geq a \geq 0$ and $N_1 \geq 1$. Let H be a normal subgroup of G of index $[G : H] = N_1$ and $F_1 = F^H$ of genus g_1. Then F_1/F_0 is a tame Galois extension of degree N_1. By Equation (1.6), we have

$$2g_1 - 2 = N_1 \left(-2 + \frac{n - 1}{n} \right). \tag{2.8}$$

Equation (2.8) implies that $n = N_1 = 1$. Therefore, G is a p-group, i.e., we have $N = |G| = p^t$ and $e(P) = p^a$ for some $t \geq a > 0$.
By Lemma 2.2.3-(i), P is totally ramified. In particular, we have $\gamma(F) = 0$. Then by [34, Satz 1], we conclude the desired result.

□

2.2.5 Examples

In this section, we will give examples of function fields that attain the bounds we obtained in Theorem 2.2.5, 2.2.6, 2.2.7 and 2.2.8. This implies that the bounds cannot be improved, i.e., the bounds are sharp.

The following example shows that the bound given in Theorem 2.2.6 is sharp.

Example 2.2.9. (1) Let $p \neq 2$. Consider the function field F with defining equation

$$y^2 = x(x^4 - 1).$$

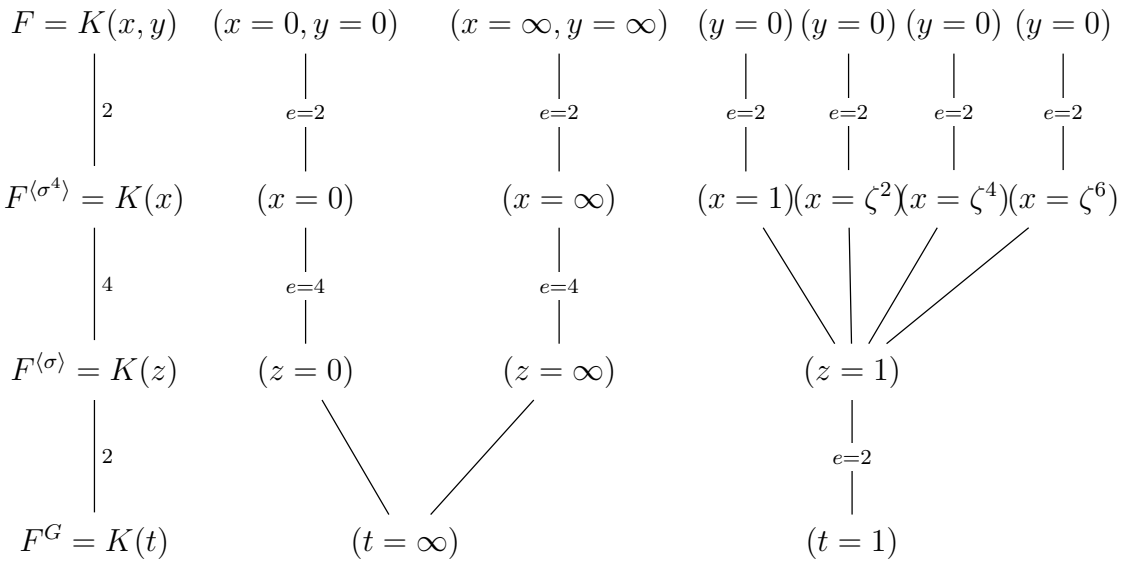
By Proposition 1.2.14, we conclude that the genus $g(F)$ of F is 2. Let ζ be a primitive 8-th root of unity. We define two maps $\sigma, \tau : F \to F$ as follows:

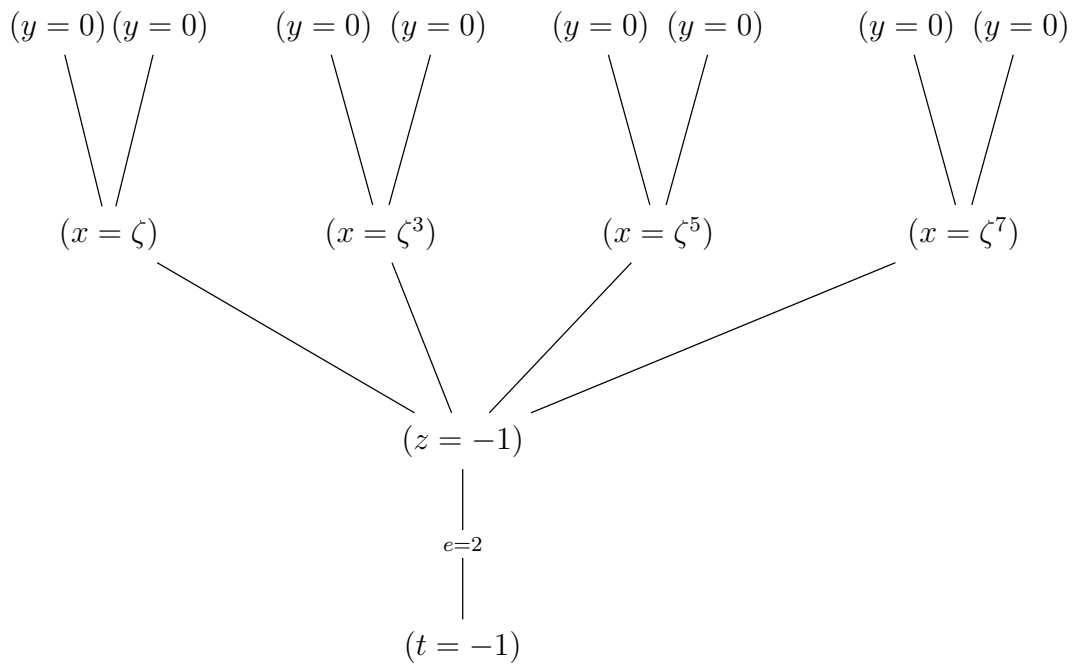
$$\sigma : \begin{cases} x \mapsto \zeta^2 x \\ y \mapsto \zeta y \end{cases} \qquad \text{and} \qquad \tau : \begin{cases} x \mapsto -1/x \\ y \mapsto y/x^3. \end{cases}$$

Then

$$\sigma(y)^2 = \zeta^2 y^2 = \zeta^2 x(x^4 - 1) = \sigma(x)(\sigma(x)^4 - 1) \quad \text{and}$$
$$\tau(y)^2 = \frac{y^2}{x^6} = \frac{x(x^4 - 1)}{x^6} = \tau(x)(\tau(x)^4 - 1).$$

Therefore, σ and τ define automorphisms of F/K. Note that $\operatorname{ord}\sigma = 8$ and $\tau^2 = \sigma^4$ so that $\operatorname{ord}\tau = 4$. Let G be the subgroup of $\operatorname{Aut}(F/K)$ generated by σ, τ, i.e., $G = \langle \sigma, \tau \rangle$. Define $z := x^4$ and $t := \dfrac{z^2 + 1}{2z}$. Since $K(t) \subseteq F^{\langle \sigma \rangle}$ and $K(t) \subseteq F^{\langle \tau \rangle}$, we have $K(t) \subseteq F^G$. Since $\tau \notin \langle \sigma \rangle$, this implies that $K(t) = F^G$. Then we have the following picture:





Note that

(i) $\tau_{\restriction K(x)}$ sends the place $(x = 0)$ to the place $(x = \infty)$, therefore, $(z = 0)$ maps to $(z = \infty)$. Also, $\tau_{\restriction K(x)}$ sends the place $(x = \infty)$ to the place $(x = 0)$, then $(z = \infty)$ maps to $(z = 0)$. Hence, $(z = 0)$ and $(z = \infty)$ lie over the same place $(t = \infty)$ of $K(t)$. Thus, $(t = \infty)$ is unramified in $K(z)/K(t)$.

(ii) $\tau_{\restriction K(x)}$ fixes the places $(z = 1)$ and $(z = -1)$. Then $(z = 1)$ and $(z = -1)$ are totally ramified in $K(z)/K(t)$. By Hurwitz's genus formula, we know that there are no other ramification in $K(z)/K(t)$.

Hence, we obtain a subgroup $G = \mathrm{Aut}(F/K(t))$ of $\mathrm{Aut}(F/K)$ of order 16 and the ramified places of $K(t)$ in F are $(t = \infty)$, $(t = 1)$ and $(t = -1)$ with ramification indices $8, 4, 2$, respectively. Thus, F is of type $(2, 4, 8)$. Therefore, $N = |G| = 16(g - 1)$.

Now, we study the group structure of G. Note that the subgroup $\langle\sigma\rangle \simeq C_8$ is normal in G, since $\operatorname{ord}\sigma = 8$ and $|G| = 16$. Moreover, we have $(\sigma\tau)^2 = \mathrm{id}_F$ and $(\sigma\tau)\sigma(\sigma\tau)^{-1} = \sigma^3$. Therefore,

$$G = \langle\sigma, \sigma\tau\rangle \simeq C_8 \rtimes_\varphi C_2,$$

where $\varphi : \langle\sigma\tau\rangle \to \mathrm{Aut}(\langle\sigma\rangle)$ is given by $\varphi_{\sigma\tau}(\sigma) = \sigma^3$.

(2) For any $m \geq 1$, F has a unique maximal unramified abelian extension F' such that $[F' : F] = 2^{4m}$, see [30, Section 4.7]. Let $\tilde{F}$ be the Galois closure of $F'/K(t)$. We first show that $\tilde{F} = F'$. To this end, let $\gamma \in \mathrm{Aut}(\tilde{F}/K(t))$. In particular,

$\gamma(t) = t$. Then $\frac{\gamma(z)^2+1}{\gamma(z)} = \frac{z^2+1}{z}$. Therefore, either $\gamma(z) = z$ or $\gamma(z) = \frac{1}{z}$. In the former case, we have $x^4 = \gamma(x^4) = \gamma(x)^4$. Hence, $\gamma(x) = \alpha x$, where α is a 4-th root of unity. Then $\gamma(y)^2 = \gamma(x)(\gamma(x)^4 - 1) = \alpha x(x^4 - 1) = \alpha y^2$. Thus, $\gamma(y) = \beta y$ with $\beta^2 = \alpha$, i.e., β is a 8-th root of unity. In the latter case, we have $\frac{1}{x^4} = \gamma(x)^4 = \gamma(x^4)$. Hence, $\gamma(x) = \alpha\frac{1}{x}$, where α is a 4-th root of unity. Then $\gamma(y)^2 = \gamma(x)(\gamma(x)^4 - 1) = \alpha\frac{1}{x}\left(\frac{1}{x^4} - 1\right) = \frac{1-x^4}{x^5} = \frac{-y^2}{x^6}$. Thus, $\gamma(y) = \beta\frac{y}{x^3}$, where $\beta^2 = -1$. Therefore, in both cases we have $\gamma(x), \gamma(y) \in F$. Hence, $\gamma(F) \subseteq F$, i.e., $\gamma(F) = F$. Moreover, we also have $\gamma(F') = F'$ since F' is the unique maximal unramified abelian extension F' such that $[F' : F] = 2^{4m}$. Therefore, $\tilde{F} = F'$. This means that we obtain a Galois extension $F'/K(t)$ having exactly 3 ramified places of $K(t)$, namely, $(t = -1)$, $(t = 1)$ and $(t = \infty)$ whose ramification indices are 2, 4, 8, respectively. Thus, F' is of type $(2, 4, 8)$. Moreover, $[F' : K(t)] = 2^{4m+4}$ and $g(F') = 2^{4m} + 1$, that is, $[F' : K(t)] = 16 \cdot (g(F') - 1)$.

By using Example 2.2.9-(2), we obtain the following example which shows that the bound given in Theorem 2.2.5 is sharp.

Example 2.2.10. Let $F'/K(t)$ be the Galois extension given in Example 2.2.9-(2). Recall that $p \neq 2$. We consider the Kummer extension $K(w)/K(t)$ given by $w^2 = t-1$. Since $w^2 = \frac{(x^4-1)^2}{2x^4}$, we have $w \in F'$ and $F'/K(w)$ is of degree 2^{4m+3}. By Proposition 1.2.14, we conclude that $(t = 1)$ and $(t = \infty)$ are the only ramified places of $K(t)$ in $K(w)/K(t)$. Let P_1, P_2 be places of $K(w)$ lying over $(t = -1)$ and P_3, P_4 be places lying over $(t = 1)$ and $(t = \infty)$, respectively. By Abhyankar's Lemma (see [36, Theorem 3.9.1]), we conclude that the places P_i are the only ramified places of $K(w)$ in $F'/K(w)$ and the ramification indices are given by

$$e(P_1) = e(P_2) = e(P_3) = 2 \quad \text{and} \quad e(P_4) = 4.$$

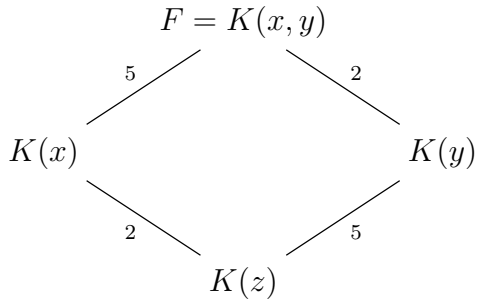
Hence, F' is a function field of genus $g(F') = 2^{4m} + 1$ of type $(2, 2, 2, 4)$ satisfying $N = 8(g(F') - 1)$.

The following two examples show that both cases, where the bound in Theorem 2.2.7 can be attained, appear.

Example 2.2.11. (1) Let $p = 5$. Consider the function field F with defining equation

$$y^5 - y = x^2.$$

Set $z := x^2$. Then we have the following picture:



We consider F as a Kummer extension over $K(y)$. The ramified places in $F/K(y)$ are the pole $(y = \infty)$ of y and the places $y = \alpha$ with $\alpha^5 - \alpha = 0$. Then by Hurwitz's genus formula we obtain

$$2g - 2 = 2\bigg(-2 + (5+1) \cdot \frac{1}{2}\bigg) = 2,$$

hence, $g = 2$. Note that the only ramified places of $K(z)$ in F are $(z = 0)$ and $(z = \infty)$ and F is of type $(2, 10)$. Moreover, the automorphism group G of $F/K(z)$ is generated by automorphisms

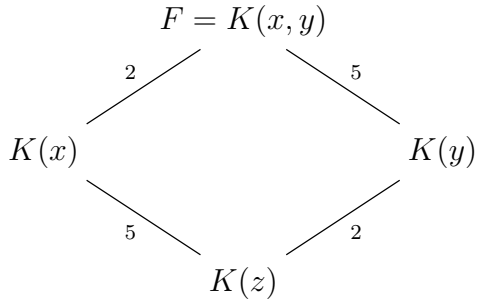
$$\sigma : \begin{cases} x \mapsto \zeta x \\ y \mapsto y + \alpha \end{cases}$$

where ζ is a primitive 2-root of unity and α is a root of $y^5 - y = 0$ and $G \simeq C_5 \times C_2 \simeq C_{10}$. Then $N = |G| = 10 = 10(g - 1)$.

(2) Let $p = 2$. Consider the function field F with defining equation

$$y^2 - y = x^5.$$

Set $z := x^5$. Then we have the following picture:



We consider F as a Kummer extension over $K(y)$. The ramified places in $F/K(y)$ are the pole $(y = \infty)$ of y and the places $(y = 0)$ and $(y = 1)$. Then by Hurwitz's genus formula we obtain

$$2g - 2 = 5\bigg(-2 + 3 \cdot \frac{4}{4}\bigg) = 2,$$

hence, $g = 2$. Note that the only ramified places of $K(z)$ in F are $(z = 0)$ and $(z = \infty)$ and F is of type $(5, 10)$. Moreover, the automorphism group G of $F/K(z)$ is generated by automorphisms

$$\sigma : \begin{cases} x \mapsto \zeta x \\ y \mapsto y + \alpha \end{cases}$$

where ζ is a primitive 5-root of unity and α is a root of $y^2 - y = 0$ and $G \simeq C_5 \times C_2 \simeq C_{10}$. Then $N = |G| = 10 = 10(g - 1)$.

The following example shows that the bound in Theorem 2.2.8 holds, for further details see [35].

Example 2.2.12. Let $p \geq 5$ and $n, k \geq 1$ be integers. Consider the function field $F := K(x, y)$ defined by

$$y^{p^n} + y = x^{p^{nk}+1}.$$

F can be considered as a Kummer extension over $K(y)$, which is of degree $p^{nk} + 1$. The zero of $y - \alpha$, where $\alpha^{p^n} + \alpha = 0$, and the pole of y in $K(y)$ are the only places ramified in F and they are totally ramified by Proposition 1.2.14. Hence, by Hurwitz's genus formula the genus of F is $g(F) = \dfrac{p^{nk}(p^n - 1)}{2}$.

Let $G = (\mathrm{Aut}(F/K))_{P_\infty}$ and $\sigma \in G$. Then $\sigma(\mathscr{L}(kP_\infty)) = \mathscr{L}(kP_\infty)$. This implies that $\sigma \in G$ is given by

$$\begin{aligned} \sigma : \ & x \mapsto x + d \\ & y \mapsto y + Q(x) \end{aligned}$$

where $d \in K$ and $p^n \deg Q(x) \leq v_{P_\infty}(y) = p^{nk} + 1$. Note that

$$Q(x)^{p^n} + Q(x) = (x + d)^{p^{nk}+1} - x^{p^{nk}+1}.$$

Say $Q(x) = q_0 + q_1 x + \ldots + q_{p^{n(k-1)}} x^{p^{n(k-1)}}$. We can write

$$Q(x) + Q(x)^{p^n} = \sum_{\substack{i \not\equiv 0 \bmod p^n \\ i \leq p^{n(k-1)}}} q_i x^i + \sum_{j=0}^{p^{n(k-2)}} (q_{jp^n} + q_j^{p^n}) x^{jp^n} + \sum_{l=p^{n(k-2)}+1} q_l^{p^n} x^{lp^n}.$$

On the other hand,

$$\begin{aligned} (x + d)^{p^{nk}+1} - x^{p^{nk}+1} &= x^{p^{nk}+1} + dx^{p^{nk}} + d^{p^{nk}} x + d^{p^{nk}+1} - x^{p^{nk}+1} \\ &= dx^{p^{nk}} + d^{p^{nk}} x + d^{p^{nk}+1}. \end{aligned}$$

Therefore, $Q(x) + Q(x)^{p^n} = (x+d)^{p^{nk}+1} - x^{p^{nk}+1}$ if and only if we have the following equalities.

1) $q_0 + q_0^{p^n} = d^{p^{nk}+1}$,

2) $q_1 = d^{p^{nk}}$,

3) $q_{p^{n(k-1)}}^{p^n} = d$,

4) $q_i = 0$ for $i \neq 1$ and $i \not\equiv 0 \mod p^n$, $i \leq p^{n(k-2)}$.

5) $q_{jp^n} + q_j^{p^n}$ for all $j = 1, \ldots, p^{n(k-2)}$.

6) $q_l = q_l^{p^n}$ for all $l = p^{n(k-2)}, \ldots, p^{n(k-1)} - 1$

From 4) and 5) above, we get $q_{jp^n} = 0$ for $1 < j < p^{n(k-2)}$ and $j \not\equiv 0 \mod p^n$. Also, $q_\ell = 0$ for $p^{n(k-2)} < l < p^{n(k-1)}$. That is, $Q(x)$ is of the form

$$Q(x) = q_0 + q_1 x + q_{p^n} x^{p^n} + q_{p^{2n}} x^{p^{2n}} + \ldots + q_{p^{n(k-2)}} x^{p^{n(k-2)}} + q_{p^{n(k-1)}} x^{p^{n(k-1)}}$$

such that

$$\begin{aligned}
&q_0 + q_0^{p^n} = d^{p^{nk}+1} \\
&q_1 = d^{p^{nk}} \\
&q_{p^n(k-1)}^{p^n} = d \\
&q_{sp^n} = -q_s^{p^n} \text{for all } s = 1, \ldots, p^{n(k-2)}.
\end{aligned}$$

These imply that

$$\begin{aligned}
&q_{p^n} = -q_1^{p^n}, \\
&q_{p^{2n}} = -q_{p^n}^{p^n} = -(-q_1^{p^n})^{p^n} = q_1^{p^{2n}}, \\
&q_{p^{tn}} = (-1)^t q_1^{p^{tn}} \\
&q_{p^{n(k-1)}} = -(q_{p^{n(k-2)}})^{p^n} = -((-1)^{k-2} q_1^{p^{n(k-2)}})^{p^n} = (-1)^{k-1} q_1^{p^{n(k-1)}}.
\end{aligned}$$

That is, d uniquely determines the coefficients $q_1, q_{p^n} \ldots q_{p^{n(k-1)}}$. Moreover, we have

$$d = q_{p^n(k-1)}^{p^n} = ((-1)^{k-1} q_1^{p^{n(k-1)}})^{p^n} = (-1)^{k-1} q_1^{p^{nk}} = (-1)^{k-1} (d^{p^{nk}})^{p^{nk}} = (-1) d^{p^{2nk}}.$$

Therefore, $d^{p^{2nk}} = (-1)^{k-1} d$. There exists p^{2nk} distinct such d. For each d, there are p^n distinct q_0 such that $q_0 + q_0^{p^n} = d^{p^{nk}+1}$. Hence, there exist $p^{2nk} \cdot p^n = p^{n(2k+1)}$ such automorphisms. In other words, $|G| = p^{n(2k+1)}$.

Recall that $v_{P_\infty}(x) = -p^n$, and $v_{P_\infty}(y) = -(p^{nk}+1)$. By setting $t := \dfrac{x^{p^{n(k-1)}}}{y}$, we obtain

$$v_{P_\infty}(t) = -p^{n(k-1)}v_{P_\infty}(x) - v_{P_\infty}(y) = -p^{n(k-1)}p^n + p^{nk} + 1 = 1$$

That is, t is a prime element for P_∞. Moreover,

$$\begin{aligned}\sigma(t) - t &= \frac{\sigma(x)^{p^{n(k-1)}}}{\sigma(y)} - \frac{x^{p^{n(k-1)}}}{y} = \frac{(x+d)^{p^{n(k-1)}}}{y+Q(x)} - \frac{x^{p^{n(k-1)}}}{y} \\ &= \frac{y(x^{p^{n(k-1)}} + d^{p^{n(k-1)}}) - (y+Q(x))x^{p^{n(k-1)}}}{y(y+Q(x))} \\ &= \frac{d^{p^{n(k-1)}}y - x^{p^{n(k-1)}}Q(x)}{y(y+Q(x))}\end{aligned}$$

where $Q(x) = q_0 + q_1x + q_{p^n}x^{p^n} + q_{p^{2n}}x^{p^{2n}} + \ldots + q_{p^{n(k-2)}}x^{p^{n(k-2)}} + q_{p^{n(k-1)}}x^{p^{n(k-1)}}$.
If $d = 0$, then $q_i = 0$ for $i > 0$. Thus, $Q(x) = q_0$. Note that if $q_0 = 0$, then $\sigma = \mathrm{id}$, i.e., $\sigma \in G^{(i)}_{P_\infty}$ for all $i \geq 0$. Suppose that $q_0 \neq 0$. Then we have

$$\sigma(t) - t = \frac{x^{p^{n(k-1)}}q_0}{y(y+q_0)}.$$

Thus,

$$v_{P_\infty}(\sigma(t) - t) = p^{n(k-1)}(-p^n) + 2(p^{nk}+1) = p^{nk} + 2,$$

i.e., $\sigma \in G^{(i)}_{P_\infty}$ for $i = 1, \ldots, p^{nk}+1$. Note that there are p^n such automorphisms.
If $d \neq 0$, then $v_{P_\infty}(Q(x)) = v_{P_\infty}(x^{p^{n(k-1)}}) = -p^{nk}$. Thus,

$$v_{P_\infty}(\sigma(t) - t) = -2p^{nk} + 2(p^{nk}+1) = 2.$$

That is, $\sigma \in G^{(1)}_{P_\infty}$ and $\sigma \notin G^{(i)}_{P_\infty}$ for $i \geq 2$. Therefore, we obtain $|G^{(2)}_{P_\infty}| = p^n$.

We remark that

$$|G| = \frac{4|G^{(2)}_{P_\infty}|}{(|G^{(2)}_{P_\infty}| - 1)^2}g^2 \leq \frac{4p}{(p-1)^2}g^2.$$

Note that for $n = 1$ and $k \geq 1$ we have the bound stated in Theorem 2.2.8.

Remark 2.2.13. Note that the bound $N = 10(g-1)$ can only be attained when the function field is of type $(2, 10)$ and $(5, 10)$, in which case $N = 10$ or $g = 2$. In particular, it is impossible to obtain infinitely many genera for this case as in the other examples.

3

Maximal Function Fields

3.1 Background

Let $\mathbb{F}_q$ be the finite field with q elements. The number of rational places of a function field defined over a finite field $\mathbb{F}_q$ can be estimated as follows.

Theorem 3.1.1 (Hasse-Weil Theorem)**.** *Let F be a function field of genus g defined over $\mathbb{F}_q$ and $N(F)$ be the number of its rational places. Then $N(F)$ satisfies*

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

Definition 3.1.2. *A function field F of genus g defined over $\mathbb{F}_q$ is called maximal (resp. minimal) if $N(F)$ attains the upper (resp. lower) bound in the Hasse-Weil Theorem, i.e.,*

$$N(F) = q + 1 + 2g\sqrt{q}$$

(resp. $N(F) = q + 1 - 2g\sqrt{q}$).

Remark 3.1.3. If q is not a square and $F/\mathbb{F}_q$ is maximal or minimal, this implies that $g = 0$. Thus, we will always assume that q is a square, i.e., $q = \ell^2$ for a prime power ℓ.

For a function field $F/\mathbb{F}_q$, we can consider the constant field extension $F_n = F\mathbb{F}_{q^n}$ of $F/\mathbb{F}_q$ of degree n. If $F/\mathbb{F}_q$ is a maximal function field, then the number of rational places of $F_n/\mathbb{F}_{q^n}$ is also known. In particular, if $F/\mathbb{F}_q$ is a maximal function field and n is a positive integer then

$$N(F_n) = q^n + 1 + (-1)^{n-1} 2g\sqrt{q^n}. \tag{3.1}$$

This gives rise to the following result.

Theorem 3.1.4. *Let $F/\mathbb{F}_q$ be a maximal function field and n be a positive integer. If n is odd, then $F_n/\mathbb{F}_{q^n}$ is also maximal. If n is even, then $F/\mathbb{F}_{q^n}$ is minimal.*

The following theorem is one of the main tools for the classification of maximal function fields.

Theorem 3.1.5. *[25, Proposition 6] Let E, F be two function fields defined over $\mathbb{F}_q$. If F is maximal over $\mathbb{F}_q$ and E is a subfield of F then E is also maximal over $\mathbb{F}_q$.*

The following characterization result is one of the useful tools we have, which is due to Garcia and Tafazolian; see [37, Theorem 4.1] and [11, Theorem 5.2].

Theorem 3.1.6. *Let ℓ be a prime power and $q = \ell^2$. Let F be a maximal function field over $\mathbb{F}_q$. Suppose that there exists $H \leq \mathrm{Aut}(F/\mathbb{F}_q)$ such that H is abelian of order ℓ and F^H is rational. Then there exists a divisor m of $\ell+1$ such that F is $\mathbb{F}_q$-isomorphic to the function field defined by*

$$\mathcal{H}_m : x^\ell + x = y^m.$$

In particular, the Hermitian function field $\mathcal{H}_{\ell+1}$ is a Galois extension of F over $\mathbb{F}_q$.

The known results on maximal function fields over $\mathbb{F}_q$ of large genus might be collected as follows, see [7, 8, 21, 24, 32].

Lemma 3.1.7. *Let ℓ be a prime power and $q = \ell^2$. Let $F/\mathbb{F}_q$ be a maximal function field of genus g. Then we have the following.*

(1) $g = g_1 := \dfrac{\ell(\ell-1)}{2}$, *or* $g = g_2 := \left\lfloor \dfrac{(\ell-1)^2}{4} \right\rfloor$, *or* $g \leq g_3 := \left\lfloor \dfrac{q-\ell+4}{6} \right\rfloor$.

(2) $g = g_1$ *if and only if F is $\mathbb{F}_q$-isomorphic to $\mathcal{H}_{\ell+1}$.*

(3) If q is odd then $g = g_2$ if and only if F is $\mathbb{F}_q$-isomorphic to $\mathcal{H}_{(\ell+1)/2}$.
If q is even then $g = g_2$ if and only if F is $\mathbb{F}_q$-isomorphic to the function field defined by $y^{\ell+1} = x^{\ell/2} + \ldots + x$.
In particular, the Hermitian function field $\mathcal{H}_{\ell+1}$ is a Galois extension of F over $\mathbb{F}_q$.

3.1.1 Examples of Maximal Function Fields

In this section, we present the Garcia-Stichtenoth (GS), the Giulietti-Korchmáros (GK) and the Garcia-Güneri-Stichtenoth (GGS) function fields.

The first function field we mention is the Garcia-Stichtenoth function field. In [10], Garcia and Stichtenoth constructed the function field $\mathcal{C}_3$ over $\mathbb{F}_{27^2}$ defined by

$$\mathcal{C}_3 : y^7 = x^9 - x$$

and proved that $\mathcal{C}_3$ is maximal over $\mathbb{F}_{27^2}$. Moreover, they showed that the Hermitian function field $\mathcal{H}_{28}$ is not a Galois extension of C_3. This was the first example of a maximal function field, which is not Galois covered by the Hermitian function field.

Let ℓ be a prime power and $q = \ell^3$. Consider the function field $\mathcal{C}_\ell$ over $\mathbb{F}_{q^2}$ defined by

$$\mathcal{C}_\ell : \qquad y^{\ell^2-\ell+1} = x^{\ell^2} - x.$$

We collect the results from ([10],[19, Section 12.1], [13]) on the Garcia-Stichtenoth function field $\mathcal{C}_\ell$ below.

Proposition 3.1.8. *The function field $\mathcal{C}_\ell$ has the following properties:*

(1) $\mathcal{C}_\ell$ is maximal over $\mathbb{F}_{q^2}$ of genus $\frac{1}{2}(\ell^2-\ell)(\ell^2-1)$.

(2) $\mathcal{C}_2$ is Galois covered by the Hermitian function field $\mathcal{H}_9$.

(3) For $\ell \geq 3$, the function field $\mathcal{C}_\ell$ is not Galois covered by the Hermitian function field $\mathcal{H}_{\ell^3+1}$.

The Galois extension $\mathcal{X}_\ell$ of the Garcia-Stichtenoth function field $\mathcal{C}_\ell$ given by

$$\mathcal{X}_\ell : \begin{cases} z^{\ell^2-\ell+1} & = y^{\ell^2} - y \\ y^{\ell+1} & = x^\ell + x \end{cases}$$

is introduced by Giulietti and Korchmáros in [12]. They showed that $\mathcal{X}_\ell$ is also maximal over $\mathbb{F}_{\ell^6}$ and the Hermitian function field $\mathcal{H}_{\ell^3+1}$ is not a Galois extension of $\mathcal{X}_\ell$ for any $\ell > 2$. This function field is referred as GK function field.

Proposition 3.1.9. *The function field $\mathcal{X}_\ell$ has the following properties:*

(1) $\mathcal{X}_\ell$ is maximal over $\mathbb{F}_{\ell^6}$ of genus $g(\mathcal{X}_\ell) = \frac{(\ell^3+1)(\ell^2-2)}{2} + 1$.

(2) For $\ell > 2$, the function field $\mathcal{X}_\ell$ is not Galois covered by the Hermitian function field $\mathcal{H}_{\ell^3+1}$.

(3) The full automorphism group $\mathrm{Aut}(\mathcal{X}_\ell)$ has order $\ell^3(\ell^3+1)(\ell^2-1)(\ell^2-\ell+1)$ and is defined over $\mathbb{F}_{\ell^6}$.

(4) $\mathrm{Aut}(\mathcal{X}_\ell)$ has exactly 2 short orbits on $\mathcal{X}_\ell$. One is wild of size ℓ^3+1, consists of all $\mathbb{F}_{\ell^2}$-rational places of $\mathcal{X}_\ell$. The other is tame of size $\ell^3(\ell^3+1)(\ell^2-1)$, consisting of all $\mathbb{F}_{\ell^6}$-rational places of $\mathcal{X}_\ell$ which are not $\mathbb{F}_{\ell^2}$-rational.

(5) $\mathrm{Aut}(\mathcal{X}_\ell)$ has a normal subgroup of index $d = gcd(3, \ell+1)$ isomorphic to $\mathrm{SU}(3,\ell) \times C_{(\ell^2-\ell+1)/d}$, where $\mathrm{SU}(3,\ell)$ is the special unitary group which preserves the set $\mathcal{X}_\ell(\mathbb{F}_{\ell^2})$ of $\mathbb{F}_{\ell^2}$-rational places of $\mathcal{X}_\ell$ and $C_{(\ell^2-\ell+1)/d}$ is cyclic of order $(\ell^2-\ell+1)/d$. The subgroup isomorphic to $\mathrm{SU}(3,\ell)$ is normal in $\mathrm{Aut}(\mathcal{X}_\ell)$.

(6) The stabilizer $\mathrm{Aut}(\mathcal{X}_\ell)_{P_\infty}$ *of* P_∞*, which is the unique pole of* x, y, z*, has order* $\ell^3(\ell^2-1)(\ell^2-\ell+1)$ *and contains a subgroup* $(Q_{\ell^3} \rtimes C_{\ell^2-1}) \rtimes C_{(\ell^2-\ell+1)/d}$*, where* Q_{ℓ^3} *is a Sylow* p*-subgroup of* $\mathrm{Aut}(\mathcal{X}_\ell)$ *and* C_{ℓ^2-1} *is cyclic of order* ℓ^2-1*.*

The next example is called the Garcia-Güneri-Stichtenoth (GGS) function field which is a generalization of the Giulietti-Korchmáros function field. In [9], the authors showed that GGS function field $\mathcal{X}_{\ell^n}$ is $\mathbb{F}_{\ell^{2n}}$-maximal. The automorphism group of $\mathcal{X}_{\ell^n}$ was determined in [16] and [17].

Let $n \geq 5$ be an odd integer. The GGS function field $\mathcal{X}_{\ell^n}$ is defined by

$$\mathcal{X}_{\ell^n} : \begin{cases} z^{\frac{\ell^n+1}{\ell+1}} & = y^{\ell^2} - y \\ y^{\ell+1} & = x^\ell + x \end{cases}$$

Note that $\mathcal{X}_{\ell^n}$ coincides with $\mathcal{X}_\ell$ when $n = 3$.

Proposition 3.1.10. *The GGS function field* $\mathcal{X}_{\ell^n}$ *has the following properties:*

(1) $\mathcal{X}_{\ell^n}$ *is maximal over* $\mathbb{F}_{\ell^{2n}}$ *of genus* $g(\mathcal{X}_{\ell^n}) = (\ell-1)(\ell^{n+1}+\ell^n-\ell^2)/2$*.*

(2) For $\ell \geq 3$*, the function field* $\mathcal{X}_{\ell^n}$ *is not Galois covered by the Hermitian function field* $\mathcal{H}_{\ell^n}$*.*

(3) The full automorphism group $\mathrm{Aut}(\mathcal{X}_{\ell^n})$ *has order* $\ell^3(\ell-1)(\ell^n+1)$ *and is defined over* $\mathbb{F}_{\ell^{2n}}$*.*

(4) $\mathrm{Aut}(\mathcal{X}_{\ell^n})$ *has a unique fixed place.*

3.1.2 Preliminary Results

Let F be a function field of genus $g = g(F)$ defined over the finite field $\mathbb{F}_q$ of characteristic p. Let K be an algebraic closure of $\mathbb{F}_q$. In [26], Lehr and Matignon considered the function fields whose automorphism group G fixes a place of F with $|G| > \frac{4}{(p-1)^2}g^2$ and obtained a complete characterization of F. Their results provide a birational isomorphism for F and an Artin-Schreier function field $\mathcal{X}_f$ defined by $w^p - w = f(x)$, which is a priori defined just over K. They also showed that if $F/\mathbb{F}_q$ is maximal then the isomorphism between F and $\mathcal{X}_f$ in general does not preserve the maximality, but it preserves both $\mathrm{Aut}(F/K) = \mathrm{Aut}(F/\mathbb{F}_q)$ and g, see [15]. We will use these results to relate $\mathrm{Aut}(F/K)$ and $\mathrm{Aut}(\mathcal{X}_f/K)$ and to obtain an upper bound for the order of a p-subgroup of the automorphism group of a maximal function field over $\mathbb{F}_{p^4}$.

Using the same notation as in [26] we give the following definition and state their results, see [26, Proposition 8.5.] and [26, Proposition 8.6.].

Definition 3.1.11. *Let F/K be a function field of genus g. Let G be a p-subgroup of* $\mathrm{Aut}(F/K)$. *We say that (F, G) satisfies the condition (N) if*

$$g > 0 \qquad \text{and} \qquad |G| > \frac{2p}{p-1} g.$$

Proposition 3.1.12. *Assume (F, G) with $g \geq 2$ satisfies the condition (N). Then there is a totally ramified rational place, say $Q \in \mathbb{P}_F$. Moreover, F^G is rational and Q is the only ramified place in F/F^G. Let i_0 be the integer such that*

$$G_Q^{(2)} = G_Q^{(3)} = \ldots = G_Q^{(i_0)} \supsetneq G_Q^{(i_0+1)},$$

where $G_Q^{(j)}$ denotes the j-th ramification group. Then

(1) $G_Q^{(1)} \neq G_Q^{(2)}$ and the fixed field $F^{G_Q^{(2)}}$ of $G_Q^{(2)}$ is rational.

(2) If $H \lhd G$ with $g(F^H) > 0$, then G/H is a p-subgroup of $Aut(F^H/K)$ and

$$\frac{|G|}{g} \leq \frac{|G/H|}{g(F^H)}.$$

In particular, $(F^H, G/H)$ satisfies the condition (N). Moreover, if $M \leq |G|/g^2$ for some M one gets

$$|H| \leq \frac{(1/M)|G/H|}{g(F^H)^2}.$$

(3) If $H \lhd G$ and $G_Q^{(2)} \supsetneq H \supset G_Q^{(i_0+1)}$, then $g(F^H) = (|G_Q^{(2)}/H| - 1)(i_0 - 1)/2 > 0$ and $(F^H, G/H)$ satisfies the condition (N).

We continue with a structural result on the short orbits of the automorphism group of a function field F/K for which the classical Hurwitz bound $84(g-1)$ does not hold. This result is due to Stichtenoth [34] and Henn [18]. Recall that a short orbit of $G \leq \mathrm{Aut}(F/K)$ corresponds to a unique ramified place of F^G, see Lemma 1.2.11 and Remark 1.2.13.

Theorem 3.1.13. *[19, Thorem 11.56, Theorem 11.126] Let F be a function field over K of genus $g \geq 2$ and $G \leq \mathrm{Aut}(F/K)$ with $|G| > 84(g-1)$. Then the fixed field F^G is rational and G has at most three short orbits on F as follows:*

(1) exactly three short orbits, one wild and two tame such that each rational place in the tame short orbits has stabilizer in G of order 2;

(2) exactly two short orbits, both wild;

(3) only one short orbit which is wild;

(4) exactly two short orbits, one tame and one wild. In this case $|G| < 8g^3$ *with the following exceptions.*

- $p = 2$ *and* F *is isomorphic to the hyperelliptic function field given by the equation* $y^2 + y = x^{2^k+1}$ *of genus* 2^{k-1}.
- $p > 2$ *and* F *is isomorphic to the Roquette function field given by the equation* $y^2 = x^q - x$ *of genus* $(q-1)/2$.
- $p \geq 2$ *and* F *is isomorphic to the Hermitian function field given by the equation* $y^{q+1} = x^q + x$ *of genus* $(q^2-q)/2$.
- $p = 2$ *and* F *is isomorphic to the Suzuki function field given by the equation* $y^q + y = x^{q_0}(x^q + x)$ *of genus* $q_0(q-1)$, *where* $q_0 = 2^n$ *and* $q = 2^{2n+1}$ *for some positive integer* n.

The following lemma guarantees that a Sylow p-subgroup of a wild automorphism group of an $\mathbb{F}_q$-maximal function field F fixes exactly one rational place of F.

Lemma 3.1.14. *[15, Proposition 3.8 and Theorem 3.10] The automorphism group* $\mathrm{Aut}(F/\mathbb{F}_q)$ *of a maximal function field* $F/\mathbb{F}_q$ *of genus at least two fixes the set of rational places of* F. *Moreover, automorphisms of* $\mathbb{F}_q$*-maximal function fields are always defined over* $\mathbb{F}_q$.

As a consequence of this lemma we obtain the following corollary.

Corollary 3.1.15. *If* S *is a Sylow* p*-subgroup of* $\mathrm{Aut}(F/\mathbb{F}_q)$ *then* S *fixes exactly one rational place* Q *of* F *and acts semiregularly on the set of the remaining rational places of* F, *i.e., the identity automorphism is the only automorphism fixing the remaining rational places of* F. *In particular, if* $p \nmid g$ *then every* $\sigma \in S$ *has order at most equal to* $\sqrt{q}$.

3.2 Maximal function fields over $\mathbb{F}_{p^4}$

Let F be an $\mathbb{F}_{p^4}$-maximal function field of genus $g = g(F) \geq 2$. We denote by G its full automorphism group $\mathrm{Aut}(\mathcal{X}/\mathbb{F}_{p^4})$.

Proposition 3.2.1. *Let* $F/\mathbb{F}_{p^4}$ *be a maximal function field of genus* $g = g(F) \geq 2$. *If* p *divides* $|G|$, *then a Sylow* p*-subgroup of* G *is of order at most* p^3*; unless* F *is either the Hermitian function field* $\mathcal{H}_{p^2+1}$ *or Galois covered by* $\mathcal{H}_{p^2+1}$.

Proof. Suppose that F is not the Hermitian function field. Therefore, by Lemma 3.1.7 $g < \frac{p^2(p^2-1)}{2}$. Let S be a Sylow p-subgroup of G. Since $F/\mathbb{F}_{p^4}$ is maximal, S fixes exactly one rational place $Q \in \mathbb{P}_F$, [19, Lemma 11.129], and since it is defined over $\mathbb{F}_{p^4}$ from [15, Theorem 3.10], it acts semiregularly on the remaining $p^4 + 2gp^2$ rational

places of F. In particular, $|S|$ divides $p^4 + 2gp^2$. Note that if $|S| \geq p^4$ then p^2 divides $2g$. Also, as $p^4 + 2gp^2 < p^4 + p^2(p^2-1)p^2 = p^6$ we have that $|S| = p^k$ with $k = 1, \ldots, 5$.

Now suppose that $|S| \geq p^4$. Then $g(F^S) = 0$; otherwise from [19, Theorem 11.78] we have $|S| \leq g < \frac{p^2(p^2-1)}{2}$, i.e., $|S| < p^4$. Applying Hurwitz genus formula to F/F^S, we have

$$2g - 2 = |S|(2g(F^S) - 2) + |S| - 1 + \Delta_Q^{(1)} = \Delta_Q^{(2)} - 2,$$

where $\Delta_Q^{(j)} = \sum_{i \geq j}(|S_Q^{(i)}| - 1)$ represents the contribution of the higher ramification groups at Q for $j = 1, 2$. That is,

$$2g = \Delta_Q^{(2)}.$$

Thus, we have $p \leq |S_Q^{(2)}| < p^4$ since $2 \leq g < \dfrac{p^2(p^2-1)}{2}$. Moreover, $p-1$ divides $\Delta_Q^{(2)}$ implying that $2g$ is divisible by $p^2(p-1)$, say $2g = rp^2(p-1)$, where $1 \leq r < p+1$ is an integer. If $r = p$ then $g = p^3(p-1)/2 > g_3$, where g_3 is given in Lemma 3.1.7. This implies that the Hermitian function field $\mathcal{H}_{p^2+1}$ is a Galois extension of F. Therefore, we can assume that $2g = rp^2(p-1)$ for some $1 \leq r < p$. Then (F, S) satisfies the condition (N) as

$$|S| \geq p^4 > \frac{rp^3(p-1)}{p-1} = \frac{2pg}{p-1}.$$

Hence, from Proposition 3.1.12 (1), we also obtain that the fixed field $F^{S_Q^{(2)}}$ is rational.

- If $|S_Q^{(2)}| = p$, then there is a normal subgroup $H \lhd S$ of order p^2 containing $S_Q^{(2)}$. Therefore, the fixed field F^H of H is also rational. Then by Theorem 3.1.6, we conclude that the Hermitian function field $\mathcal{H}_{p^2+1}$ is a Galois extension of $F/\mathbb{F}_q$.

- If $|S_Q^{(2)}| = p^2$, by Theorem 3.1.6, the Hermitian function field $\mathcal{H}_{p^2+1}$ is a Galois extension of $F/\mathbb{F}_q$.

- If $|S_Q^{(2)}| = p^3$, then from [19, Theorem 11.75 (v)] the integers k such that $S_Q^{(k)} \neq S_Q^{(k+1)}$ are all congruent modulo p. Then we get

  $$S_Q^{(2)} = S_Q^{(3)} = \ldots = S_Q^{(k)} \neq S_Q^{(k+1)},$$

  where $k \equiv 1 \mod p$. Hence,

  $$rp^2(p-1) = 2g = \Delta_Q^{(2)} \geq p(p^3 - 1),$$

  which implies $r \geq p + 1$, a contradiction.

□

From now on, we suppose that G satisfies $|G| > 84(g-1)$. Using Theorem 3.1.13, we proceed with a case-by-case analysis on the structure of the short orbits of G according to the following cases.

(1) G has exactly two short orbits, which are both wild.

(2) G has only one short orbit, which is wild.

(3) G has exactly three short orbits, one wild and two tame such that each rational place in the tame short orbits has stabilizer in G of order 2.

(4) G has exactly two short orbits, one tame and one wild.

Remark 3.2.2. Note that Nakajima in [29] proved that if G is an abelian group then $|G| \leq 4g + 4$. Therefore, G cannot be abelian.

We start with the case $p = 2$. Then by Lemma 3.1.7, the third largest genus g_3 is 2. Therefore, if $g > 2$, the Hermitian function field $\mathcal{H}_5$ is Galois extension of F. If $g = 2$, from [6, Theorem 9] we conclude that F is birationally equivalent to the hyperelliptic function field defined by $x^2 + x = y^5$. Hence, the Hermitian function field $\mathcal{H}_5$ is again a Galois extension of F.

From now on, we assume that $p > 2$.

Theorem 3.2.3. *There exists no $\mathbb{F}_{p^4}$-maximal function field F such that $G = \mathrm{Aut}(F/\mathbb{F}_{p^4})$ admits exactly two short orbits, which are both wild.*

Proof. Suppose that G has two wild short orbits, say O_1 and O_2. Since G has a wild short orbit, its order is congruent to 0 modulo p. From Lemma 3.1.14, we know that the fixed rational places of the Sylow p-subgroups of G lie on the set of all rational places of $F(\mathbb{F}_{p^4})$, and hence O_1 and O_2 are contained in $F(\mathbb{F}_{p^4})$. Moreover, the size of each wild short orbit of G is congruent to 1 modulo p as a p-group fixing a rational place Q in O_i act semiregularly on $O_i \setminus \{Q\}$ for $i = 1, 2$.

The size of the set $F(\mathbb{F}_{p^4}) \setminus O_1$ is congruent to 0 modulo p. As also $O_2 \subsetneq F(\mathbb{F}_{p^4})$ has length congruent to 1 modulo p, and $|G|$ is congruent to 0 modulo p we have a contradiction. □

Theorem 3.2.4. *Let $F/\mathbb{F}_{p^4}$ be a maximal function field. Suppose that $G = \mathrm{Aut}(F/\mathbb{F}_{p^4})$ has only one short orbit, which is wild. Then the Hermitian function field $\mathcal{H}_{p^2+1}$ is a Galois extension of F.*

Proof. Let S be a Sylow p-subgroup of G and O be the short orbit of G. By Corollary 3.1.15, S fixes exactly one place $Q \in O$. We consider the stabilizer G_Q of Q in G. Note that the extension F^{G_Q} over F^G is unramified [36, Theorem 3.8.2], and therefore we obtain $\mathrm{Diff}(F/F^G) = \mathrm{Diff}(F/F^{G_Q})$ from the transitivity of the different divisor.

Now, let g' be the genus of the function field F^{G_Q}. Applying Hurwitz genus formula to F/F^G and F/F^{G_Q} we have

$$\begin{aligned} 2g-2 &= -2|G| + \deg(\mathrm{Diff}(F/F^G)) \\ &= |G_Q|(2g'-2) + \deg(\mathrm{Diff}(F/F^{G_Q})). \end{aligned}$$

Hence $-2|G| = |G_Q|(2g'-2)$, which is true only if $g' = 0$ and $G = G_Q$ as $-2|G| < 0$. This implies that $|O| = 1$, i.e., $O = \{Q\}$. Then $|G| = p^k h$, where $k \in \{1, 2, 3\}$, h is relatively prime to p and G is a semidirect product of its unique Sylow p-subgroup S of order p^k and a cyclic group H of order h. From the Hurwitz's genus formula applied to F/F^G, we have

$$2g-2 = -2p^k h + (p^k h - 1) + \Delta_Q^{(1)},$$

where $\Delta_Q^{(1)} = \sum_{i\geq 1}(|S_Q^{(i)}| - 1)$ represents the contribution of the higher ramification groups at Q. Applying now the Hurwitz genus formula to F/F^S, we obtain

$$\begin{aligned} 2g-2 &= p^k(2g(F^S)-2) + (p^k-1) + \Delta_Q^{(1)} \\ &= p^k(2g(F^S)-2) + (p^k-1) + 2g - 2 + 2p^k h - (p^k h - 1), \end{aligned} \tag{3.2}$$

and hence

$$2g(F^S) - 1 + h = 0.$$

If $h > 1$, then $2g(F^S) - 1 + h > 0$, a contradiction. Hence $h = 1$ and $g(F^S) = 0$.

Thus, $G = S$ is a p-group of order p^k where $k = 1, 2, 3$ from Proposition 3.2.1. Since the groups of order p and p^2 are abelian, by Remark 3.2.2 this cannot be the case. Hence, we should only consider $|S| = p^3$ and S is not abelian. Note that S satisfies the condition (N) by our assumption $p^3 > 84(g-1) > 2pg/(p-1)$. From Proposition 3.1.12, the second ramification $S_Q^{(2)}$ of G does not coincide with $S_Q^{(1)} = S$ and the fixed field $F^{S_Q^{(2)}}$ is rational. If $|S_Q^{(2)}| = p^2$, then the claim follows from Theorem 3.1.6. Hence, we can assume that $|S_Q^{(2)}| = p$. Since $S_Q^{(2)} \lhd S$, we can find a normal subgroup H of S containing $S_Q^{(2)}$ of order p^2. Then F^H is rational, and by Theorem 3.1.6, F is Galois covered by the Hermitian function field $\mathcal{H}_{p^2+1}$. □

Theorem 3.2.5. *There exists no $\mathbb{F}_{p^4}$-maximal function field F such that $G = \mathrm{Aut}(F/\mathbb{F}_{p^4})$ admits exactly one wild short orbit, and two tame short orbits whose stabilizers have order 2 with $p \geq 3$.*

Proof. Suppose that G has exactly one wild short orbit, say O, and two tame short orbits whose stabilizers have order 2. Since G has a wild short orbit, $|G|$ has order congruent to 0 modulo p and a Sylow p-subgroup S of G is nontrivial.

From Lemma 3.1.14, we know that the fixed rational places of the Sylow p-subgroups of G lie on the set $F(\mathbb{F}_{p^4})$ of rational places of $F/\mathbb{F}_{p^4}$, and hence O is contained in

$F(\mathbb{F}_{p^4})$. Moreover, $|O|$ is congruent to 1 modulo $|S|$ (and hence modulo p) as S fixes a unique rational place Q in O and acts semiregularly on $O \setminus \{Q\}$, i.e., $|O| = n|S| + 1$ for some $n \geq 0$.

From the Hurwitz's genus formula applied to F/F^G we have

$$\begin{aligned} 2g-2 &= -2|G| + |O|(|G_Q| - 1 + \Delta_Q^{(1)}) + |G|/2 + |G|/2 \\ &= -|G| + |O|(|G_Q| - 1 + \Delta_Q^{(1)}) = |O|(\Delta_Q^{(1)} - 1), \end{aligned}$$

where $\Delta_Q^{(1)} = \sum_{i \geq 1}(|G_Q^{(i)}| - 1)$ represents the contribution of the higher ramification groups at Q. Therefore, we obtain that $|O|$ divides $2g-2$ since $\Delta_Q^{(1)} - 1 \geq |S| - 1 \geq p-1$.

Suppose that S is the Sylow p-subgroup of G_Q. From the Hurwitz genus formula applied to F/F^S, we obtain

$$\begin{aligned} 2g-2 &= |S|(2g(F^S) - 2) + |S| - 1 + \Delta_Q^{(1)} \\ &= |S|(2g(F^S) - 2) + |S| - 1 + \left(\frac{2g-2}{|O|} + 1\right). \end{aligned}$$

Hence,

$$g(F^S) = \frac{(2g-2)(|O|-1) + |S||O|}{2|S||O|}. \tag{3.3}$$

Since $g(F^S)$ is a nonnegative integer, we get that $|O| > 1$ and $g(F^S) > 0$. Moreover, $|O|$ is even as p is odd, and hence $|S|$ is odd.

Call the ramified places of F^G in F corresponding to the tame short orbits as T_1, T_2. Note that the ramification indices $e(T_1) = e(T_2) = 2$ in this case, [36, Proposition 3.8.5]. Now, we consider the stabilizer G_Q of Q in G. There are three cases:

I. T_1 and T_2 are both unramified in F^{G_Q}/F^G.
This case is impossible; otherwise we would have $\mathrm{Diff}(F/F^G) = \mathrm{Diff}(F/F^{G_Q})$, and as before, this is only possible if $g(F^{G_Q}) = 0$ and $|G| = |G_Q|$. This implies that $|O| = 1$, which is a contradiction.

II. Only one of T_1, T_2 is ramified in F^{G_Q}/F^G, say T_1.
Since T_1 is ramified in F^{G_Q}/F^G and $e(T_1) = 2$, all places in F^{G_Q} lying over T_1 are unramified in F/F^{G_Q}. Therefore, we have

$$\deg(\mathrm{Diff}(F/F^{G_Q})) + \frac{|G|}{2} = \deg(\mathrm{Diff}(F/F^G)).$$

Applying Hurwitz genus formula to F/F^G and F/F^{G_Q}, we have

$$\begin{aligned} 2g-2 &= -2|G| + \deg(\mathrm{Diff}(F/F^G)) \\ &= |G_Q|(2g(F^{G_Q})-2) + \deg(\mathrm{Diff}(F/F^{G_Q})). \end{aligned}$$

Hence, $\frac{-3|G|}{2} = |G_Q|(2g(F^{G_Q})-2)$, which is true only if $g(F^{G_Q}) = 0$ and $|O| = |G|/|G_Q| = 4/3$ as $\dfrac{-3|G|}{2} < 0$; therefore, this case also cannot occur.

III. T_1 and T_2 are both ramified in F^{G_Q}/F^G.
As in the second case, the places lying above T_1 and T_2 are unramified in F/F^{G_Q}. Thus,

$$\deg(\mathrm{Diff}(F/F^G)) = \deg(\mathrm{Diff}(F/F^{G_Q})) + |G|.$$

Then $-|G| = |G_Q|(2g(F^{G_Q})-2)$, which holds only if $g(F^{G_Q}) = 0$ and $|G| = 2|G_Q|$, i.e., $|O| = 2$, a contradiction.

Therefore, an $\mathbb{F}_{p^4}$-maximal function field whose full automorphism group admits exactly three short orbits, two tame and one wild, does not exist. □

We remark that the only remaining case is the one that G admits exactly one wild short orbit, say O_1, and one tame orbit, say O_2. Even though we could not the settle the case, we have some partial results on this case.

Note that $|G|$ has order congruent to 0 modulo p as G has a wild short orbit. In particular, a Sylow p-subgroup of G is nontrivial. As before, O_1 lies in the set $F(\mathbb{F}_{p^4})$ of rational places of F. Let $Q_1 \in O_1$ and $Q_2 \in O_2$. We denote by S the Sylow p-subgroup of the stabilizer G_{Q_1} of Q_1.

The following lemma will be our main tool.

Lemma 3.2.6. *The genus of the fixed field of S is given as follows:*

$$g(F^S) = \frac{(2g-2)(|O_1|-1) + |O_1||S| - |O_2|}{2|O_1||S|}. \tag{3.4}$$

Proof. From the Hurwitz's genus formula, we have the following equalities.

$$\begin{aligned} 2g-2 &= -2|G| + \frac{|G|}{|G_{Q_1}|}(|G_{Q_1}| - 1 + \Delta_{Q_1}^{(1)}) + \frac{|G|}{|G_{Q_2}|}(|G_{Q_2}|-1) \\ &= \frac{|G|}{|G_P|}(\Delta_{Q_1}^{(1)} - 1) - \frac{|G|}{|G_{Q_2}|} \qquad (3.5) \\ &= |O_1|(\Delta_{Q_1}^{(1)} - 1) - |O_2|, \qquad (3.6) \end{aligned}$$

where $\Delta_{Q_1}^{(1)} = \sum_{i\geq 1}(|G_{Q_1}^{(i)}| - 1)$ represents the contribution of the higher ramification groups at Q_1. Note that $G_{Q_1}^{(1)} = S$, and hence $\Delta_{Q_1}^{(1)} \geq |S| - 1$. Also, from the Hurwitz's

genus formula applied to F/F^S, we obtain

$$2g - 2 = |S|(2g(F^S) - 2) + |S| - 1 + \Delta_{Q_1}^{(1)}. \tag{3.7}$$

Multiplying both sides of Equation (3.7) by $|O_1|$ and replacing $|O_1|(\Delta_{Q_1}^{(1)} - 1)$ by $2g - 2 + |O_2|$, we get the desired result. □

Proposition 3.2.7. *Let $F(\mathbb{F}_{p^4}) = O_1 \cup O_2$. Then F is Galois covered by the Hermitian function field if*

(a) $g(F^S) = 0$,

(b) $g(F^S) > 0$ *and* $|S| \geq p^3$.

Proof. Note that if $|O_1| = 1$, since $g(F^S)$ is a nonnegative integer, we get $|O_2| = |S|$ and $g(F^S) = 0$. Therefore, we conclude that $|O_1| > 1$. Using Equation (3.6) and Equation (3.7), we get

$$|S|(2g(F^S) - 1) + p^2 = \frac{(|O_1| - (p^2 + 1))\Delta_{Q_1}^{(1)}}{p^2 + 1}. \tag{3.8}$$

(a) Suppose that $g(F^S) = 0$.

- If $|S| = p$, then from [19, Theorem 12.5] (recalling that every function field admits a plane model, possibly singular) we know that a plane model of our function field is given by separated polynomials. Note that applying [19, Theorem 12.11] we have that either the automorphism group of our function field fixes a place (we know that it is not our case since $|O_1| > 1$) or it is one of the following function fields:
  (i) $y^p + y = x^m$, where m divides $p + 1$ or
  (i) $y^p + y = x^{p+1}$.
  Since these function fields are both $\mathbb{F}_{p^2}$-maximal, they are $\mathbb{F}_{p^4}$-minimal, a contradiction.
- If $|S| = p^2$, then $\mathcal{H}_{p^2+1}$ is a Galois extension of $F/\mathbb{F}_{p^4}$ from Theorem 3.1.6.
- If $|S| = p^3$, then LHS of (3.8) is negative. Thus, $|O_1| < 1 + p^2$, which is impossible as $|O_1| \geq 1 + |S|$.

(b) Suppose that $g(F^S) > 0$ and $|S| \geq p^3$. By Proposition 3.2.1, we can without loss of generality consider the case that $|S| = p^3$. Then RHS of Equation (3.8) is divisible by $p - 1$ and as $(p^2 + 1, p - 1) = 2$ we get that $g(F^S) > (p - 1)/4$. Therefore, $g \geq p^3(p - 1)/4 > g_3$, which proves the claim.

□

Proposition 3.2.8. *Let $F(\mathbb{F}_{p^4}) = O_1$. Then F is Galois covered by the Hermitian function field if*

(a) $g(F^S) = 0$,

(b) $g(F^S) > 0$ *and* $|S| \geq p^2$.

Proof. By Equation (3.5), we have

$$|G| = \frac{2(g-1)|G_{Q_1}||G_{Q_2}|}{|G_{Q_2}|(\Delta_{Q_1}^{(1)} - 1) - |G_{Q_1}|}.$$

Since $|G_{Q_2}|(\Delta_{Q_1}^{(1)} - 1) - |G_{Q_1}| \geq 1$, we have

$$\frac{\Delta_{Q_1}^{(1)} - 1}{|G_{Q_1}| + 1} \geq \frac{1}{|G_{Q_2}|}.$$

This yields

$$\frac{2(g-1)}{|G|} = -\frac{1}{|G_{Q_2}|} + \frac{\Delta_{Q_1}^{(1)} - 1}{|G_{Q_1}|} \geq -\frac{\Delta_{Q_1}^{(1)} - 1}{|G_{Q_1}| + 1} + \frac{\Delta_{Q_1}^{(1)} - 1}{|G_{Q_1}|} = \frac{\Delta_{Q_1}^{(1)} - 1}{|G_{Q_1}|(|G_{Q_1}| + 1)},$$

and hence

$$\frac{1}{p^2|G_{Q_1}|} \geq \frac{2(g-1)}{2p^2 g|G_{Q_1}|} \geq \frac{2(g-1)}{|G|} \geq \frac{\Delta_{Q_1}^{(1)} - 1}{|G_{Q_1}|(|G_{Q_1}| + 1)}. \tag{3.9}$$

From Equation (3.9), we get $1 + |G_{Q_1}| \geq p^2(\Delta_{Q_1}^{(1)} - 1)$ and $|G_{Q_2}| \geq p^2$. Hence,

$$|O_2| = \frac{|G|}{|G_{Q_2}|} \leq \frac{|G|}{p^2}.$$

(a) Suppose that $g(F^S) = 0$. Using Equation (3.4), we have

$$\begin{aligned}
|G| \geq p^2|O_2| &= p^2((2g-2)(|O_1| - 1) + |O_1||S|) \\
&= p^2(2g(|O_1| - 1) + |O_1|(|S| - 2) + 2) \\
&= 2gp^2(|O_1| - 1) + p^2|O_1|(|S| - 2) + 2p^2 \\
&\geq (2g)(2g)(2g) + p^2(2p^2 g + p^4)(p-2) + 2p^2 \\
&> 8g^3.
\end{aligned}$$

Using Henn's classification [19, Theorem 11.126], we conclude that F is Galois covered by the Hermitian function field.

(b) Suppose that $g(F^S) > 0$ and $|S| \geq p^2$. Let $|G_{Q_1}| = h|S|$, where h is relatively prime to p. By [19, Theorem 11.60], we have $h \leq 4g(F^S) + 2$, as h is the order of a

cyclic group $H \simeq G_{Q_1}/S$ of order relatively prime to p. From Equation (3.9) and using $h \leq 4g(F^S) + 2$, we get

$$(4g(F^S) + 2)|S| + 1 \geq |G_{Q_1}| + 1 \geq p^2(\Delta_{Q_1}^{(1)} - 1),$$

and hence

$$g(F^S) \geq \frac{p^2(\Delta_{Q_1}^{(1)} - 1) - 2|S| - 1}{4|S|} \geq \frac{p^2(|S| - 2) - 2|S| - 1}{4|S|} = \frac{|S|(p^2 - 2) - 2p^2 - 1}{4|S|},$$

while $g \geq \dfrac{|S|(p^2 - 2) - 2p^2 - 1}{4}$.

- If $|S| \geq p^2 \geq 11$, then we get $g > g_3 = \lfloor \frac{p^4 - p^2 + 4}{6} \rfloor$. Hence, F is Galois covered by $\mathcal{H}_{p^2+1}$.
- If $|S| \geq p^2 = 9$, then $g \geq (p^4 - 4p^2 - 1)/4 = 11$. This implies that $g = 11$ or $g = 12$ or that F is Galois covered by the Hermitian function field (indeed the first, the second and the third largest genera in this case are 36, 16 and 12, respectively). Using $|O_1| = |F(\mathbb{F}_{p^4})|$, we have

  $$|O_1| = \begin{cases} 280, & \text{if } g = 11, \\ 298, & \text{if } g = 12. \end{cases}$$

  In particular, $9|O_1|$ divides the order of G.

  Using Equation (3.4), the genus $g(F^S)$ is given by

  $$g(F^S) = \begin{cases} \dfrac{20 \cdot 279 + 280 \cdot |S| - |O_2|}{2 \cdot 280 \cdot |S|}, & \text{if } g = 11, \\ \dfrac{22 \cdot 297 + 298 \cdot |S| - |O_2|}{2 \cdot 298 \cdot |S|}, & \text{if } g = 12. \end{cases}$$

  Note that $|S|$ divides $|O_2|$ since O_2 is a tame short orbit. Hence, $|S|$ divides 279, if $g = 11$ and $|S|$ divides 297, if $g = 12$. Also, $|O_2|$ is even as $g(F^S)$ is an integer.

  We analyze further the cases $g = 11$ and $g = 12$ separately.

  (i) Suppose that $g = 11$. Therefore, $|S| = 9$ as $27 \nmid 279$. Since 9 divides $|O_2|$ and $|O_2|$ is even; hence, $|O_2|$ is at least 18. Using this fact we obtain that

  $$g(F^S) = \frac{20 \cdot 279 + 280 \cdot |S| - |O_2|}{2 \cdot 280 \cdot |S|} \leq 1.$$

  Therefore, $g(F^S) = 1$ and $|O_2| = 3060$. Since both $|O_2|$ and $9|O_1|$ divide $|G|$, we have that $\text{lcm}(3060, 9|O_1|) = 42840$ divides $|G|$, where lcm denotes

the least common multiple. In particular, $|G| \gg 8g^3$. Therefore, we get the claim.

(ii) Suppose that $g = 12$. If $|S| = 27$, then $g(F^S) = \dfrac{14580 - |O_2|}{16092} = 0$. Thus, we have $|S| = 9$, and hence

$$g(F^S) = \frac{9216 - |O_2|}{5364} \leq 1.$$

Therefore, $g(F^S) = 1$ and $|O_2| = 3852$. As before, since $\mathrm{lcm}(9 \cdot 298, 3852) \gg 8g^3$, we get the claim.

□

We remark that the question of whether all $\mathbb{F}_{p^4}$-maximal function fields are Galois covered by the Hermitian function field remains open for the following cases: The automorphism group G admits exactly one tame short orbit and one wild short orbit such that

- $F(\mathbb{F}_{p^4}) = O_1 \cup O_2$, $g(F^S) > 0$ and $|S| \leq p^2$,
- $F(\mathbb{F}_{p^4}) = O_1$, $g(F^S) > 0$ and $|S| = p$,
- $F(\mathbb{F}_{p^4})$ contains O_1 and a long orbit G.

A through investigation on these cases might result in new values of the genus spectrum of $\mathbb{F}_{p^4}$-maximal function fields.

Remark 3.2.9. Let F be a $\mathbb{F}_{p^2}$-maximal function field of genus $g := g(F) \geq 2$ and let $G = \mathrm{Aut}(F)$ with $|G| > 84(g-1)$. Suppose that p divides $|G|$. Then similarly as in Proposition 3.2.1, we see that a Sylow subgroup of G, is of order at most p; unless F is either the Hermitian function field $\mathcal{H}_{p+1}$ or a Galois subcover of $\mathcal{H}_{p+1}$. Hence, it remains to consider the case that a Sylow p-subgroup S of G is of order p. By Corollary 3.1.15, S fixes exactly one rational place Q of F and S acts semiregularly on the remaining set $F(\mathbb{F}_{p^2}) \setminus \{Q\}$ of rational places of F. As in $\mathbb{F}_{p^4}$-maximal function fields, we continue with a case-by-case analysis on the short orbits structure of G.

(1) Suppose that G has exactly two short orbits O_1, O_2, which are both wild. This case cannot occur as in Lemma 3.2.3.

(2) Suppose that G has only one short orbit O, which is wild. Following the same steps in Lemma 3.2.4, we get $|O| = 1$. Therefore, $G = S$. However a group of order p is abelian, by Remark 3.2.2 it satisfies the Hurwitz's bound. Hence, this case also cannot occur.

Therefore, differently from [2], we say more on the orbit structure of the automorphism group of $F/\mathbb{F}_{p^2}$.

(3) Suppose that G has exactly three short orbits, one wild O_1 and two tame O_2, O_3. We follow the same argument in Lemma 3.2.5 to get $|O_1| > 1$ and $g(F^S) > 0$. Moreover, $|O_1|$ is even. We analyze the ramification in F^{G_Q} over F^G as in Lemma 3.2.5, and see that this case cannot occur.

Bibliography

[1] N. Anbar, H. Stichtenoth, and S. Tutdere, *Asymptotically good towers with small p-rank and many automorphisms*, preprint.

[2] D. Bartoli, M. Montanucci, and F. Torres, $\mathbb{F}_{p^2}$*-maximal curves with many automorphisms are Galois-covered by the Hermitian curve*, preprint.

[3] D. Bartoli, M. Montanucci, and G. Zini, *AG codes and AG quantum codes from the GGS curve*, Designs, Codes and Cryptography **86** (2018), no. 10, 2315–2344.

[4] P. Beelen and M. Montanucci, *A new family of maximal curves*, J. Lond. Math. Soc. (2) **98** (2018), no. 3, 573–592.

[5] D. S. Dummit and R. M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[6] S. Fanali and M. Giulietti, *On maximal curves with Frobenius dimension 3*, Designs, Codes and Cryptography **53** (2009), no. 3, 165–174.

[7] R. Fuhrmann, A. Garcia, and F. Torres, *On maximal curves*, J. Number Theory **67** (1997), no. 1, 29–51.

[8] R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), no. 1, 103–106.

[9] A. Garcia, C. Güneri, and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom. **10** (2010), no. 3, 427–434.

[10] A. Garcia and H. Stichtenoth, *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bull. Braz. Math. Soc. (N.S.) **37** (2006), no. 1, 139–152.

[11] A. Garcia and S. Tafazolian, *Certain maximal curves and Cartier operators*, Acta Arith. **135** (2008), no. 3, 199–218.

[12] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), no. 1, 229–245.

[13] M. Giulietti, M. Montanucci, and G. Zini, *On maximal curves that are not quotients of the Hermitian curve*, Finite Fields Appl. **41** (2016), 72–88.

[14] M. Giulietti, L. Quoos, and G. Zini, *Maximal curves from subcovers of the GK-curve*, J. Pure Appl. Algebra **220** (2016), no. 10, 3372–3383.

[15] B. Gunby, A. Smith, and A. Yuan, *Irreducible canonical representations in positive characteristic*, Res. Number Theory **1** (2015), Art. 3, 25.

[16] C. Güneri, M. Özdemir, and H. Stichtenoth, *The automorphism group of the generalized Giulietti-Korchmáros function field*, Adv. Geom. **13** (2013), no. 2, 369–380.

[17] R. Guralnick, B. Malmskog, and R. Pries, *The automorphism groups of a family of maximal curves*, J. Algebra **361** (2012), 92–106.

[18] H.-W. Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115.

[19] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.

[20] A. Hurwitz, *Über algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1893), 403–442 (ger).

[21] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 721–724 (1982).

[22] G. Korchmáros and M. Montanucci, *Large odd prime power order automorphism groups of algebraic curves in any characteristic*, preprint.

[23] G. Korchmáros and M. Montanucci, *Ordinary algebraic curves with many automorphisms in positive characteristic*, Algebra Number Theory **13** (2019), no. 1, 1–18.

[24] G. Korchmáros and F. Torres, *On the genus of a maximal curve*, Math. Ann. **323** (2002), no. 3, 589–608.

[25] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 16, 729–732.

[26] C. Lehr and M. Matignon, *Automorphism groups for p-cyclic covers of the affine line*, Compos. Math. **141** (2005), no. 5, 1213–1237.

[27] L. Ma and C. Xing, *The asymptotic behavior of automorphism groups of function fields over finite fields*, Trans. Amer. Math. Soc. **372** (2019), no. 1, 35–52.

[28] A. M. Macbeath, *On a theorem of Hurwitz*, Proc. Glasgow Math. Assoc. **5** (1961), 90–96.

[29] S. Nakajima, *On abelian automorphism groups of algebraic curves*, J. Lond. Math. Soc. **s2-36** (1987), no. 1, 23–32.

[30] R. Pries and K. Stevenson, *A survey of Galois theory of curves in characteristic p*, WIN—women in numbers, Fields Inst. Commun., vol. 60, Amer. Math. Soc., Providence, RI, 2011, pp. 169–191.

[31] P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, Math. Z. **117** (1970), no. 1, 157–163.

[32] H. G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.

[33] H. L. Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik.*, J. Reine Angew. Math. **179** (1938), 5–15.

[34] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. (Basel) **24** (1973), 527–544.

[35] ———, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern*, Arch. Math. (Basel) **24** (1973), 615–631.

[36] ———, *Algebraic function fields and codes*, second ed., GTM, vol. 254, Springer-Verlag, Berlin, 2009.

[37] S. Tafazolian and F. Torres, *A note on certain maximal curves*, Comm. Algebra **45** (2017), no. 2, 764–773.

[38] R. Zomorrodian, *Nilpotent automorphism groups of Riemann surfaces*, Trans. Amer. Math. Soc. **288** (1985), no. 1, 241–255.