ON ALGEBRAIC CURVES IN PRIME CHARACTERISTIC

APPROVED BY

Prof. Dr. Henning Stichtenoth ....
(Thesis Supervisor)

Assist. Prof. Massimo Giulietti ....

Assoc. Prof. Cem Güneri ....

Assoc. Prof. Erkay Savaş ....

Prof. Dr. Alev Topuzoğlu ....

DATE OF APPROVAL: 31.05.2012

ON ALGEBRAIC CURVES IN PRIME CHARACTERISTIC

by
NURDAGÜL ANBAR

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
Spring 2012

ON ALGEBRAIC CURVES IN PRIME CHARACTERISTIC

APPROVED BY

Prof. Dr. Henning Stichtenoth ....
(Thesis Supervisor)

Assist. Prof. Massimo Giulietti ....

Assoc. Prof. Cem Güneri ....

Assoc. Prof. Erkay Savaş ....

Prof. Dr. Alev Topuzoğlu ....

DATE OF APPROVAL: 31.05.2012

ON ALGEBRAIC CURVES IN PRIME CHARACTERISTIC

Nurdagül Anbar

Mathematics, PhD Thesis, 2012

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: Artin-Schreier extension, automorphism, curve, degree r point, function field, Hurwitz genus formula, order sequence.

Abstract

In this thesis we consider two problems related to algebraic curves in prime characteristic.

In the first part, we study curves defined over the finite field $\mathbb{F}_q$. We prove that for each sufficiently large integer g there exists a curve of genus g with prescribed number of degree r points for $r = 1, \dots, m$. This leads to the existence of a curve whose L-polynomial has prescribed coefficients up to some degree.

In the second part, we consider curves defined over algebraically closed fields $\mathbb{K}$ of odd characteristic. We show that a plane smooth curve which has a $\mathbb{K}$-automorphism group of order larger than $3(2g^2 + g)(\sqrt{8g+1} + 3)$ must be birationally equivalent to a Hermitian curve.

ASAL KARAKTERİSTİKTEKİ CEBİRSEL EĞRİLER

Nurdagül Anbar

Matematik, Doktora Tezi, 2012

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: Artin-Schreier genişlemesi, otomorfizma, eğri, derecesi r olan nokta, fonksiyonel cisimler, Hurwitz cins formülü, derece dizisi.

Özet

Bu tezde asal karakteristikte tanımlanmış cebirsel eğriler konusundaki iki problemi ele aldık.

İlk bölümde sonlu bir cisim olan $\mathbb{F}_q$ üzerinde tanımlı eğrileri çalıştık. Yeteri kadar büyük her tamsayı g için öngörülmüş sayıda r dereceli $(r = 1, \ldots, m)$ noktası olan cinsi g bir eğrinin varlığını gösterdik. Bu sonuç, belli bir dereceye kadar öngörülmüş katsayılı L-polinomu olan bir eğrinin varlığnı göstermiştir.

İkinci bölümde tek karakteristikli, cebirsel olarak kapalı $\mathbb{K}$ cismi üzerinde tanımlı eğrileri göz önüne alık. Otomorfizma grubunun sayısı $3(2g^2 + g)(\sqrt{8g+1} + 3)$'den büyük olan düzlemsel düzgün bir eğrinin Hermitian eğrisine birasyonel olarak eşdeğer olduğunu gösterdik.

To my twin Sultan

Acknowledgments

First and foremost, I would like to thank my advisor Prof. Dr. Henning Stichtenoth for his motivation, guidance and encouragement throughout my graduate study. His contributions to my academic experience and my personality have been enormous. I also would like to thank Dr. Massimo Gulietti who has treated me not only as a student but also as a colleague. I will always be grateful for his guidance and his hospitality during my stay in Italy.

I would like to thank all my professors for the knowledge they provided me during my studies, especially Alev Topuzoğlu-who always care for us like a mother-, Cem Güneri, Ali Ulaş Özgür Kişisel, Ayşe Berkman and Feza Arslan.

I am deeply grateful to Sultan Anbar for being the best friend of mine throughout my life, and my family for their endless love and care. I am thankful to Wilfried Meidl for his friendship, care and patience. I was fortunate to meet him.

I also would like to thank all my friends, especially Leyla Işık, Buket Özkaya, Alp Bassa, Matteo Paganin, Seher Tutdere and Kağan Kurşungöz for the greatest party I have ever seen in my life and I will never forget.

Last, but not least, I would like to thank all my friends for all the useful discussions we made and joyful moments we shared.

This work is supported by TÜBİTAK.

Table of Contents

CHAPTER 1

Introduction

In this thesis we consider two problems related to algebraic curves defined over a field $\mathbb{K}$ of positive characteristic. Throughout this thesis by a curve $\mathcal{X}$ we mean a smooth, projective and absolutely irreducible curve defined over $\mathbb{K}$.

Let $\mathbb{K} = \mathbb{F}_q$ be the finite field with q elements. For a curve $\mathcal{X}$ defined over $\mathbb{F}_q$ we denote by $N(\mathcal{X})$ and $g(\mathcal{X})$ the number of rational points and the genus of $\mathcal{X}$, respectively. Of particular interest is then the question for which non-negative integers g, N and a power of a prime number q does there exist a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus $g(\mathcal{X}) = g$ with exactly N rational points. This question represents an attractive mathematical challenge studied extensively (see [18]). A necessary condition for the existence of such a curve is given by the Hasse-Weil bound which states that

$$\mid N - (q+1) \mid \leq 2g\sqrt{q} \ . \tag{1.1}$$

This bound is improved by the Serre bound for non-square q, namely

$$\mid N - (q+1) \mid \leq g[2\sqrt{q}\,] \ , \tag{1.2}$$

where $[n]$ is the integer part of the real number n.

A common approach to the problem is to investigate the set $\mathcal{N}(q,g)$ defined by

$$\mathcal{N}(q,g) := \{N \ \mid \ \text{there exists a curve over } \mathbb{F}_q \text{ of genus } g \text{ having } N \text{ rational points}\}$$

for a fixed integers q and g. As a consequence of (1.2) the set $\mathcal{N}(q,g)$ lies in the finite interval

$$\mathcal{N}(q,g) \subseteq [\, q+1-g[2\sqrt{q}\,], q+1+g[2\sqrt{q}\,]\,] \ ;$$

however it is not known exactly for which integers $N \in [\, q+1-g[2\sqrt{q}\,], q+1+g[2\sqrt{q}\,]\,]$ there exists a curve over $\mathbb{F}_q$ of genus g with exactly N rational points.

In chapter two we approach the problem differently. Instead of fixing the parameters q and g, we fix the parameters q and N. In other words, we deal with the question for which integer values of g there exists a curve over $\mathbb{F}_q$ of genus g with exactly N rational points, and we investigate the set $\mathfrak{G}(q,N)$ defined by

$$\mathfrak{G}(q,N) := \{g \mid \text{there exists a curve over } \mathbb{F}_q \text{ of genus } g \text{ having exactly } N \text{ rational points}\} \ .$$

Again a necessary condition for a non-negative integer g to be in $\mathfrak{G}(q, N)$ comes from the Serre bound; i.e.,

$$g \geq \frac{\mid N - (q+1) \mid}{[2\sqrt{q}\,]} \ .$$

However, (1.2) is not sufficient; for example $2 \notin \mathfrak{G}(2, 7)$ (see Theorem 2.1.1).

A sufficient condition is given by Stichtenoth [39] stated as follows:

Theorem 1.0.1 *For any non-negative integer N, there is a constant g_0 such that for all integers $g \geq g_0$, there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus $g(\mathcal{X}) = g$ having exactly N rational points.*

Hence

$$[g_0, \infty) \subseteq \mathfrak{G}(q, N) \subseteq \left[\frac{\mid N - (q+1) \mid}{[2\sqrt{q}\,]}, \infty\right) ,$$

which implies that the set $\mathbb{N} \setminus \mathfrak{G}(q, N)$ is finite for all q and N.

In [39] it is noted that the constant g_0 depends on the parameters q and N. Here our aim is to estimate how small g_0 can be and to show that it is possible to give g_0 as an explicit function of q and N. More precisely, we show that for given q there are constants $f(q)$ and $h(q)$ (depending only on q) such that for any non-negative integers g and N with $g \geq f(q)N + h(q)$, there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus $g(\mathcal{X}) = g$ having exactly N rational points. In other words, for given q there exist constants $\alpha(q)$ and $\beta(q)$ such that the interval $[0, \alpha(q)g - \beta(q)] \subseteq \mathcal{N}(q, g)$.

In chapter three we give a proof of a generalization of Theorem 1.0.1. We show that for any given non-negative integers $b_1, \ldots, b_m$ there is an integer $g_0 \geq 0$ such that for all integers $g \geq g_0$, there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus $g(\mathcal{X}) = g$ having exactly b_r points of degree r, for $r = 1, \ldots, m$. As a consequence of this result, we see the existence of a curve defined over $\mathbb{F}_q$ of sufficiently large genus g whose L-polynomial has prescribed coefficients up to some degree.

In chapter four we assume that $\mathbb{K}$ is an algebraically closed field of odd characteristic p. Let $\mathrm{Aut}(\mathcal{X})$ be the $\mathbb{K}$-automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$. It is well known that $\mathrm{Aut}(\mathcal{X})$ is finite and that the classical Hurwitz bound holds if $p \nmid |\mathrm{Aut}(\mathcal{X})|$; i.e.,

$$|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1) \ .$$

If p divides $|\mathrm{Aut}(\mathcal{X})|$, then the curve $\mathcal{X}$ may have a much larger $\mathbb{K}$-automorphism group when compared to its genus. This was first pointed out by Roquette [29]. Later on, Stichtenoth [36, 37] proved that if

$$|\mathrm{Aut}(\mathcal{X})| \geq 16g^4 \ ,$$

then $\mathcal{X}$ is birational equivalent to a Hermitian curve $\mathcal{H}(n)$, that is, to a non-singular plane curve with affine equation $Y^n + Y - X^{n+1} = 0$, for some $n = p^h \geq 3$. Here,

$g = (n^2 - n)/2$, $\mathrm{Aut}(\mathcal{H}(n)) \cong \mathrm{PGU}_3(n)$, and $|\mathrm{Aut}(\mathcal{H}(n))| = n^3(n^3+1)(n^2-1)$. The curves $\mathcal{X}$ with $|\mathrm{Aut}(\mathcal{X})| \geq 8g^3$ were classified by Henn [15] and as a corollary of Henn's classification one gets: if

$$|\mathrm{Aut}(\mathcal{X})| > 16g^3 + 24g^2 + g \ , \tag{1.3}$$

then $\mathcal{X}$ is birational equivalent to a Hermitian curve. Here the aim is to improve the bound (1.3) in the case that $\mathcal{X}$ is a non-singular plane curve. More precisely we show that if $\mathcal{X}$ has a $\mathbb{K}$-automorphism group of order larger than $3(2g^2+g)(\sqrt{8g+1}+3)$, then $\mathcal{X}$ is birationally equivalent to the Hermitian curve $\mathcal{H}(n)$ for some $n = p^h$.

In the appendix we recall some facts and definitions we used throughout this thesis.

CHAPTER 2

Function Fields with Prescribed Number of Rational Places

As the theory of algebraic curves is essentially the same as the theory of function fields of one variable, we use the language of functions fields. For detailed information see [38]. First we fix some notations.

Let $F/\mathbb{F}_q$ be a function field with full constant field $\mathbb{F}_q$. Denote by

$p = \text{char } \mathbb{F}_q$, the characteristic of the field $\mathbb{F}_q$,

$g(F)$ the genus of F,

$N(F)$ the number of rational places (= places of degree 1) of F over $\mathbb{F}_q$,

$\mathbb{P}_F$ the set of all places of $F/\mathbb{F}_q$,

$\mathcal{O}_P$ the valuation ring of the place $P \in \mathbb{P}_F$,

$\mathcal{O}_P/P$ the residue class field of the place P,

$x \mod P$ the residue class of an element $x \in \mathcal{O}_P$ in $\mathcal{O}_P/P$,

(x) the principal divisor of an element $0 \neq x \in F$,

$(x)_\infty$ the divisor of poles of x,

$(x)_0$ the divisor of zeros of x,

$\mathcal{L}(A)$ the Riemann-Roch space associated to the divisor A.

Then for the fixed parameters q and N the set $\mathfrak{G}(q, N)$ is defined in terms of the language of function fields as follows.

$$\mathfrak{G}(q,N) := \{g \mid \text{there exists a function field over } \mathbb{F}_q \text{ of genus } g \text{ having exactly } N \text{ rational places}\}$$

2.1. $\mathfrak{G}(q, N)$ for Small Values q and N

We have seen that there is an integer g_0 (depending on q and N) such that

$$[g_0, \infty) \subseteq \mathfrak{G}(q, N) \subseteq \left[\frac{|\, N - (q+1) \,|}{[2\sqrt{q}\,]}, \infty\right).$$

It seems difficult to describe the set $\mathfrak{G}(q, N)$ explicitly for any given values of q and N. However for some small values, more precise results are obtained by constructing function fields with prescribed number of rational places. It is worth noting that in these cases the difference set $\mathbb{N} \setminus \mathfrak{G}(q, N)$ is smaller compared to the results obtained by an estimate for the constant g_0 given in the following sections when q is a prime number.

Theorem 2.1.1 *Given small q and N as below we have the following results on $\mathfrak{G}(q, N)$.*

$\mathfrak{G}(2,0) = [2,\infty)$	$\mathfrak{G}(2,1) = [1,\infty)$	$\mathfrak{G}(2,2) = [1,\infty)$
$\mathfrak{G}(2,3) = [0,\infty)$	$\mathfrak{G}(2,4) = [1,\infty)$	$\mathfrak{G}(2,5) = [1,\infty)$
$\mathfrak{G}(2,6) = [2,\infty)$	$\mathfrak{G}(2,7) = [3,\infty)$	$\mathfrak{G}(2,8) = [4,\infty)$[a]
$[5,\infty) \subseteq \mathfrak{G}(2,9) \subseteq [4,\infty)$	$\mathfrak{G}(3,0) = [2,\infty)$	$\mathfrak{G}(3,1) = [1,\infty)$
$\mathfrak{G}(3,2) = [1,\infty)$	$\mathfrak{G}(3,3) = [1,\infty)$	$\mathfrak{G}(3,4) = [0,\infty)$
$\mathfrak{G}(3,5) = [1,\infty)$	$\mathfrak{G}(3,6) = [1,\infty)$	$\mathfrak{G}(3,7) = [1,\infty)$
$\mathfrak{G}(3,8) = [2,\infty)$	$\{4,6\} \cup [8,\infty) \subseteq \mathfrak{G}(3,9) \subseteq [3,\infty)$	$\mathfrak{G}(4,0) = [2,\infty)$
$\mathfrak{G}(4,5) = [0,\infty)$	$\mathfrak{G}(5,0) = [2,\infty)$	$\mathfrak{G}(5,6) = [0,\infty)$
$\mathfrak{G}(7,8) = [0,\infty)$		

[a] $3 \notin \mathfrak{G}(2,8)$ comes from [41].

Furthermore,

$[\frac{q-1}{2}, \infty) \subseteq \mathfrak{G}(q, q+1)$	*for odd values of q;*
$[\frac{q}{2}, \infty) \subseteq \mathfrak{G}(q, q+1)$	*for even values of q;*
$[q-1, \infty) \subseteq \mathfrak{G}(q, 2q+1)$	*for even values of q;*
$[\frac{q-1}{2}, \infty) \subseteq \mathfrak{G}(q, 2q+1)$	*for odd values of q; and*
$[\frac{q-1}{2}, \infty) \subseteq \mathfrak{G}(q, 1)$	*for odd values of q.*

Proof: Here we only give a proof of the more involved cases.

<u>$q = 2$, $N = 7$:</u>

$0, 1 \notin \mathfrak{G}(2, 7)$ comes from the Serre's bound (1.2). It is known that a function field F

of genus $g(F) = 2$ is hyperelliptic. So, F contains a rational function field $\mathbb{F}_2(x) \subseteq F$ with $[F : \mathbb{F}_2(x)] = 2$. Since $\mathbb{F}_2(x)$ has 3 rational places, the number of rational places of F cannot be bigger than 6, that is, $2 \notin \mathfrak{G}(2, 7)$.
For $g = 3$ the existence of a function field over $\mathbb{F}_2$ of genus 3 with exactly 7 rational places is given by Serre in [34, part II p.41] and [33, p. 401].
Now we consider the case $g \geq 4$. We need to show that for all integers $g \geq 4$ there exists a function field $F/\mathbb{F}_2$ of genus g with exactly 7 rational places. Let $E = \mathbb{F}_2(x, y)$ be the function field with $y^2 + y = x + \frac{1}{x}$. Then $(x = \infty)$ and $(x = 0)$ are the only ramified places of $\mathbb{F}_2(x)$ in $E/\mathbb{F}_2(x)$ with ramification indexes and different exponents 2 (see Theorem 5.0.23), so by the Hurwitz genus formula (5.2) $g(E) = 1$. Furthermore, $(x = 1)$ splits in $E/\mathbb{F}_2(x)$; i.e. $N(E) = 4$. Denote by R, S the rational places of E over $(x = 1)$ and by P, Q the rational places over $(x = \infty)$, $(x = 0)$, respectively. From the defining equation a place of F is a pole y if an only if it is a zero or pole of x. Hence from the fact that $\deg(y)_\infty = [E : \mathbb{F}_2(y)] = 2$ we conclude that $(y)_\infty = (y + 1)_\infty = P + Q$. Since y and $y + 1$ can not have a common zero divisor and the zeros of y and $y + 1$ lie over the place $(x = 1)$ of $\mathbb{F}_2(x)$, $(y)_0 = 2S$ and $(y+1)_0 = 2R$. As a result, the principal divisors of x, $x + 1$, y and $y + 1$ in E are given as follows.

$$(x) = 2Q - 2P \qquad (x + 1) = R + S - 2P$$
$$(y) = 2S - P - Q \qquad (y + 1) = 2R - P - Q$$

Now consider the function field $F = E(z)$ defined by the equation

$$z^2 + z = x^{g-3}y(x + 1) \quad \text{for } g > 3.$$

Since the principal divisor of $x^{g-3}y(x + 1)$ in E is $(2g - 7)Q + 3S + R - (2g - 3)P$, P is the only ramified place with different exponent $2g - 2$, and the places Q, S, R split in F/E. Hence F is a function field over $\mathbb{F}_2$ of genus g with exactly 7 rational places, which completes the proof of the case $q = 2$, $N = 7$ and shows that $\mathfrak{G}(2, 7) = [3, \infty)$.

$q = 4$, $N = 5$:
$0 \in \mathfrak{G}(4, 5)$ comes from the fact that a rational function field over $\mathbb{F}_4$ has exactly 5 rational places. Now set $\mathbb{F}_4 := \mathbb{F}_2(\alpha)$, where $\alpha^2 + \alpha = 1$; i.e., $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. Let $F = \mathbb{F}_4(x, y)$ be a function field with a defining equation

$$y^2 + y = \begin{cases} x^{2g}(x + 1) & \text{, if } g \equiv 0 \mod 3 \\ x^{2g}(x + \alpha) & \text{, otherwise} \end{cases}$$

for $g > 0$. In the case of $g \equiv 0 \mod 3$, the places $(x = 0)$, $(x = 1)$ split, and $(x = \alpha)$, $(x = \alpha + 1)$ are inert in $F/\mathbb{F}_4(x)$ as $y^2 + y = \alpha + 1$ and $y^2 + y = \alpha$ are irreducible polynomials over $\mathbb{F}_4$. In the other case $(x = 0)$, $(x = \alpha)$ split and $(x = 1)$, $(x = \alpha + 1)$ are inert. Furthermore, in both cases $(x = \infty)$ is the only ramified place, which is totally ramified, with a different exponent $d = 2g + 2$. Therefore F has exactly 5 rational places and as a consequence of the Hurwitz genus formula $g(F) = g$, giving that $\mathfrak{G}(4, 5) = [0, \infty)$.

<u>$N = 2q + 1$ **for even values of** q**:**</u>
For $q > 2$ and $g \geq q - 1$, let $h(x)$ and $g(x)$ be irreducible polynomials over $\mathbb{F}_q$ of degree 3 and $2g - (q + 2)$, respectively. Set $F = \mathbb{F}_q(x, y)$ with the defining equation $y^2 + y = \frac{x^q+x}{h(x)} g(x)$. Then $(x = \infty)$ and the zero of $h(x)$ are the only ramified places in $F/\mathbb{F}_q(x)$ with different exponents $2g - 4$ and 2, respectively. So, by the Hurwitz genus formula (5.2)

$$g(F) = -1 + \frac{1}{2}\mathrm{degDiff}(F/\mathbb{F}_q(x)) = -1 + \frac{1}{2}(2\mathrm{deg}h(x) + 2g - 4) = g$$

All rational places other than $(x = \infty)$ split by Kummer's Theorem 5.0.21. So, F has exactly $2q + 1$ rational places.
For $q = 2$ the equation $y^2 + y = x^{2g}(x + 1)$ defines a function field $F = \mathbb{F}_q(x, y)$ over $\mathbb{F}_q$ of genus $g(F) = g$ and $N(F) = 5$. Therefore $[q - 1, \infty) \subseteq \mathfrak{G}(q, 2q + 1)$ for even values of q.

<u>$N = 2q + 1$ **for odd values of** q**:**</u>
Consider the function field $F = \mathbb{F}_q(x, y)$ with $y^2 = u(x)$, where $u(x)$ is a separable polynomial of degree $2g + 1$ such that $u(\alpha) = 1$ for all $\alpha \in \mathbb{F}_q$. By Kummer's Theorem 5.0.21 all rational places of $(x = \alpha)$ split in $F/\mathbb{F}_q(x)$. The ramified places of $\mathbb{F}_q(x)$ are exactly the zeros of $u(x)$ and $(x = \infty)$ with different exponents 1 (see Theorem 5.0.22). Therefore the number of rational places of F is $2q + 1$, and by the Hurwitz genus formula, the genus of F is g. Now we show the existence of such a polynomial $u(x)$ for all odd integers $2g + 1 \geq q$.
Write $2g + 1 = t(q - 1) + \ell$, where t, ℓ are integers with $0 < \ell < q - 1$. Define

$$u(x) := \begin{cases} (x^\ell + x)(x^{q-1} - 1)^t + 1 & \text{, if } p \mid \ell \text{ and } p \mid t \\ ax^\ell(x^{q-1} - 1)^t + 1 & \text{, otherwise} \end{cases} ,$$

where a is a non-zero element in $\mathbb{F}_q$. Then $u(x)$ is a polynomial of degree $2g+1$. In the first case, i.e. $p \mid \ell$ and $p \mid t$, it is clear that $u(x)$ is a separable polynomial satisfying the desired conditions. For the other case, it is sufficient to show that there exists an element $a \in \mathbb{F}_q \setminus \{0\} =: \mathbb{F}_q^*$ such that $u(x)$ is separable. Note that the derivative of $u(x)$ is

$$u'(x) = ax^{\ell-1}(x^{q-1} - 1)^{t-1}((\ell - t)x^{q-1} - \ell) .$$

If $\ell - t \equiv 0 \mod p$, $t \equiv 0 \mod p$ or $\ell \equiv 0 \mod p$, then $u(x)$ is separable for any chosen $a \in \mathbb{F}_q^*$. Hence we can assume that $\ell - t$, t and ℓ are not congruent to 0 modulo p.

We give a proof by contradiction. Assume that for all $a \in \mathbb{F}_q^*$, $u(x)$ and $u'(x)$ have a common root in the algebraic closure of $\mathbb{F}_q$, say $\alpha_{(a)}$. This is possible only if $\alpha_{(a)}$ is a common root of $u(x)$ and $(\ell - t)x^{q-1} - \ell$. As $(\ell - t)\alpha_{(a)}^{q-1} - \ell = 0$ and $u(\alpha_{(a)}) = 0$, $\alpha_{(a)}^{\ell} = -\frac{1}{a}\left(\frac{\ell-t}{t}\right)^t$. In other words, $\alpha_{(a)}$ is a common root of the polynomials

$$x^{q-1} = \frac{\ell}{\ell - t} \qquad \text{and} \qquad x^{\ell} = -\frac{1}{a}\left(\frac{\ell - t}{t}\right)^t.$$

Denote by $\alpha_1, \ldots, \alpha_{q-1}$ all distinct roots of $x^{q-1} = \frac{\ell}{\ell-t}$.

If $\mathbb{F}_q^* \backslash \{\alpha_1^{\ell}, \ldots, \alpha_{q-1}^{\ell}\}$ is non-empty, then to obtain a contradiction it is enough to choose $a \in \mathbb{F}_q^*$ such that $-\frac{1}{a}\left(\frac{\ell-t}{t}\right)^t \in \mathbb{F}_q^* \setminus \{\alpha_1^{\ell}, \ldots, \alpha_{q-1}^{\ell}\}$.

Assume that $\mathbb{F}_q^* = \{\alpha_1^{\ell}, \ldots, \alpha_{q-1}^{\ell}\}$, then $(\alpha_1 \ldots \alpha_{q-1})^{\ell} = -1$. Also $\alpha_1 \ldots \alpha_{q-1} = -\frac{\ell}{\ell-t}$ since α_i's are roots of $x^{q-1} = \frac{\ell}{\ell-t}$. As a result, $\left(\frac{\ell}{\ell-t}\right)^{\ell} = 1$. This shows that ℓ can not be relatively prime to $q-1$. Let $m = \gcd(\ell, q-1)$, then $q - 1 = rm$ and $\ell = sm$ for some $s, r \in \mathbb{Z}_{>0}$. The equality $(\alpha^{q-1})^s = (\alpha^{\ell})^r$ gives that a must be a root of $x^r - d$, where $d = \frac{(-1)^r(\ell-t)^{tr+s}}{\ell^s t^{tr}}$. Hence it is enough to choose $a \in \mathbb{F}_q^* \setminus \{\beta \in \mathbb{F}_q \mid \beta^r = d\}$ to get a contradiction.

So we conclude that $[\frac{q-1}{2}, \infty) \subseteq \mathfrak{G}(q, 2q+1)$

□

2.2. Bound for g_0 by Riemann-Roch Spaces

In [39] Stichtenoth gave a proof for the existence of the constant g_0 by using Riemann-Roch spaces. In this section with the same construction we give g_0 as a function of the given number of rational places N and the cardinality q of the finite field. For this, we need some preliminary results which we also make use of in the following sections.

Lemma 2.2.2 *Let F be a function field over $\mathbb{F}_q$ of genus $g(F) > 1$ and let r be an integer $> 2g(F)$. Then there exists a place P of F of degree r.*

Proof: See [6], Lemma 2.1. □

Lemma 2.2.3 *Let F be a function field over $\mathbb{F}_q$ of genus $g(F) > 1$ and $\alpha \in \mathbb{F}_q$. For given integers N, r with*

$$0 \leq N \leq N(F) \quad \textit{and} \quad r \geq 2g + 1 + N(F) - N,$$

set $s := N(F) - N$ and denote by $P_1, \ldots, P_N, Q_1, \ldots, Q_s$ the distinct rational places of F. Then there exist a place P of F of degree r and an element $x \in F$ with the following properties:

(i) *x has simple poles at $P, P_1, \ldots, P_N$, and has no other poles.*

(ii) $x \mod Q_i = \alpha$ *for* $i = 1, \ldots, s$.

Proof: By Lemma 2.2.2, there exists a place P of F of degree r. As $r - s \geq 2g + 1$, the Riemann-Roch theorem gives that there exist non-zero elements $x_1, \ldots, x_N, u$ of F with

$$u \in \mathcal{L}(P - \sum_{i=1}^{s} Q_i) \quad \text{and} \quad x_j \in \mathcal{L}(P + P_j - \sum_{i=1}^{s} Q_i) \setminus \mathcal{L}(P - \sum_{i=1}^{s} Q_i)$$

for $j = 1, \ldots, N$ (see (5.1)). Set

$$\tilde{x} := \begin{cases} \sum_{j=1}^{N} x_j & \text{, if } P \text{ is a pole of } \sum_{j=1}^{N} x_j \\ u + \sum_{j=1}^{N} x_j & \text{, otherwise.} \end{cases}$$

Then $x := \tilde{x} + \alpha$ has the desired properties. □

Lemma 2.2.4 *Let $q = p^n$, where $p = \mathrm{char}\mathbb{F}_q$, and let r be a positive divisor of n. Assume that $E/\mathbb{F}_q$ is a function field of genus $g = g(E) > 1$. Then for any non-negative integers j, N with $N \leq N(E)$ there exists a function field $F/\mathbb{F}_q$ with*

$$N(F) = N \quad \textit{and} \quad g(F) = g(E) + (p^r - 1)(3g(E) + N(E)) + j(p^r - 1).$$

Proof: Set $s := N(E) - N$ and denote by $P_1, \ldots, P_N, Q_1, \ldots, Q_s$ the distinct rational places of E. Choose $\alpha \in \mathbb{F}_q \setminus \mathrm{Im}(\varphi)$, where φ is the map from $\mathbb{F}_q$ to $\mathbb{F}_q$ given by $\beta \mapsto \beta^{p^r} - \beta$. By Lemma 2.2.3, there exist $x \in E$ and a place P of E of degree $2g(E) + 1 + s + j$ with pole divisor $(x)_\infty = P + P_1 + \ldots + P_N$ and $x \mod Q_i = \alpha$. Then by Theorems 5.0.21 and 5.0.23, the equation $y^{p^r} - y = x$ defines a function field $F := E(y)$ over $\mathbb{F}_q$ such that

(i) F/E is a Galois extension of degree $[F : E] = p^r$,

(ii) $P, P_1, \ldots, P_N$ are totally ramified in F/E with different exponents $2(p^r - 1)$, all other places of E are unramified in F, and

(iii) $Q_1, \ldots, Q_s$ are inert.

Hence $N(F) = N$ and by the Hurwitz genus formula (5.2)

$$2g(F) - 2 = p^r(2g(E) - 2) + 2(p^r - 1)(2g(E) + 1 + s + j + N) ;$$

or equivalently $g(F) = g(E) + (p^r - 1)(3g(E) + N(E)) + j(p^r - 1)$. □

Now we can state the main theorem of this section.

Theorem 2.2.5 *Let q be a power of a prime number. Then there exist constants $c(q) > 0$ and $1 < e(q) < 3$ (depending only on q) such that for any integers N, g with $N > 2q$ and $g \geq c(q)N^{e(q)}$ there exists a function field F over $\mathbb{F}_q$ of genus $g(F) = g$ with exactly N rational places. In other words, for sufficiently large integers N, $[c(q)N^{e(q)}, \infty) \subseteq \mathfrak{G}(q, N)$.*

Proof: First fix an integer i in the set $\{1, \cdots, q-1\}$ and consider a function field $E_0/\mathbb{F}_q$ of genus $g(E_0) = (q-1)+i$ with exactly $2q+1$ rational places, which is possible by Theorem 2.1.1. Since $g(E_0) < N(E_0)$, by Lemma 2.2.2, we can choose a place Q_0 of E_0 of degree $g(E_0) + N(E_0)$. Denote by $P_1^{(0)}, \cdots, P_{2q+1}^{(0)}$ the distinct rational places of E_0. According to the Riemann-Roch theorem (5.1) there exists a non-zero element $z_0 \in \mathcal{L}(Q_0 - \sum_{k=1}^{2q+1} P_k^{(0)})$. Define $E_1 = E_0(y_1)$ by the equation $y_1^q - y_1 = z_0$. Then by Theorems 5.0.21 and 5.0.23, Q_0 is the only ramified place with a different exponent $2(q-1)$ and all rational places split in E_1/E_0. So, $N(E_1) = q(2q+1)$ and by the Hurwitz genus formula we have:

$$\begin{aligned} g(E_1) &= qg(E_0) + (q-1)(\deg Q_0 - 1) \\ &= qg(E_0) + (q-1)(g(E_0) + N(E_0) - 1) \\ &= q(q+i-1) + (q-1)(3q+i) \\ &\leq q(2q-2) + (q-1)(4q-1) \\ &< 9q^2 \ . \end{aligned}$$

As $N(E_1) < g(E_1)$, we can take $z_1 \in \mathcal{L}(Q_1 - \sum_{k=1}^{q(2q+1)} P_k^{(1)}) \setminus \{0\}$, where Q_1 is a degree $2g(E_1)+1$ place and for $k = 1, \cdots, q(2q+1)$, $P_k^{(1)}$'s are the distinct rational places of E_1. Set $E_2 = E_1(y_2)$, where y_2 satisfies the equation $y_2^q - y_2 = z_1$. Then $N(E_2) = q^2(2q+1)$ and

$$g(E_2) = qg(E_1) + 2(q-1)g(E_1) < 27q^3 \ .$$

Inductively for each $n \geq 3$, we can do the same construction as follows:
Denote by $P_0^{(n-1)}, \ldots, P_{q^{(n-1)}(2q+1)}^{(n-1)}$ the distinct rational places of E_{n-1} and choose a place Q_{n-1} of E_{n-1} of degree $2g(E_{n-1})+1$. Then take a non-zero element

$$z_{n-1} \in \mathcal{L}(Q_{n-1} - \sum_{k=1}^{q^{(n-1)}(2q+1)} P_{k_{(n-1)}}) \ ,$$

which is possible as $g(E_{n-1}) > N(E_{n-1})$ for all $n-1 \geq 2$. The equation $y_n^q - y_n = z_{n-1}$ defines a function field $E_n = E_{n-1}(y_n)$ over $\mathbb{F}_q$ such that $N(E_n) = q^n(2q+1)$ and $g(E_n) < (3q)^{n+1}$. Since all extensions are of Artin-Schreier type, $g(E_n) \equiv i \mod (q-1)$ for all $n \geq 0$.

In the case $N > 2q$ there exists an integer $t > 0$ such that $q^t < \frac{N}{2} \leq q^{t+1}$. Set $E := E_t$ and

$$g_0^{(i)} := g(E) + (q-1)(3g(E) + N(E)) \ .$$

By Lemma 2.2.4, for all integers $g \geq g_0^{(i)}$ with $g \equiv g_0^{(i)} \mod (q-1)$ there exists a function field $F/\mathbb{F}_q$ of genus $g(F) = g$ with exactly N rational places. Hence it is enough to set

$$g_0 := \max\{g_0^{(i)}\}_{i=1}^{q-1} < 4qg(E) < 4q(3q)^{t+1}.$$

Since $q^t < \frac{N}{2}$, $g_0 < 6q^2 N 3^{\log_q \frac{N}{2}}$, which gives the desired result. □

Remark 2.2.1 *In the same way, it can also be shown that* $[8q^2, \infty) \subseteq \mathfrak{G}(q, N)$ *for* $0 \leq N \leq 2q$*.*

Remark 2.2.2 *The result of Theorem 2.2.5 is improved in Theorem 2.4.15, in particular the constant* g_0 *is given as a linear function of* N*.*

2.3. Improvement of g_0 for Square Constant Fields by Garcia-Stichtenoth Tower

The Hasse-Weil bound (1.1) shows that there exists a constant $d(q) > 0$ depending on q such that $g_0 > d(q)N$. In other words, a lower bound for the constant g_0 can be given as a linear function on N. Then the question whether one can improve g_0 so that it becomes a linear function on N naturally arises.

In the previous section the genus of an inductively constructed function field grows much faster than does the number of its rational places. To have a better estimate for g_0 we need a function field whose number of rational places is sufficiently large compared to its genus. For this reason we use asymptotically good towers over square constant fields given by Garcia and Stichtenoth [7]. In addition, instead of q-extensions we use p-extensions, where $p = \mathrm{char}\mathbb{F}_q$, so that the constants defined as $c(q)$ and $e(q)$ can be given in terms of the prime number p.

Theorem 2.3.6 *[Garcia-Stichtenoth Tower] Let* $\mathcal{H} := (H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots)$ *be the tower over* $\mathbb{F}_{q^2}$ *recursively defined by*

$$H_0 := \mathbb{F}_{q^2}(x_0) \quad \textit{and} \quad H_{i+1} := H_i(z_{i+1}),$$

where $z_{i+1}^q + z_{i+1} = x_i^{q+1}$ *and* $x_{i+1} := \frac{z_{i+1}}{x_i}$ *for all* $i \geq 0$*.*
The tower has the following properties, for all $i \geq 0$*:*

(i) *The extensions H_{i+1}/H_i are Galois of degree $[H_{i+1} : H_i] = q$.*

(ii) *The zero of $x_0 - \alpha$ splits completely in H_i/H_0 for all $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$.*

(iii) *The pole of x_0 is totally ramified in H_i/H_0 and the remaining ramified places lie over the zero of x_0.*

(vi) *The genus $g_i = g(H_i)$ is given by the following formula*

$$g_i = \begin{cases} q^{i+1} + q^i - q^{\frac{i+2}{2}} - 2q^{\frac{i}{2}} + 1 & , \text{ if } i \equiv 0 \mod 2 \\ q^{i+1} + q^i - \frac{1}{2}q^{\frac{i+3}{2}} - \frac{3}{2}q^{\frac{i+1}{2}} - q^{\frac{i-1}{2}} + 1 & , \text{ if } i \equiv 1 \mod 2 \end{cases} .$$

(v) *$N(H_i) \geq (q-1)g(H_i)$.*

For details and the proof of the Theorem, see [7].

From now on we assume that $p = \mathrm{char}\mathbb{F}_{q^2}$ and $q = p^n$ for an integer $n > 0$.

Lemma 2.3.7 *Let H_0 and H_1 be the function fields over $\mathbb{F}_{q^2}$ as given in Theorem 2.3.6. Then there exists a sequence of function fields $F_0 := H_0 \subseteq F_1 \subseteq \ldots \subseteq F_n := H_1$ with the following properties:*

(i) *The extensions F_{i+1}/F_i are Galois of degree $[F_{i+1} : F_i] = p$ for $0 \leq i \leq n-1$.*

(ii) *$g(F_i) = \frac{1}{2}q(p^i - 1)$ and $N(F_i) = p^i q^2 + 1$ for $0 \leq i \leq n$.*

Proof: All rational places of H_0 except the pole of x_0 split in H_1 and the pole of x_0 is the only (totally) ramified place. Denote the Galois group of H_1/H_0 by G, then elements of G can be given by

$$\alpha := \begin{cases} x_0 & \mapsto & x_0 \\ z_1 & \mapsto & z_1 + c \end{cases} , \quad c \in \mathbb{F}_{q^2} \text{ with } c^q + c = 0.$$

Since G is a p-group, it has a normal subseries

$$G_0 := G \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{id\} \quad \text{with } |G_i| = p^{n-i} \quad \text{for } i = 0, \ldots, n.$$

Set F_i as the fixed field of G_i, then F_{i+1}/F_i and F_n/F_i are Galois extensions of degree $[F_{i+1} : F_i] = p$ and $[F_n : F_i] = p^{n-i}$ for $i = 0, \ldots, n-1$. Denote the pole of x_0 in F_i by P_i, and j-th ramification group at $P_n \mid P_i$ by $G_i^{(j)}$. $t = \frac{x_0}{z_1}$ is a local parameter at P_n and for $\alpha \in G_i \setminus \{id\}$

$$v_{P_n}(\alpha(t) - t) = v_{P_n}(x_0) - 2v_{P_n}(z_1) = q + 2$$

since $v_{P_n}(x_0) = -q$ and $z_1^q + z_1 = x_0^{q+1}$ gives that $v_{P_n}(z_1) = -(q+1)$. Hence $\alpha \in G_i^{(j)}$ for $j = 0, \ldots, q+1$ and by Hilbert's different formula the different exponent $d(P_n \mid P_i)$ can be computed as follows:

$$d(P_n \mid P_i) = \sum_{j=0}^{q+1} |G_i^{(j)}| - 1 = (q+2)(|G_i| - 1) = (q+2)(p^{n-i} - 1) .$$

Then from the facts that

$$g(H_1) = \frac{q(q-1)}{2} \quad \text{and} \quad 2g(H_1) - 2 = p^{n-i}(2g(F_i) - 2) + d(P_n \mid P_i)$$

we obtain $g(F_i) = \frac{1}{2}q(p^i - 1)$. Since all rational places of H_0 but the pole of x_0 split in F_i/H_0, $N(F_i) = p^i q^2 + 1$ for $0 \le i \le n$. □

We can refine all steps of the Garcia-Stichtenoth tower into degree p-extensions as in Lemma 2.3.7 to get the following result.

Lemma 2.3.8 *There exists an infinite tower of function fields over* $\mathbb{F}_{q^2}$

$$\mathcal{F} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_k \subseteq \ldots$$

with the following properties: For all $i \ge 0$,

(i) $F_0 = \mathbb{F}_{q^2}(x_0)$ *is a rational function field, and each extension* F_{i+1}/F_i *is Galois of degree* $[F_{i+1} : F_i] = p$;

(ii) $g(F_1) = q\frac{p-1}{2}$, *and* $g(F_{i+1}) \ge pg(F_i)$;

(iii) $p^i(q^2 - 1) < N(F_{i+1}) \le p^i q^2 + 1$; *and*

(vi) $N(F_i) \ge (q-1)g(F_i)$.

Proof: Let $\mathcal{H} := (H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots)$ be the Garcia-Stichtenoth tower over $\mathbb{F}_{q^2}$ given in Theorem 2.3.6. For each integer $k \ge 1$ divide H_k/H_{k-1} into p-extensions

$$H_{k-1} = F_{(k-1)n} \subseteq F_{(k-1)n+1} \subseteq F_{(k-1)n+2} \subseteq \ldots \subseteq F_{kn} = H_k$$

as in Lemma 2.3.7 and set

$$\mathcal{F} := (F_0 = H_0 \subseteq \ldots \subseteq F_n = H_1 \subseteq \ldots \subseteq F_{2n} = H_2 \subseteq \ldots) .$$

Then each extension F_{i+1}/F_i is Galois of degree $[F_{i+1} : F_i] = p$ for all $i \ge 0$. By Theorem 2.3.6, the pole of x_0 is totaly ramified in F_{i+1}/F_i with a different exponent $d \ge 2(p-1)$. (In fact it can be easily seen that the different exponent is $(q+2)(p-1)$ by choosing a local parameter $t = \frac{x_{k-1}}{z_k}$ at the pole of x_0 in H_k as in Theorem 2.3.7, where $H_{k-1} \subsetneq F_{i+1} \subseteq H_k$, and applying transitivity of the different.) Hence the Hurwitz genus formula gives that $g(F_{i+1}) \ge pg(F_i)$ for all $i \ge 0$. Property (iii) comes from the fact that the zero of $x_0 - \alpha$ splits completely in each step for all $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$.

To show (iv), let $i \ge 0$ be an integer, then $(k-1)n < i \le kn$ for some positive integer k. By (ii) and (iii) together with the inequality $N(H_k) \ge (q-1)g(H_k)$ we get the following inequalities.

$$p^{kn-i}N(F_i) > N(F_{kn}) = N(H_k) \ge (q-1)g(H_k) = (q-1)g(F_{kn}) \ge (q-1)p^{kn-i}g(F_i)$$

Hence $N(F_i) \ge (q-1)g(F_i)$ for all $i \ge 0$. □

Lemma 2.3.9 *Fix an integer* $j \in \{0, \cdots, p-2\}$*. Then there is a tower* $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ *over* $\mathbb{F}_{q^2}$ *with the following properties: For all* $i \geq 0$,

(i) E_{i+1}/E_i *is Galois of degree* $[E_{i+1} : E_i] = p$*;*

(ii) $g(E_i) \equiv j \mod (p-1)$*; and*

(iii) $g(E_i) < \frac{3}{q-1} N(E_i)$.

Proof: For $p = 2$, Lemma 2.3.8 shows the existence of the required tower, that is, it is enough to take $\mathcal{E} = \mathcal{F}$. So from now on we assume that p is an odd prime.
Let $\mathcal{F} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n \subseteq \ldots$ be the tower given in Lemma 2.3.8 and let $E_0 = F_0(y)$ be the function field defined by $y^2 = cf(x_0)$, where $f(x_0)$ is an irreducible polynomial over $\mathbb{F}_{q^2}$ of degree $2j+2$ and $c \in \mathbb{F}_{q^2} \setminus \{0\}$ such that for at least $\frac{q^2-1}{2}$ elements $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$ the value $cf(\alpha)$ is square in $\mathbb{F}_{q^2}$. Set

$$\mathcal{E} = (E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots), \text{ where } E_i := E_0 F_i \text{ for all } i \geq 1.$$

As p is an odd prime, E_i/F_i and E_i/E_{i-1} are Galois extensions of degree $[E_i : F_i] = 2$ and $[E_i : E_{i-1}] = p$ for all $i \geq 1$ (see Theorems 5.0.22 and 5.0.23). By Abhyankar's Lemma (see Theorem 5.0.24(i)), the ramified places of F_i in E_i are exactly the places lying over the zero of $f(x_0)$ with different exponents 1. Then the Hurwitz genus formula gives the following equations.

$$\begin{aligned} g(E_i) &= 2g(F_i) + \tfrac{1}{2}\deg\mathrm{Diff}(E_i/F_i) - 1 \\ &= 2g(F_i) + \tfrac{1}{2}\deg\mathrm{Con}_{F_i/F_0}(f(x_0)) - 1 \\ &= 2g(F_i) + \tfrac{1}{2}p^i(2j+2) - 1 \end{aligned} \tag{2.1}$$

Since $g(F_i) \equiv 0$ or $\frac{p-1}{2} \mod (p-1)$, $g(E_i) \equiv j \mod (p-1)$.
Furthermore by Theorem 5.0.24(ii) there are at least $\frac{q^2-1}{2}$ rational places of F_0 that split completely in both extensions F_i and E_0, so we have

$$p^i(q^2-1) \leq N(E_i) \leq 2(p^i q^2 + 1)\ . \tag{2.2}$$

By (2.1), (2.2) and Lemma 2.3.8, we obtain the following inequalities.

$$\begin{aligned} g(E_i) &< 2g(F_i) + p^i(j+1) \\ &\leq \tfrac{2}{q-1}N(F_i) + \tfrac{p-1}{q^2-1}N(E_i) \\ &= \left(\tfrac{2}{q-1} \cdot \tfrac{N(F_i)}{N(E_i)} + \tfrac{p-1}{q^2-1}\right) N(E_i) \end{aligned}$$

Then $\frac{N(F_i)}{N(E_i)} \leq \frac{q^2+1}{(q^2-1)}$ gives that $g(E_i) < \frac{3}{q-1}N(E_i)$. □

Now we can give the main theorem of this section which improves the constant g_0 in the case of square constant fields.

Theorem 2.3.10 *Let $p = \mathrm{char}\mathbb{F}_{q^2}$. Assume that N is an integer with $N > q^2 - 1$ (and $N > 6$ in case $q = 2$). Then for every integer $g \geq 4p(p+11)N$ there is a function field F over $\mathbb{F}_{q^2}$ of genus $g(F) = g$ having exactly N rational places. In other words, for given integer N with $N > q^2 - 1$ (and $N > 6$ in case $q = 2$), $[4p(p+11)N, \infty) \subseteq \mathfrak{G}(q^2, N)$.*

Proof: First we consider the case $q > 2$. For $N > q^2 - 1$ there exists an integer $i \geq 0$ such that

$$p^i(q^2 - 1) < N \leq p^{i+1}(q^2 - 1) \ . \tag{2.3}$$

For fixed $j \in \{0, \ldots, p-2\}$, set

$$E := E_{i+1} \quad \text{and} \quad g_0^{(j)} := g(E) + (p-1)(3g(E) + N(E)) \ ,$$

where E_{i+1} is the function field given in Lemma 2.3.9. Then by Lemma 2.2.4, for all integers $g \geq \max\{g_0^{(j)}\}_{j=0}^{p-2}$, there exists a function field $F/\mathbb{F}_{q^2}$ of genus $g(F) = g$ having exactly N rational places. For any $j \in \{0, \ldots, p-2\}$, we have the following inequalities.

$$\begin{aligned}
g_0^{(j)} &= (3p-2)g(E) + (p-1)N(E) \\
&< \left((3p-2)\tfrac{3}{q-1} + p - 1\right) N(E) \qquad \text{(by Lemma 2.3.9)} \\
&< \left((3p-2)\tfrac{3}{q-1} + p - 1\right) 2p^{i+1}(q^2+1) \\
&< 2p\tfrac{q^2+1}{q^2-1}\left((3p-2)\tfrac{3}{q-1} + p - 1\right) N \qquad \text{(by Inequality 2.3)} \\
&\leq 2p(p+11)\tfrac{q^2+1}{q^2-1} \\
&< 4p(p+11)N
\end{aligned}$$

Note that $g(E_1) = 1$ if $q = 2$; so we need the condition $N > 6$ for $q = 2$. However the same proof works for $i + 1 \geq 2$. □

Remark 2.3.3 *By Lemma 2.3.8, we have seen that $g(E) \leq \frac{N(E)}{q-1}$ for $p = 2$. The same computation gives the following results:*

(i) $[34N, \infty) \subseteq \mathfrak{G}(4, N)$ *if $N > 6$;*

(ii) $[11N, \infty) \subseteq \mathfrak{G}(q^2, N)$ *if q is even with $q > 2$ and $N > q^2 - 1$; and*

(iii) $[4p(p+2)N, \infty) \subseteq \mathfrak{G}(q^2, N)$ *if q is odd with $q > p$ and $N > q^2 - 1$.*

Remark 2.3.4 $[2q^2(p-1) + 3p^2 - 2, \infty) \subseteq \mathfrak{G}(q^2, N)$ *holds for an integer N with $0 \leq N \leq q^2 - 1$.*

Proof: For $p \neq 2$, let $E := E_0$ be the function field over $\mathbb{F}_{q^2}$ with the same defining equation as in Lemma 2.3.9 for $j = 2, \ldots, p$. Then for any $j \in \{2, \ldots, p\}$, we have

$$g_0^{(j)} := (3p-2)g(E) + (p-1)N(E) \leq (3p-2)p + 2(p-1)(q^2+1) = 2q^2(p-1) + 3p^2 - 2 \ .$$

For $p = 2$, the same result can be obtained by choosing a function field $E/\mathbb{F}_{q^2}$ with $g(E) = 2$ and $N(E) \geq q^2 + 1$ and applying Theorem 2.3.10. □

2.4. Improvement of g_0 for Non-square Constant Fields

In this section we give an improvement of the constant g_0 for non-square constant fields by using a sequence of function fields $(F_n/\mathbb{F}_q)_{n\geq 0}$ with $\lim_{n\to\infty} N(F_n)/g(F_n) > 0$. First we deal with the case of prime constant fields $q = 2$ and $q = 3$, then we consider $q > 3$.

2.4.1. The Case $q = 2$ and $q = 3$

For these cases we make use of the results in [4] given in Lemmas 2.4.11 and 2.4.13.

Lemma 2.4.11 *There exists a sequence of function fields $\mathcal{F} = (F_0, F_1, \ldots)$ over $\mathbb{F}_2$ such that $g(F_0) = 0$, $g(F_1) = 2$ and for all $n \geq 0$*

$$N(F_n) = 3.2^n \quad \text{and} \quad g(F_n) \leq d \cdot N(F_n) \quad \text{with } d = 3.1546\ldots \ .$$

Proof: See Proposition 5.5 in [4]. □

For an integer $N > 3$ there exists an integer $i \geq 0$ such that $3.2^i < N \leq 3.2^{i+1}$. Set $E := F_{i+1}$ and $g_0 := 4g(E) + N(E)$. (Note that $g(E) \geq 2$ and $N(E) \geq N$.) Then

$$g_0 \leq (4d+1)N(E) = (4d+1)32^{i+1} < 2(4d+1)N \ . \qquad (2.4)$$

Hence from (2.4) and Lemma 2.2.4 we have the following result.

Lemma 2.4.12 *Let N be integer > 3, then $[28N, \infty) \subseteq \mathfrak{G}(2, N)$.*

Now we consider the case $q = 3$. For this case we need the following lemma.

Lemma 2.4.13 *Let $H = \mathbb{F}_3(x, y)$ with the defining equation $y^2 = x^3 - x + 1$. Then for all $n \geq 0$ there is a function field F_n over $\mathbb{F}_3$, which is an extension of H of degree $[F_n : H] = 3^n$ with $N(F_n) = 7.3^n$ and $g(F_n) \leq dN(F_n)$, where $d = 2.02890\ldots$.*

Proof: See Proposition 5.6 in [4]. □

Let $f(x)$ be an irreducible monic polynomial over $\mathbb{F}_3$ of degree 6 or 7. The place of $\mathbb{F}_3(x)$ corresponding the zero $f(x)$ is not ramified in the sequence of function fields constructed in the proof of Lemma 2.4.13. Then let $K = \mathbb{F}_3(x,z)$ be the function field with $z^2 = cf(x)$ such that at least 2 rational places $\mathbb{F}_3(x)$, other than the pole of x, split in K. Set $E_n := F_nK$, then by Theorem 5.0.24(ii), $N(E_n) \geq 8.3^n$. Furthermore, Theorem 5.0.24(i) gives that the ramified places of F_n in E_n are the places lying over the zero of $f(x)$. As a result of the Hurwitz genus formula we obtain

$$g(E_n) = 2g(F_n) + 3^n(\deg f(x)) - 1 \ . \tag{2.5}$$

Equation 2.5 implies that

$$g(E_n) \equiv \begin{cases} 0 \mod 2 & , \text{if } \deg f(x) = 7 \\ 1 \mod 2 & , \text{if } \deg f(x) = 6 \end{cases}$$

and

$$g(E_n) < 2g(F_n) + 3^n(\deg f(x)) \leq 2dN(F_n) + 3^n 7 = 7(2d+1)3^n < 5N(E_n),$$

where $d = 2.02890\ldots$. In the last inequality we used the fact that $3^n \leq N(E_n)/8$.

Let N be an integer with $8.3^i < N \leq 8.3^{i+1}$ for some integer $i \geq 0$. For a fixed $j \in \{0,1\}$ set $E := E_{i+1}$ and $g_0^{(j)} := 7g(E) + 2N(E)$. Then we have:

$$g_0^{(j)} < 37N(E) = 37 \cdot 7 \cdot 3^{i+1} < 98N$$

Therefore we have the following result.

Lemma 2.4.14 *Let N be integer > 8, then $[98N, \infty) \subseteq \mathfrak{G}(3,N)$.*

Remark 2.4.5 *Let N be an integer with $N \leq 3$ if $p = 2$ and $N \leq 8$ if $p = 3$. Then one can show as in Remark 2.3.4 $[14, \infty) \subseteq \mathfrak{G}(2,N)$ and $[84, \infty) \subseteq \mathfrak{G}(3,N)$.*

2.4.2. The Case $q > 3$

For the case $q > 3$ we use a result of Elkies et al. [6] stated as follows:

(*)*For every prime power q there is a positive constant c_q (which depends only on q) with the following property: for every integer $g \geq 0$, there is a function field over $\mathbb{F}_q$ with at least $c_q g$ rational places.*

Theorem 2.4.15 *For given q there are constants $f(q)$ and $h(q)$ (depending only on q) such that for any non-negative integers g and N with $g \geq f(q)N + h(q)$ there exists a function field F over $\mathbb{F}_q$ of genus $g(F) = g$ having exactly N rational places.*

Proof: Let c_q be the constant given in (*) and N be a non-negative integer. Define

$$d_j := \left\lceil \frac{N}{c_q} \right\rceil + j \quad \text{for } j = 2, \ldots, p \ ,$$

where $\lceil n \rceil$ is the smallest integer bigger than n; therefore $\{d_2, \ldots, d_p\}$ forms a complete set of representatives of the factor group $\mathbb{Z}/(p-1)\mathbb{Z}$. As a consequence of (*), for each $j \in \{2, \ldots, p\}$ there exists a function field $E_j/\mathbb{F}_q$ with $g(E_j) = d_j$ and

$$N(E_j) \geq c_q d_j = c_q \left(\left\lceil \frac{N}{c_q} \right\rceil + j \right) > N \ .$$

Set

$$g_0^{(j)} = d_j + (p-1)(3d_j + N(E_j)) \ ,$$

then we have

$$g_0^{(j)} < 3pd_j + pN(E_j) \leq 3pd_j + p(q + 1 + 2d_j\sqrt{q}) = (3p + 2p\sqrt{q})d_j + p(q+1) \ .$$

Note that the second inequality comes from the Hasse-Weil bound (1.1). Moreover, $d_j < \frac{N}{c_q} + p + 1$ gives that $g_0^{(j)} < \frac{(3p+2p\sqrt{q})}{c_q}N + p(q + 2p\sqrt{q} + 4\sqrt{q} + 3p + 7)$. Then the result follows from Lemma 2.2.4. □

A restatement of Theorem 2.4.15 is that for given any prime power q, there are constants $f(q)$ and $h(q)$ depending only on q such that for any non-negative integer N

$$[f(q)N + h(q), \infty) \subseteq \mathfrak{G}(q, N) \ .$$

CHAPTER 3

Function Fields with Prescribed Number of Places of Certain Degrees and Their L-polynomials

3.1. Function Fields with Prescribed Number of Places of Certain Degrees

In this section we prove a far-reaching generalization of Theorem 1.0.1 stated as follows.

Theorem 3.1.1 *Let q be a power of a prime number and let $b_1, \ldots, b_m$ be non-negative integers. Then there is an integer $g_0 \geq 0$ with the following property: for every $g \geq g_0$ there exists a function field $F/\mathbb{F}_q$ of genus $g(F) = g$ such that F has exactly b_r places of degree r for $r = 1, \ldots, m$.*

The proof of Theorem 3.1.1 is divided into several steps and in the proof we repeatedly use Riemann-Roch spaces and Artin-Schreier type extensions.

From now on for a non-negative integer r, we denote by $B_r(F)$ the number of degree r places of a function field $F/\mathbb{F}_q$.

Lemma 3.1.2 *For every $\ell \in \{0, \ldots, q-2\}$ there exists a function field $F/\mathbb{F}_q$ with $g(F) = \ell$ and $B_1(F) > 0$.*

Proof: In the case of even characteristic, the function field $F = \mathbb{F}_q(x, y)$ defined by the equation $y^2 + y = x^{2\ell+1}$ has genus ℓ and $B_1(F) > 0$ as the zero of x splits in $F/\mathbb{F}_q(x)$. Now assume that q is a power of an odd prime number. Consider the function field $F = \mathbb{F}_q(x, y)$ given by the equation

$$y^2 = \begin{cases} x^{2\ell+1} + x + 1 & \text{, if } p \mid 2\ell + 1 \\ x^{2\ell+1} + 1 & \text{, otherwise.} \end{cases}$$

In both cases, the genus of F is ℓ, and the zero of x in $\mathbb{F}_q(x)$ splits into two rational places of F.

□

Lemma 3.1.3 *For every $\ell \in \{0, \ldots, q-2\}$ and every non-negative integer c there exists a function field $F/\mathbb{F}_q$ with $g(F) \equiv \ell \mod (q-1)$ and $B_1(F) \geq c$.*

Proof: By induction over c. For the case $c = 1$ the assertion is true by Lemma 3.1.2. Now assume that there exists a function field $E/\mathbb{F}_q$ with $g(E) \equiv \ell \mod (q-1)$ and $B_1(E) \geq c$. Denote c distinct rational places of E by $P_1, \ldots, P_c$ and choose a place Q of E of sufficiently large degree so that the Riemann-Roch space $\mathcal{L}(Q-(P_1+\ldots+P_c))$ is non-trivial. Consider the extension $F = E(y)$ given by the equation $y^q - y = x$, where x is a non-zero element in $\mathcal{L}(Q-(P_1+\ldots+P_c))$. Then by Theorems 5.0.23 and 5.0.22 we have:

(i) F/E is Galois of degree $[F : E] = q$;

(ii) Q is the only ramified place in F/E with different exponent $2(q-1)$; and

(iii) the places $P_1, \ldots, P_c$ split completely in F/E.

Therefore $B_1(F) \geq qc > c$ and by the Hurwitz genus formula

$$2g(F) - 2 = q(2g(E) - 2) + \deg \mathrm{Diff}(F/E) = q(2g(E) - 2) + 2(q-1) \deg Q \ .$$

This shows that $g(F) \equiv g(E) \equiv \ell \mod (q-1)$. □

Now we generalize the result of Lemma 3.1.3 to the number of places of any degree.

Lemma 3.1.4 *Let $\ell \in \{0, \ldots, q-2\}$ and $c_1, \ldots, c_m$ be non-negative integers. Then there exists a function field $F/\mathbb{F}_q$ with*

$$g(F) \equiv \ell \mod (q-1) \quad \textit{and} \quad B_1(F) \geq c_1, \ \ldots, \ B_m(F) \geq c_m \ .$$

Proof: By induction over m. The case $m = 1$ was established in Lemma 3.1.3. Now assume that the statement is true for $m - 1 \geq 1$. For given $c_1, \ldots, c_m$, we can assume that at least one of the c_i is strictly positive; otherwise the assertion is trivial. Set $c := \max\{c_1, \ldots, c_m\}$. By the induction hypothesis, there exists a function field $E/\mathbb{F}_q$ with $g(E) \equiv \ell \mod (q-1)$ and $B_i(E) \geq c$ for $i = 1, \ldots, m-1$. Let

$$S := \{P \in \mathbb{P}_E \mid \deg P \leq m-1\} \ ,$$

and Q be a place of E of sufficiently large degree. Consider the extension F/E with the defining equation

$$y^{q^m} - y = x \ ,$$

where x is a non-zero element in $\mathcal{L}(Q - \sum_{P\in S} P)$. Note that $Y^{q^m} - Y \in \mathbb{F}_q[Y]$ factors into distinct irreducible polynomials over $\mathbb{F}_q$. By Kummer's Theorem 5.0.21, for each $P \in S$ there is a one-to-one correspondence between the set of the irreducible factors of $Y^{q^m} - Y$ over $\mathbb{F}_q$ and the set of places of F lying over P such that the relative degree is equal to degree of the corresponding irreducible polynomial. Among them, there are factors of degree one, so there are places $R \in \mathbb{P}_F$ lying above P with $\deg R = \deg P$. This shows that $B_j(F) \geq B_j(E) \geq c \geq c_j$ for $j = 1, \ldots, m-1$. Also $Y^{q^m} - Y$ has irreducible factors of degree m. So each rational place P has an extension $R \in \mathbb{P}_F$ with $\deg R = m$; therefore $B_m(F) \geq c \geq c_m$. Furthermore $g(F) \equiv \ell \mod (q-1)$ comes from the Hurwitz genus formula. □

The next result indicates that inequalities in the statement of Lemma 3.1.4 can be replaced by equalities.

Lemma 3.1.5 *Let $\ell \in \{0, \ldots, q-2\}$ and $c_1, \ldots, c_m$ be non-negative integers. Then there exists a function field $F/\mathbb{F}_q$ with*

$$g(F) \equiv \ell \mod (q-1) \quad \textit{and} \quad B_1(F) = c_1, \ \ldots, \ B_m(F) = c_m \ .$$

Proof: Let $F_0/\mathbb{F}_q$ be a function field with $g(F_0) \equiv \ell \mod (q-1)$ and $B_j(F_0) \geq c_j$ for $j = 1, \ldots, m$, whose existence is known by Lemma 3.1.4. Let S_1 be a subset of $\mathbb{P}_{F_0}$ consisting of c_1 places of degree 1, c_2 places of degree 2, ..., c_m places of degree m. Set

$$S_2 := \{R \in \mathbb{P}_{F_0} \mid \deg R \leq m \text{ and } R \notin S_1\} \ .$$

As the map from $\mathcal{O}_R/R$ to $\mathcal{O}_R/R$ given by $\alpha \mapsto \alpha^q - \alpha$ has a non-trivial kernel, for each $R \in S_2$ we can choose an element $a_R \in \mathcal{O}_R/R$ such that the equation

$$T^q - T = a_R \quad \text{has no solution in } \mathcal{O}_R/R \ .$$

Choose a place $Q \in \mathbb{P}_{F_0}$ of degree $\deg Q > m$ such that $\deg(Q - \sum_{R\in S_2} R) \geq 2g(F_0)$, and choose for all $P \in S_1$, a P-prime element $t_P \in F_0$. Then we define an $\mathbb{F}_q$-linear map ψ as follows:

$$\psi : \begin{cases} \mathcal{L}(Q + \sum_{P\in S_1} P) & \to \quad \bigoplus_{P\in S_1} \mathcal{O}_P/P \ \oplus \ \bigoplus_{R\in S_2} \mathcal{O}_R/R \\ \quad u & \mapsto \Big(\big(t_P \cdot u \bmod P\big)_{P\in S_1}, \big(u \bmod R\big)_{R\in S_2} \Big) \end{cases}$$

The kernel of ψ is the space $\mathcal{L}(Q - \sum_{R\in S_2} R)$; hence the rank of ψ is

$$\begin{aligned} \text{rank}\psi &= \ell\big(Q + \textstyle\sum_{P\in S_1} P\big) - \ell\big(Q - \textstyle\sum_{R\in S_2} R\big) \\ &= \deg\big(Q + \textstyle\sum_{P\in S_1} P\big) - \deg\big(Q - \textstyle\sum_{R\in S_2} R\big) \\ &= \textstyle\sum_{P\in S_1} \deg P + \textstyle\sum_{R\in S_2} \deg R \ . \end{aligned} \tag{3.1}$$

The second equality comes from the Riemann-Roch theorem and the fact that the degree of the divisor $Q - \sum_{R \in S_2} R$ is greater than $2g(F_0)$. Equation (3.1) shows that ψ is surjective. Let x_1 be an inverse image of $((0)_{P \in S_1}, (a_R)_{R \in S_2})$. Then for all $P \in S_1$, x_1 has a simple pole at P and for all $R \in S_2$, $x_1 \bmod R = a_R$. Set $x := x_1$ if also Q is a pole of x_1; otherwise set $x := x_1 + z$ with a non-zero element $z \in$ Ker ψ. Then we have:

(i) x has simple poles at Q and at all places $P \in S_1$, and

(ii) $x \bmod R = a_R$ for all $R \in S_2$.

Now consider the extension

$$F_1 := E(y) \;\text{ with }\; y^q - y = x \;.$$

Then by (i) all places $P \in S_1$ are totally ramified in F_1/F_0 giving c_j places of degree j in F_1, for $j = 1, \ldots, m$, and by (ii) for any place $R_1 \in \mathbb{P}_{F_1}$ lying above a place $R \in S_2$, the degree of R_1 is strictly larger than is the degree of R (see Theorems 5.0.23 and 5.0.22). Note that all other places of F_1 have still degree $> m$. There may still be some places of F_1 of degree $\leq m$, lying above places in S_2. However, by repeating this construction, after finitely many steps we obtain a function field F with $B_j(F) = c_j$ for $j = 1, \ldots, m$. As all extensions are of Artin-Schreier type, $g(F) \equiv \ell \mod (q-1)$. □

Proof of Theorem 3.1.1: Let $b_1, \ldots, b_m$ be given non-negative integers. It is enough to show that for all $\ell \in \{0, \ldots, q-2\}$ there exists a positive integer g_ℓ congruent to ℓ modulo $(q-1)$ with the following property: for every integer $g \geq g_\ell$ with $g \equiv g_\ell \mod (q-1)$, there exists a function field $F/\mathbb{F}_q$ of genus g having exactly b_j places of degree j for $j = 1, \ldots, m$.
We can start with a function field F_0 over $\mathbb{F}_q$ of genus $g(F_0) =: g_0 \equiv \ell \mod (q-1)$ with $B_j(F_0) = b_j$ for $j = 1, \ldots, m$. Note that this is possible by Lemma 3.1.5. Choose $r_0 \geq 2g_0 + 1$ such that for all $r_1 \geq r_0$ there is a place $Q \in \mathbb{P}_{F_0}$ with $\deg Q = r_1$. Let

$$S := \{P \in \mathbb{P}_{F_0} \mid \deg P \leq m\} \;\text{ and }\; D := \sum_{P \in S} P \;,$$

and set

$$g_\ell := g_0 + (q-1)(\deg D + g_0 - 1 + r_0) \;.$$

Note that $g_\ell \equiv \ell \mod (q-1)$; then for all $r \geq 0$ we need to construct a function field $F/\mathbb{F}_q$ of genus $g(F) = g_\ell + (q-1)r$ with $B_j(F) = b_j$ for $j = 1, \ldots, m$. This can be done as follows:
We choose a place $Q \in \mathbb{P}_{F_0}$ of degree $r_1 := r_0 + r$. As a result of the Riemann-Roch theorem for every $P \in S$,

$$\ell(Q + P) > \ell(Q) > 1.$$

Hence we can choose an element $x_P \in \mathcal{L}(Q+P) \setminus \mathcal{L}(Q)$ and $z \in \mathcal{L}(Q) \setminus \{0\}$. Set

$$x := \begin{cases} \sum_{P\in S} x_P & \text{, if also } Q \text{ is a pole of } \sum_{P\in S} x_P \\ \sum_{P\in S} x_P + z & \text{, otherwise.} \end{cases}$$

Note that x has simple poles at Q and at all places $P \in S$, and no other poles. Let $F := F_0(y)$ with the defining equation $y^q - y = x$. Then all places in the set S are totally ramified in F/F_0; i.e., $B_j(F) = B_j(F_0) = b_j$ for $1 \le j \le m$ by Theorem 5.0.23. Then the Hurwitz genus formula gives that

$$2g-2 = q(2g_0-2) + \deg\ \mathrm{Diff}(F/F_0) = q(2g_0-2) + 2(q-1)\deg(D+Q)\ .$$

This is what we need as

$$g = g_0 + (q-1)(\deg D + g_0 - 1 + (r_0+r)) = g_1 + (q-1)r\ .$$

□

3.2. Inequalities for the Coefficients of $L(t)$

In this section we give some inequalities for the coefficients of the L-polynomial of a function field F over $\mathbb{F}_q$. First we inductively define some polynomials over $\mathbb{Z}$ to formulate the result. We set

$$\sigma_0 := 0 \ \text{ and } \ \sigma_r(T_1,\ldots,T_r) := rT_r - \sum_{j=1}^{r-1} \sigma_{r-j}(T_1,\ldots,T_{r-j})\cdot T_j \ \text{ for all } \ r \ge 1\ . \quad (3.2)$$

Then we define

$$\beta_r(T_1,\ldots,T_r) := \sum_{d|r} \mu\big(\frac{r}{d}\big)\sigma_d(T_1,\ldots,T_d) + \sum_{d|r} \mu\big(\frac{r}{d}\big)(q^d+1)\ , \quad (3.3)$$

where $\mu(.)$ denotes the Möbius function. (3.2), (3.3) give that

$$\varphi_r(T_1,\ldots,T_{r-1}) := rT_r - \beta_r(T_1,\ldots,T_r) \quad (3.4)$$

is a polynomial in variables $T_1,\ldots,T_{r-1}$. For example, for $r \le 4$ the polynomials φ_r are given as follows:

$$\begin{aligned} &\varphi_1 = -(q+1)\ , \\ &\varphi_2(T_1) = T_1^2 + T_1 - (q^2-q)\ , \\ &\varphi_3(T_1,T_2) = -T_1^3 + T_1 + 3T_1T_2 - (q^3-q)\ , \\ &\varphi_4(T_1,T_2,T_3) = T_1^4 - T_1^2 - 4T_1^2T_2 + 4T_1T_3 + 2T_2^2 + 2T_2 - (q^4-q^2)\ . \end{aligned} \quad (3.5)$$

Now we can state the main theorem of this section which provides necessary inequalities for the coefficient of the L-polynomial of a function field.

Theorem 3.2.6 *Let $F/\mathbb{F}_q$ be a function field of genus $g \geq 1$ with its L-polynomial $L(t) = 1 + a_1 t + \ldots + a_{2g} t^{2g}$ and let $\varphi_r(T_1, \ldots, T_{r-1})$ be polynomials defined by Equation* (3.4). Then for $r = 1, \ldots, g$

$$ra_r \geq \varphi_r(a_1, \ldots, a_{r-1}).$$

Proof: Denote by $N_r = N_r(F)$ the number of rational places of the constant field extension $F_r := F\mathbb{F}_{q^r}$ over $\mathbb{F}_{q^r}$, and set $S_r = S_r(F) := N_r - (q^r + 1)$. Then the following formulas are well-known, see [38, Chapter 5].

$$a_1 = N - (q+1) \ ,$$

$$ra_r = S_r + \sum_{j=1}^{r-1} S_{r-j} a_j \quad \text{for} \quad r = 1, \ldots, g \ , \tag{3.6}$$

$$rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) \cdot (q^d + 1 + S_d) \quad \text{for all} \quad r \geq 1 \ . \tag{3.7}$$

Note that $\sigma_1(a_1) = a_1 = S_1$, and by induction over r using the definition of σ_r (3.2) and Equation (3.6), it is easy to show that

$$\sigma_r(a_1, \ldots, a_r) = S_r \quad \text{for} \quad r = 1, \ldots, g \ . \tag{3.8}$$

Then Equations (3.7), (3.8), (3.3) and (3.4) gives that for $1 \leq r \leq g$,

$$rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) \cdot (q^d + 1 + \sigma_d(a_1, \ldots, a_d)) = \beta_r(a_1, \ldots, a_r) = ra_r - \varphi_r(a_1, \ldots, a_{r-1}) \ ;$$

therefore

$$ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r \quad \text{for} \quad 1 \leq r \leq g \ . \tag{3.9}$$

As B_r being the number of places of degree r is a non-negative integer, Equation (3.9) gives the desired result.

□

As a consequence of Theorem 3.2.6 using the formulas for φ_r given in (3.5), we obtain (for all $g \geq 4$)

$$\begin{aligned}
&a_1 \geq -(q+1) \ , \\
&2a_2 \geq a_1^2 + a_1 - (q^2 - q) \ , \\
&3a_3 \geq -a_1^3 + a_1 + 3a_1 a_2 - (q^3 - q) \ , \\
&4a_4 \geq a_1^4 - a_1^2 - 4a_1^2 a_2 + 4a_1 a_3 + 2a_2^2 + 2a_2 - (q^4 - q^2) \ .
\end{aligned}$$

3.3. Function Fields with Prescribed Coefficients of $L(t)$

Now we consider the following question: For given m-tuple of integers $(a_1, a_2, \ldots, a_m)$ which satisfy the inequalities of Theorem 3.2.6; i.e., $ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$ for all $r = 1, \ldots, m$, and for given integer $g \geq m$ does there exist a function field $F/\mathbb{F}_q$ of genus $g(F) = g$ whose L-polynomial has the form

$$L(t) = 1 + a_1 t + \ldots + a_m t^m + \ldots ?$$

In this section we will show that the above question has an affirmative answer if g is sufficiently large with respect to m. Let $f(t), h(t)$ be polynomials in $\mathbb{Z}[t]$ with $f(t) = h(t) + t^m \cdot u(t)$ for some $u(t) \in \mathbb{Z}[t]$ and $m \in \mathbb{Z}_{\geq 0}$. Then we use the congruence notation $f(t) \equiv h(t) \mod t^m$. With this convention the main result can be stated as follows.

Theorem 3.3.7 *Let $a_1, \ldots, a_m$ be integers which satisfy the inequalities of Theorem (3.2.6), that is,*

$$ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$$

for all $r = 1, \ldots, m$. Then there is an integer $g_0 \geq m$ such that for all $g \geq g_0$, there exists a function field $F/\mathbb{F}_q$ whose L-polynomial satisfies the congruence

$$L(t) \equiv 1 + a_1 t + \ldots + a_m t^m \mod t^{m+1} .$$

We need the following lemma whose proof is given together with the proof of Theorem 3.3.7.

Lemma 3.3.8 *For any given integers $a_1, \ldots, a_{m-1}$ with $m \geq 1$*

$$\varphi_m(a_1, \ldots, a_{m-1}) \equiv 0 \mod m .$$

Proof of Theorem 3.3.7 and Lemma 3.3.8: By induction over m. For $m = 1$, Lemma 3.3.8 trivially holds. Note that, in case $m = 1$, $ma_m \geq \varphi_m(a_1, \ldots, a_{m-1})$ means that $a_1 \geq -(q+1)$. Set $b_1 := a_1 + (q+1) \geq 0$, then by Theorem 3.1.1 there is an integer $g_0 \geq 1$ such that for all $g \geq g_0$ there exists a function field $F/\mathbb{F}_q$ with

$$g(F) = g \ \text{ and } \ B_1(F) = b_1 .$$

Let $L^{(F)}(t) = 1 + a_1^{(F)} t + a_2^{(F)} t^2 + \ldots$ be the L-polynomial of F. Then by Equation (3.9)

$$a_1^{(F)} = \varphi_1 + B_1(F) = -(q+1) + b_1 = -(q+1) + a_1 + (q+1) = a_1 ,$$

which shows that $L^{(F)}(t) \equiv 1 + a_1 t \mod t^2$. Now assume that Theorem 3.3.7 and Lemma 3.3.8 hold for $m \geq 1$. First we prove Lemma 3.3.8 for $m+1$ as follows.
Let $a_1, \dots, a_m$ be given integers. Choose integers $d_1, \dots, d_m$ such that

$$a_r \equiv d_r \mod (m+1) \text{ and } rd_r \geq \varphi_r(d_1, \dots, d_{r-1}) \text{ for } 1 \leq r \leq m \ .$$

By the induction hypothesis there exists a function field $F^*/\mathbb{F}_q$ whose L-polynomial $L^{(F^*)}(t)$ satisfies

$$L^{(F^*)}(t) \equiv 1 + d_1 t + \ldots + d_m t^m \mod t^{m+1} \ .$$

By Equation (3.9) the coefficient d_{m+1} of t^{m+1} in $L^{(F^*)}(t)$ satisfies the following equality.

$$\varphi_{m+1}(d_1, \dots, d_m) = (m+1)d_{m+1} - (m+1)B_{m+1}(F^*)$$

In other words, $\varphi_{m+1}(d_1, \dots, d_m) \equiv 0 \mod (m+1)$, and we conclude that

$$\varphi_{m+1}(a_1, \dots, a_m) \equiv \varphi_{m+1}(d_1, \dots, d_m) \equiv 0 \mod (m+1) \ .$$

Then it remains to prove the induction step for Theorem 3.3.7. Now suppose that given $m+1$ integers $a_1, \dots, a_{m+1}$ satisfy the inequalities $ra_r \geq \varphi_r(a_1, \dots, a_{r-1})$ for $r = 1, \dots, m+1$. We have seen that $\varphi_r(a_1, \dots, a_{r-1}) \equiv 0 \mod r$ holds for $r = 1, \dots, m+1$; i.e.,

$$b_r := a_r - r^{-1}\varphi_r(a_1, \dots, a_{r-1})$$

are non-negative integers. By Theorem 3.1.1 there is an integer $g_0 \geq m+1$ such that for all integers $g \geq g_0$ there exists a function field $F/\mathbb{F}_q$ with $g(F) = g$ and $B_r(F) = b_r$ for $1 \leq r \leq m+1$. Then Equation (3.9) gives that the L-polynomial $L^{(F)}(t)$ of F satisfies the congruence

$$L^{(F)}(t) \equiv 1 + a_1 t + \ldots + a_{m+1} t^{m+1} \mod t^{m+2} \ .$$

□

CHAPTER 4

On Automorphism Groups of Plane Curves

In this chapter our aim is to prove the following result.

Theorem 4.0.1 *Let $\mathcal{X}$ be a projective, non-singular, algebraic plane curve of genus $g \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 2$. Let G be an automorphism group of $\mathcal{X}$. Then either*

- *$\mathcal{X}$ is birationally equivalent to the Hermitian curve $\mathcal{H}(n)$ for some $n = p^h$, or*
- *$|G| \leq 3(2g^2 + g)(\sqrt{8g+1} + 3)$.*

First we recall some facts and definitions and then give some preliminary results that we make use of in the proof of Theorem 4.0.1.

From now on $\mathbb{K}$ is an algebraically closed field of characteristic $p > 2$. For a finite subgroup G of $\mathrm{Aut}(\mathcal{X})$ let G^* denote the associated automorphism group of the function field $\mathbb{K}(\mathcal{X})$, namely $G^* = \{\phi^* \mid \phi \in G\}$, where $\alpha^* : \mathbb{K}(\mathcal{X}) \to \mathbb{K}(\mathcal{X})$ denotes the pull-back of α.

Let $\mathbb{K}(\mathcal{X})^{G^*}$ be the fixed field of G^* and $\mathcal{Y}$ be a non-singular model of $\mathbb{K}(\mathcal{X})^{G^*}$. Then there exists a covering $\pi_G : \mathcal{X} \to \mathcal{Y}$ of degree $|G|$ such that $\pi_G^*(\mathbb{K}(\mathcal{Y}))$ coincides with $\mathbb{K}(\mathcal{X})^{G^*}$; also, two points $P, Q \in \mathcal{X}$ belong to the same orbit under G if and only if $\pi_G(P) = \pi_G(Q)$. Occasionally, $\mathcal{Y}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$.

If P is a point of $\mathcal{X}$, then the stabilizer G_P of P in G is the subgroup of G consisting of all elements fixing P. The orbit of P under G

$$\mathcal{O}_G(P) = \{Q \mid Q = P^\alpha, \ \alpha \in G\}$$

is *long* if $|\mathcal{O}_G(P)| = |G|$; otherwise $\mathcal{O}_G(P)$ is *short*.

For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $G_P^{(i)}$ and defined to be

$$G_P^{(i)} = \{\alpha \mid \mathrm{ord}_P(\alpha^*(t) - t) \geq i+1, \alpha \in G_P\},$$

where t is a uniformizing element (local parameter) at P. Here $G_P^{(0)} = G_P$, and $G_P^{(1)}$ is the unique Sylow p-subgroup of G_P. Moreover, $G_P^{(1)}$ has a cyclic complement H in G_P, that is,

$$G_P = G_P^{(1)} \rtimes H \tag{4.1}$$

with a cyclic group H of order coprime with p and not greater than $4g+2$ (see Theorem 4.0.2(iv)). Moreover, for sufficiently large i, $G_P^{(i)}$ is trivial.

For any point P of $\mathcal{X}$, let

$$e_P = |G_P| \quad \text{and} \quad d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1) \ .$$

Then $d_P \geq e_P - 1$ and equality holds if and only if $\gcd(p, |G_P|) = 1$. Let g' be the genus of the quotient curve $\mathcal{X}/G$. Hurwitz's genus formula states that

$$2g - 2 = |G|(2g' - 2) + \sum_{P \in \mathcal{X}} d_P \ . \tag{4.2}$$

Assume that $G_P^{(1)}$ only ramifies at P. Then (4.2) applied to $G_P^{(1)}$ gives

$$2g - 2 = |G_P^{(1)}|(2\tilde{g} - 2) + 2(|G_P^{(1)}| - 1) + \sum_{i \geq 2} (|G_P^{(i)}| - 1), \tag{4.3}$$

where $\tilde{g}$ denotes the genus of the quotient curve $\mathcal{X}/G_P^{(1)}$.

The following theorem summarizes some of the known upper bounds on the size of G related to the action of G on the set of points of $\mathcal{X}$.

Theorem 4.0.2 *Let r be the number of short orbits of $\mathcal{X}$ under the action of G, and let g' be the genus of the quotient curve $\mathcal{X}/G$. Let $P_1, \ldots, P_r$ be representatives from each short orbit, and let $d'_i = d_{P_i}/e_{P_i}$ for $i = 1, \ldots, r$, so that*

$$2g - 2 = |G|(d'_1 + \ldots + d'_r + 2g' - 2) \geq |G|(d'_1 + \ldots + d'_r - 2). \tag{4.4}$$

Assume without loss of generality that $d'_i \leq d'_j$ for $i \leq j$.

(i) *If $g' > 0$, then $|G| \leq 4(g - 1)$* [16, Theorem 11.56].

(ii) $|G| \leq 84(g-1)$, *with exceptions occurring only in the following cases* [16, Theorem 11.116]*:*

- **(iia)** *$r = 1$ and the only short orbit is non-tame; here $|G| \leq 8g^3$;*
- **(iib)** *$r = 2$ and both short orbits are non-tame; here $|G| \leq 16g^2$;*
- **(iic)** *$r = 3$ with precisely one non-tame orbit; here $|G| \leq 24g^2$; or*
- **(iid)** *$r = 2$ and one short orbit is tame; one is non-tame.*

(iii) *If $r \geq 5$, then $|G| \leq 4(g - 1)$* [16, Theorem 11.56].

(iv) *If $G = G_P$ and p does not divide $|G|$, then $|G| \leq 4g+2$* [36]; see also [16, Theorem 11.60].

Upper bounds on the size of $G_P^{(1)}$ are provided by the following result due to Stichtenoth [36, 37].

Theorem 4.0.3 *Let $\mathcal{X}$ be a non-singular curve of genus $g > 1$ and let P be a point of $\mathcal{X}$. Let $\mathcal{X}_i$ be the quotient curve $\mathcal{X}/G_P^{(i)}$, and let g_i denote the genus of $\mathcal{X}_i$. Then one of the following holds:*

(i) *$g_1 > 0$ and $|G_P^{(1)}| \leq g$;*

(ii) *$g_1 = 0$, $G_P^{(1)}$ has a short orbit other than $\{P\}$, and $|G_P^{(1)}| \leq \frac{p}{p-1}g$; or*

(iii) *$g_1 = g_2 = 0$, $\{P\}$ is the unique short orbit of $G_P^{(1)}$, and $|G_P^{(1)}| \leq \frac{4|G_P^{(2)}|}{(|G_P^{(2)}|-1)^2}g^2$.*

4.1. Preliminary Results

From now on, $(x_0 : x_1 : x_2)$ are homogeneous coordinates for $PG(2, \mathbb{K})$, with $\mathbb{K}$ an algebraically closed field with positive characteristic $p > 2$. We also let $x = x_1/x_0$ and $y = x_2/x_0$ be the corresponding non-homogeneous coordinates. Also, $\mathcal{X}$ denotes a projective, non-singular, geometrically irreducible, plane algebraic curve defined over $\mathbb{K}$ by the equation $F(x_0, x_1, x_2) = 0$, where F is an irreducible polynomial of degree $d > 3$. Let $\mathbb{K}(\mathcal{X})$ be the function field of $\mathcal{X}$ and denote by $\bar{x}_1$ and $\bar{x}_2$ the rational functions associated to the non-homogeneous coordinates x and y, namely

$$\bar{x}_1 = \frac{x_1 + (F)}{x_0 + (F)}, \qquad \bar{x}_2 = \frac{x_2 + (F)}{x_0 + (F)} .$$

Let $g = (d-1)(d-2)/2$ be the genus of $\mathcal{X}$. Here and subsequently, G stands for an automorphism group of $\mathcal{X}$. By a result due to B. Segre [30] every $h \in G$ is the restriction of a projectivity of $PG(2, \mathbb{K})$ preserving $\mathcal{X}$. Therefore, G can be viewed as a subgroup of $PGL_3(\mathbb{K})$ fixing $\mathcal{X}$. For an element $h \in G$, we denote by h^* the pull-back of h, that is, the associated automorphism of the function field $\mathbb{K}(\mathcal{X})$.

For a point $P \in \mathcal{X}$, the order sequence of $\mathcal{X}$ at P is the strictly increasing sequence

$$j_0(P) = 0 < j_1(P) = 1 < j_2(P)$$

such that each $j_i(P)$ is the intersection number $I(P, \mathcal{X} \cap \ell_i)$ of $\mathcal{X}$ and some line ℓ_i at P, see [40]. For $i = 2$, such a line ℓ_2 is uniquely determined as the tangent line $T_P(\mathcal{X})$ to $\mathcal{X}$ at P.

For all but a finite number of points the order sequence are the same and the set of points of $\mathcal{X}$ for which the order sequence differs from the generic order sequence $(0, \epsilon_1, \epsilon_2)$ is denoted by W. Equivalently, W is the support of the ramification divisor $R^{\mathcal{D}}$ when $\mathcal{D}$ is the linear series cut out by the lines of $PG(2, \mathbb{K})$. Finally, we denote by ℓ_∞ the line with equation $x_0 = 0$.

Proposition 4.1.4 *Let P be a point of $\mathcal{X}$ such that $I(P, \mathcal{X} \cap T_P(\mathcal{X})) = j > 2$. Then the group $G_P^{(2)}$ consists of elations with axis $T_P(\mathcal{X})$ (for definition see Section 5.0.3). Furthermore assume that*

(i) *G is a p-group such that $\{P\}$ is the only short orbit of G;*

(ii) *$j = d$; and*

(iii) *$g(\mathcal{X}/G) = 0$.*

Then

$$|G_P^{(2)}| = d \quad or \quad |G_P^{(2)}| = d - 1.$$

Proof: Without loss of generality we assume that $P = (0 : 0 : 1)$ and $T_P(\mathcal{X}) = \ell_\infty$. Let $\varphi \in G_P^{(2)}$. Since φ is a p-element fixing P and ℓ_∞, by straightforward calculation, φ is of the form

$$\varphi = \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ c & a & 1 \end{pmatrix}$$

for some $a, b, c \in \mathbb{K}$. Note that $\bar{x}_1/\bar{x}_2$ is a local parameter of $\mathcal{X}$ at P. Also,

$$\varphi(1, \overline{x}_1, \overline{x}_2) = \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ c & a & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \overline{x}_1 \\ \overline{x}_2 \end{pmatrix} = \begin{pmatrix} 1 \\ b + \overline{x}_1 \\ c + a\overline{x}_1 + \overline{x}_2 \end{pmatrix}$$

and

$$\varphi^* \left(\frac{\overline{x}_1}{\overline{x}_2} \right) - \frac{\overline{x}_1}{\overline{x}_2} = \frac{b + \overline{x}_1}{c + a\overline{x}_1 + \overline{x}_2} - \frac{\overline{x}_1}{\overline{x}_2} = \frac{b\overline{x}_2 + \overline{x}_1\overline{x}_2 - c\overline{x}_1 - a\overline{x}_1^2 - \overline{x}_1\overline{x}_2}{\overline{x}_2(c + a\overline{x}_1 + \overline{x}_2)} = \frac{b\overline{x}_2 - c\overline{x}_1 - a\overline{x}_1^2}{\overline{x}_2(c + a\overline{x}_1 + \overline{x}_2)} .$$

Then $v_P(\overline{x}_1) = 1 - j$ and $v_P(\overline{x}_2) = -j$ implies that

$$v_P \left(\varphi^* \left(\frac{\overline{x}_1}{\overline{x}_2} \right) - \frac{\overline{x}_1}{\overline{x}_2} \right) = \begin{cases} 2(1-j) - [-j-j] = 2 & , \text{if } a \neq 0 \\ -j - [-j-j] = j & , \text{if } a = 0, b \neq 0 \\ 1 - j - [-j-j] = j + 1 & , \text{if } a = 0, b = 0 \ . \end{cases} \tag{4.5}$$

As $\varphi \in G_P^{(2)}$, $a = 0$; therefore this proves the first assertion. Now assume that G is a p-group and $\{P\}$ is an orbit, then

$$G = G_P = G_P^{(1)} \ . \tag{4.6}$$

Since $\{P\}$ is the only short orbit, by the Hurwitz genus formula and (4.6) we have the following equality.

$$(d-1)(d-2) = \sum_{i=2}^{\infty}(|G_P^{(i)}|-1) \tag{4.7}$$

Furthermore from (4.5) we obtain that

$$G_P^{(2)} = G_P^{(3)} = \ldots = G_P^{(d-1)} \quad \text{and} \quad G_P^{(i)} = \{id\} \text{ for every } i \geq d+1 \ .$$

Now we show that either $G_P^{(d)} = G_P^{(d-1)}$ or $G_P^{(d)} = \{id\}$. Suppose that $G_P^{(d)}$ is a non-trivial proper subgroup of $G_P^{(d-1)}$. Then there exist elements $\varphi_1 \in G_P^{(d-1)} \setminus G_P^{(d)}$ and $\varphi_2 \in G_P^{(d)} \setminus \{id\}$ and they are of the form

$$\varphi_1 = \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ c & 0 & 1 \end{pmatrix}, \varphi_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ c' & 0 & 1 \end{pmatrix} \qquad \text{for some } b, c, c' \in \mathbb{F}_q \text{ with } b \cdot c' \neq 0.$$

Both φ_1 and φ_2 are elations with axes ℓ_∞. The centers of φ_1 and φ_2 are $Q = (0 : b : c)$ and P, respectively. Since $\mathcal{X}$ is non-strange (see Defition 5.0.2), there exist lines ℓ_1 through Q and ℓ_2 through P such that ℓ_1 and ℓ_2 intersect $\mathcal{X}$ at d distinct points. Since elations fix every line through the center, for $i = 1, 2$, φ_i acts on the set $\mathcal{X} \setminus \{P\}$. Then for $i = 1, 2$, φ_i has order p implies that $p|d$ and $p|(d-1)$, which is impossible. Hence $G_P^{(d)} = G_P^{(d-1)}$ or $G_P^{(d)} = \{id\}$. Then by Equation (4.7) we have

$$|G_P^{(2)}| = \begin{cases} d-1 & , \text{if } G_P^{(d)} = G_P^{(d-1)} \\ d & , \text{if } G_P^{(d)} = \{id\} \ . \end{cases}$$

□

Lemma 4.1.5 *Let P be a point of $\mathcal{X}$. If the genus g' of the quotient curve $\mathcal{X}/G_P^{(1)}$ is positive, then*

$$|G_P| \leq 6g.$$

Proof: By (4.1), $G_P = G_P^{(1)} \rtimes H$, where H is a cyclic group H of order coprime to p and not greater than $4g+2$. Then H is isomorphic to the automorphism group of $\mathcal{X}/G_P^{(1)}$ fixing the point lying under P. As $g' \geq 1$, the size of H is at most $4g'+2$ by Theorem 4.0.2. Also, by (4.2) for $G_P^{(1)}$ we have $|G_P^{(1)}| \leq g/g'$. Then

$$|G_P| = |G_P^{(1)}||H| \leq \frac{g}{g'}(4g'+2) \leq 4g + 2\frac{g}{g'} \leq 6g \ .$$

□

Lemma 4.1.6 *Let P be a point of W. If $|G_P| \leq 6g$, then $|G| \leq (12g^2+6g)d$.*

Proof: As $\mathcal{X}$ is non-singular $\epsilon_1 = 1$ and $\epsilon_2 < d$. The size of W can be at most degree of the Ramification divisor, so by Theorem 5.0.26

$$|W| \leq (2g-2)d + 3d\ .$$

Furthermore automorphisms of $\mathcal{X}$ act on the set W. Then the orbit stabilizer theorem implies that

$$|G| \leq |G_P||W| \leq 6g(2g+1)d\ .$$

□

Lemma 4.1.7 *Let P be a point of W. Suppose that for some $\varphi \in G_P^{(1)} \setminus \{id\}$, there exists $Q \in W \setminus \{P\}$ with $\alpha(Q) = Q$. Let Δ be an orbit under G_P other than $\{P\}$ and $\mathcal{O}_{G_P}(Q)$.*

(i) *If Δ is a long or tame short orbit, then $|G_P| \leq (2g-2) + |\Delta|$.*

(ii) *If Δ is a non-tame short orbit, then $|G_P| \leq 2g-2$.*

Proof: (i) If Δ is a long orbit, then $|G_P| = |\Delta|$. Assume then that Δ is a short orbit. Then we have at least three short orbits under G_P, two of which are non-tame. Let R be a point of Δ, then by (4.4) for G_P, we have

$$2g-2 \geq |G_P|\Big(\frac{|G_{P,R}|-1}{|G_{P,R}|}\Big)\ .$$

Also $|G_{P,R}| = |G_P|/|\Delta|$ gives

$$|G_P|\Big(\frac{|G_{P,R}|-1}{|G_{P,R}|}\Big) = |G_P| - |\Delta|\ .$$

Then we obtain the desired result.

(ii) In this case there are three different non-tame orbits under G_P. Hence the assertion then follows from (4.4) for G_P. □

Lemma 4.1.8 *Assume that $G_P^{(1)}$ is non-trivial. If G_P has at least three short tame orbits, then $|G_P| \leq 4(g-1)$.*

Proof: Let g' be the genus of the quotient curve $\mathcal{X}/G_P$ and r be the number of short orbits. Note that with the assumption that $G_P^{(1)} \neq \{id\}$, there exists at least one non-tame orbit of G_P, so $r \geq 4$. If $g' > 0$ or $r \geq 5$, then the assertion easily comes from (4.4). Assume that $g' = 0$ and $r = 4$, then (4.4) gives

$$2g-2 = |G_P|(d_1' + d_2' + d_3' + d_4' - 2)\ ,$$

where $d_4' \geq 1$ and $d_1' + d_2' + d_3' \geq 3/2$. This proves the assertion. □

Lemma 4.1.9 *Assume that $G_P^{(1)}$ is non-trivial, and that G_P has precisely 2 short tame orbits on $\mathcal{X}$, say Δ_1 and Δ_2, with $|\Delta_1| \geq |\Delta_2|$. Then $|G_P| \leq \max\{6(g-1), 2|\Delta_1|\}$.*

Proof: As in Theorem 4.1.8 we can assume that the genus of the quotient curve $\mathcal{X}/G_P$ is equal to 0. Then by (4.4) for G_P, we have

$$2g-2=|G_P|(d_1'+d_2'+d_3'-2)\ ,$$

with $d_3'\geq 1$ and $d_2'\geq d_1'\geq 1/2$. If $d_1'=1/2$, then $G_P=2|\Delta_1|$ as Δ_1 is a tame orbit. If $d_1'\geq 2/3$, then $d_1'+d_2'+d_3'\geq 7/3$. Hence $|G_P|\leq 6(g-1)$. □

In the rest, we consider the following cases:

(C1) W is the only non-tame orbit of G;

(C2) the size of W is greater than 1;

(C3) every p-element of G fixes precisely one point of W; and

(C4) for each point P in W, the size of $G_P^{(2)}$ is equal to $d-1$.

Lemma 4.1.10 *Assume that both conditions* (C1) *and* (C3) *hold. Then each Sylow p-subgroup of G coincides with $G_R^{(1)}$ for some point R in W. In particular, any two distinct Sylow p-subgroups of G intersect trivially.*

Proof: Let S be a p-Sylow subgroup of G. Since S is a p-group, it has a non-trivial center. Let h be a central element in S of order p. Then by (C3) there exists $R\in W$ such that $h(R)=R$. Then for any $s\in S$

$$s(R)=sh(R)=hs(R)\ .$$

The above equation means that h fixes both R and $s(R)$. Hence by (C3), $s(R)=R$ and therefore $s\in G_R$. This proves that $S=G_R^{(1)}$. □

Lemma 4.1.11 *Assume that both conditions* (C1) *and* (C3) *hold. Then the normalizer of $G_P^{(1)}$ in G, $N_G(G_P^{(1)})$, is equal to G_P.*

Proof: As $G_P^{(1)}$ is a normal subgroup of G_P, we only need to show that if $s\in G$ such that $sG_P^{(1)}s^{-1}\subseteq G_P^{(1)}$ then $s\in G_P$. $sG_P^{(1)}s^{-1}\subseteq G_P^{(1)}$ implies that $sh=h's$ for some $h,h'\in G_P^{(1)}$. Hence

$$s(P)=sh(P)=h's(P)\ .$$

Then h' fixes both P and $s(P)$. By (C3), $s(P)=P$; therefore $s\in G_P$. □

Lemma 4.1.12 *Assume that conditions* (C1), (C2), (C3) *and* (C4) *hold. Furthermore assume that*

(i) $|W|>d$,

(ii) $G_P^{(1)}$ *is not cyclic,*

(iii) *$I(P, \mathcal{X} \cap T_P(\mathcal{X})) = d$, and*

(vi) *the genus of $\mathcal{X}/G_P^{(1)}$ is equal to* 0.

Then the following hold:

(i) *W contains 4 points, no three of which are collinear.*

(ii) *G satisfies all the assumptions of Theorem 5.0.29 with $M = \{id\}$; in particular, G acts 2-transitively on W.*

(iii) *Either $G_P^{(1)}$ is abelian, or $C(G_P^{(1)})$, the center of $G_P^{(1)}$, is $G_P^{(2)}$.*

Proof:

(i) (C2) implies that there exists an element $R \in W \setminus \{P\}$. Let ℓ be the line passing through P and R. By (C4), i.e. $|G_P^{(2)}| = d - 1$, in Proposition 4.1.4 (in the case $G = G_P$) we have seen that $G_P^{(2)}$ consists of elations with center P. Therefore, $G_P^{(2)}$ acts on $\mathcal{X} \cap \ell$, implying that $\mathcal{O}_{G_P^{(2)}}(R) \subseteq \mathcal{X} \cap \ell$. Then by (C3) and order of $G_P^{(2)}$, we have

$$\mathcal{X} \cap \ell = (\mathcal{O}_{G_P^{(2)}}(R)) \cup \{P\} .$$

As $|W| > d$, there exists a point R' of W not on ℓ. Then, by similar arguments, the line through R' and P contains d points of W, and this proves the assertion.

(ii) By Lemma 4.1.10, a Sylow p-subgroup S of G coincides with $G_P^{(1)}$ for some point P in W. Conditions (C2) and (C3) show that S is a proper subgroup of G. Also by our assumption S is not a cyclic group. Lemma 4.1.11 implies that the normalizer of S in G is G_P, which is isomorphic to a semidirect product of $S = G_P^{(1)}$ by a cyclic group H. Furthermore by Lemma 4.1.10, for each $h \in G \setminus G_P$ we have that $h^{-1}Sh = G_R^{(1)}$ for some $R \in W \setminus \{P\}$, and hence the intersection of S and $h^{-1}Sh$ is trivial.

It remains to show that the center of G_P is trivial. Let h be a central element in G_P, and let $Q \in W \setminus \{P\}$. Since W is an orbit under G, there exists an element $m \in G$ be such that $m(P) = Q$. By Theorem 5.0.29, $C(G_P)$ is a normal subgroup of G. Then for some $h' \in C(G_P)$ we have

$$h(Q) = hm(P) = mh'(P) = m(P) = Q .$$

Therefore h fixes each point in W, and the claim follows by (i).

(iii) As in the proof of Proposition 4.1.4, without loss of generality, we assume that $P = (0 : 0 : 1)$ and that $T_P(\mathcal{X}) = \ell_\infty$. First we prove that $G_P^{(2)} \subseteq C(G_P^{(1)})$, that is, for any $A \in G_P^{(2)}$ and for any $B \in G_P^{(1)}$,

$$ABA^{-1}B^{-1} = id \tag{4.8}$$

holds. For convenience denote by $M_{a,b,c}$ the lower triangular matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ c & a & 1 \end{pmatrix}, \quad \text{for } a,b,c \in \mathbb{K} .$$

It has been noticed in the proof of Proposition 4.1.4 that $A = M_{0,b',c'}$ and that $B = M_{a,b,c}$ for some $a,b,c,b',c' \in \mathbb{K}$. Also, (C4) implies that $b' = 0$. Then straightforward calculations shows that (4.8) follows.

Suppose now that there exists $C \in C(G_P^{(1)}) \setminus G_P^{(2)}$. Then $C = M_{a_1,b_1,c_1}$ with $a_1 \neq 0$; otherwise C lies in $G_P^{(2)}$. By straightforward computation

$$CM_{a,b,c}C^{-1}M_{a,b,c}^{-1} = M_{0,0,a_1b-ab_1} . \tag{4.9}$$

Then $CM_{a,b,c}C^{-1}M_{a,b,c}^{-1} = id$ implies that $ab_1 = a_1b$. Set $\lambda := \frac{b_1}{a_1}$, and then

$$G_P^{(1)} \leq \{M_{a,\lambda\cdot a,c} \mid a,c \in \mathbb{K}\} .$$

The above explanation proves that $G_P^{(1)}$ is abelian. □

4.2. The Proof of Theorem 4.0.1

We keep the notation of previous section. In particular, $\mathcal{X}$ denotes a projective, non-singular, geometrically irreducible, algebraic curve defined over $\mathbb{K}$ by the equation $F(x_0,x_1,x_2) = 0$, where F is an irreducible polynomial of degree $d > 3$, and the genus of $\mathcal{X}$ is $g = (d-1)(d-2)/2 > 2$. Here $\mathbb{K}$ is an algebraically closed field with characteristic $p > 2$.

The proof of Theorem 4.0.1 depends on Hilbert's ramification theory. A key result of independent interest valid for any non-singular plane curve $\mathcal{X}$ is that the higher ramification groups of G at any inflection point have a faithful action in the projective plane as elation groups preserving $\mathcal{X}$. This gives heavy restrictions on the possible structure of the higher ramification groups, and hence it allows us to obtain useful information on the p-subgrups of the one-point stabilizer of G. In the proof also the Stöhr-Voloch theory on Weierstrass points with respect to a base-point-free linear series [40] and some deeper results on finite groups, such as the Kantor-O'Nan-Seitz theorem are used.

From now on, we assume that $\mathcal{X}$ is not birationally equivalent to a Hermitian curve. We are going to prove that if G is an automorphism group of $\mathcal{X}$, then

$$|G| < (12g^2 + 6g)d . \tag{4.10}$$

As $g=(d-1)(d-2)/2$, (4.10) implies Theorem 4.0.1. The proof is divided into several steps according to cases (C1), (C2), (C3), and (C4).

Lemma 4.2.13 *If G has more than one non-tame orbit, then* (4.10) *holds.*

Proof: The assertion follows from Theorem 4.0.2. □

Lemma 4.2.14 *If either W is a long orbit, or W contains a short tame orbit under the action of G, then* (4.10) *holds.*

Proof: The stabilizer G_P of a point $P \in W$ has size at most $4g+2$. Then the claim follows from Lemma 4.1.6. □

By Lemmas 4.2.13 and 4.2.14, from now on we assume that **the condition (C1) holds**.

Lemma 4.2.15 *If $W = \{P\}$, then* (4.10) *holds.*

Proof: By Lemmas 4.1.5 and 4.1.6 we may assume that the genus g' of the quotient curve $\mathcal{X}/G_P^{(1)}$ is equal to 0. Note that $W=\{P\}$ implies $G=G_P$.
If $j_2(P)<d$, then there exists an element $R \in (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$. Since every element of G fixes P, G acts on $(T_P(\mathcal{X}) \cap \mathcal{X})$; therefore $\mathcal{O}_G(R)$ is contained in $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$. As a result, $|\mathcal{O}_G(R)|<d$. As $R \notin W$, $\mathcal{O}_G(R)$ is either a long or a short tame orbit, whence $|G_R| \le 4g+2$. Then by the orbit stabilizer theorem we obtain

$$|G| = |G_R||\mathcal{O}_G(R)| < (4g+2)d < 3g^2 d \ .$$

If on the contrary $j_2(P)=d$, then Proposition 4.1.4 applies to $G_P^{(1)}$. Therefore, either $|G_P^{(2)}|=d$ or $|G_P^{(2)}|=d-1$. By Theorem 4.0.3,

$$|G_P^{(1)}| \le \frac{4|G_P^{(2)}|}{(|G_P^{(2)}|-1)^2} g^2$$

holds. By the fact that $g=\frac{(d-1)(d-2)}{2}$, we obtain the following inequalities.
For $|G_P^{(2)}|=d$

$$|G_P^{(1)}| \le \frac{4d}{(d-1)^2} g^2 = 2\frac{d-2}{d-1} dg < 2dg \ ;$$

and for $|G_P^{(2)}|=d-1$

$$|G_P^{(1)}| \le \frac{4(d-1)}{(d-2)^2} g^2 = 2\frac{d-1}{d-2}(d-1)g < 3dg \ .$$

Then from (4.1) together with $G=G_P$ we have

$$|G| < 3dg(4g+2) < 15dg^2 \ .$$

□

As a corollary, from now on we assume that **the condition (C2) holds** as well. For any points $P, Q \in W$, $j_2(P) = j_2(Q)$ as W is an orbit under G. Hence for simplicity in the rest of the proof for any point $P \in W$ the value $j_2(P)$ is denoted by j_2.

In Lemmas 4.2.16, 4.2.17 and 4.2.18 we deal with the case where condition (C3) does not hold. In other words, we assume that there exists a p-element in G fixing at least two distinct points of W.

Lemma 4.2.16 *Let P and Q be two distinct points of W such that $G_P^{(1)} \cap G_Q^{(1)}$ is not trivial. Then $j_2 < d$.*

Proof: As in the proof of Proposition 4.1.4, without loss of generality, we assume that $P = (0 : 0 : 1)$ and that $T_P(\mathcal{X}) = \ell_\infty$. Let $\alpha := M_{a,b,c}$ be a non-trivial element in $G_P^{(1)} \cap G_Q^{(1)}$. Assume that $j_2 = d$. Therefore, $T_P(\mathcal{X})$ and $T_Q(\mathcal{X})$ are distinct lines both fixed by α. Then α fixes the the point $R := T_P(\mathcal{X}) \cap T_Q(\mathcal{X})$. Let $R = (0 : r_1 : r_2)$, then $\alpha(R) = (0 : r_1 : ar_1 + r_2)$. As a result, $a = 0$; i.e. $\alpha = M_{0,b,c}$. On the other hand, for $Q = (q_0 : q_1 : q_2)$ with $q_0 \neq 0$, $\alpha(Q) = (q_0 : q_1 + bq_0 : q_2 + cq_0)$. This gives that $b = c = 0$; whence α must be identity element. However this is impossible as α is assumed to be non-trivial. □

By Lemma 4.2.16, $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ is a non-empty set. In Lemmas 4.2.17 and 4.2.18 we investigate the orbit of an element in this set.

Lemma 4.2.17 *Suppose that P and Q are distinct points of W such that $G_P^{(1)} \cap G_Q^{(1)}$ is not trivial. If there exists $R \in (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ such that $\Delta := \mathcal{O}_{G_P}(R)$ is either a long or a short tame orbit, then* (4.10) *holds.*

Proof: Since G_P fixes $T_P(\mathcal{X})$, we have that $\Delta \subseteq (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$. Therefore, $|\Delta| \leq d - j_2$. By Lemma 4.1.7(i),

$$|G_P| \leq 2g - 2 + |\Delta| \leq 2g - 2 + d - j_2 < 2g + d \ .$$

Then (4.10) follows from Lemma 4.1.6. □

Lemma 4.2.18 *Suppose that P and Q are distinct points of W such that $G_P^{(1)} \cap G_Q^{(1)}$ is not trivial. If for each $R \in (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ the orbit $\Delta := \mathcal{O}_{G_P}(R)$ is non-tame, then* (4.10) *holds.*

Proof: By Lemma 4.2.16 we have $j_2 < d$. Also, by (C1); i.e. W is the only non-tame orbit of G, $(T_P(\mathcal{X}) \cap \mathcal{X}) \subset W$.
If $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ is not an orbit under G_P, then G_P has at least 3 non-tame orbits, and $|G_P| \leq 2g - 2$ holds by (4.4); then (4.10) follows from Lemma 4.1.6. Therefore, we may assume that $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ is an orbit under G_P. Write $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\} = \{R_1, \ldots, R_h\}$.

First assume that there exists $i_0 \in \{1, \ldots, h\}$ such that $T_{R_{i_0}}(\mathcal{X}) \neq T_P(\mathcal{X})$. $j_2 < d$ implies that there exists a point $S \in (T_{R_{i_0}}(\mathcal{X}) \cap \mathcal{X}) \setminus \{R_{i_0}\}$. As $\{R_1, \ldots, R_h\}$ is an orbit under G_P, for any $i \in \{1,\dots,h\}$ there exists an element $g_i \in G_P$ such that $g_i(R_{i_0}) = R_i$. Then $g_i(S) \in T_{R_i}(\mathcal{X}) \cap \mathcal{X}$ but $g_i(S) \notin T_P(\mathcal{X})$; therefore $T_{R_i}(\mathcal{X}) \neq T_P(\mathcal{X})$ holds for all $i = 1,\dots,h$. Let $\Delta' := \mathcal{O}_{G_P}(S)$. Then $\Delta' \subseteq \cup_{i=1}^{h}(T_{R_i}(\mathcal{X}) \cap \mathcal{X}) \setminus \{R_i\}$, and therefore

$$|\Delta'| \leq (d-j_2)^2 \leq (d-3)^2 < 2g \ .$$

The second inequality comes from $j_2 > 3$. Without loss of generality we can assume that Δ' is a tame orbit under G_P; otherwise G_P would have 3 non-tame orbits. Hence, $|G_P| < 4g$ by Lemma 4.1.7(i). Then (4.10) follows from Lemma 4.1.6.

Therefore, we may assume that $T_{R_i}(\mathcal{X}) = T_P(\mathcal{X})$ for all $i = 1,\dots,h$. We are going to prove that the size of $G_P^{(2)}$ is at most d. Since $j_2 > 2$, in the proof of Proposition 4.1.4 we have seen that the group $G_P^{(2)}$ coincides with the group of elations with axis $T_P(\mathcal{X})$ fixing $\mathcal{X}$ and that

$$G_P^{(2)} = \cdots = G_P^{(j_2-1)} \ .$$

Write $R_i = (0 : a : b)$ with $a \neq 0$, then $\frac{b\bar{x}_1 - a\bar{x}_2}{\bar{x}_1}$ is a local parameter of $\mathcal{X}$ at R_i. The same calculations as in Proposition 4.1.4 give $G_P^{(2)} \subseteq G_{R_i}^{(k)}$ for $k = 2,\dots,j_2-1$. This implies that

$$G_P^{(2)} = G_{R_i}^{(2)} = \cdots = G_{R_i}^{(j_2-1)}$$

for all $i = 1,\dots,h$. Then, by the Hurwitz genus formula for $G_P^{(2)}$, we have

$$2g-2 \geq |G_P^{(2)}|(2g'-2) + (h+1)\left(\sum_{i=0}^{j_2-1}(|G_P^{(2)}|-1)\right) \ ,$$

where g' is the genus of the quotient curve $\mathcal{X}/G_P^{(2)}$. Therefore,

$$2g-2 \geq |G_P^{(2)}|(2g'-2) + \frac{d}{j_2}j_2(|G_P^{(2)}|-1) = |G_P^{(2)}|(2g'-2+d) - d \ ,$$

and hence

$$|G_P^{(2)}| \leq \frac{2g+d-2}{d-2} = d \ . \tag{4.11}$$

Now we distinguish a number of cases according to the generic order sequence $(0,1,\epsilon_2)$ of $\mathcal{X}$ and the order sequence $(0,1,j_2)$ at P.

(i) $\boldsymbol{\epsilon_2 = 2}$. Suppose there exists $S \in W \setminus T_P(\mathcal{X})$. Let $\Delta' := \mathcal{O}_{G_P}(S)$. Since $\mathcal{X}$ is classical and Δ' is contained in $W \setminus (T_P(\mathcal{X}) \cap \mathcal{X})$, we have

$$|\Delta'| \leq \deg R^{\mathcal{D}} - |T_P(\mathcal{X}) \cap \mathcal{X}| = 6g-6+3d-(h+1) \leq 6g-8+3d \ .$$

Then, by Lemma 4.1.7, $|G_P| \leq 8g-10+3d$ holds. Therefore

$$|G| = |G_P||W| \leq (8g-10+3d)(6g-6+3d) \ .$$

Then (4.10) follows from $d \geq 6$, which holds as $T_P(\mathcal{X})$ contains at least two points of W.

Now we can assume that W coincides with $T_P(\mathcal{X})\cap\mathcal{X}$. Then clearly $|W| = \frac{d}{j_2}$ holds. Note that the stabilizer of R_1 in $G_P^{(1)}$ coincides with $G_P^{(2)}$. Then by the orbit-stabilizer theorem $|G_P^{(1)}| \leq h|G_P^{(2)}|$ holds. Therefore, taking into account (4.4) and (4.11), we obtain

$$|G| = |G_P||W| \leq hd(4g+2)\frac{d}{j_2} < d(4g+2)\left(\frac{d}{j_2}\right)^2 < d(4g+2)g < 5dg^2 \ .$$

(ii) $\boldsymbol{\epsilon_2 > 2}$. Let $\mathcal{D}_0$ be the base-point-free linear series cut out on $\mathcal{X}$ by the lines through P. Denote by W_0 and $R^{\mathcal{D}_0}$ the set of Weierstrass points and the ramification divisor of $\mathcal{D}_0$, respectively. Then the following hold:

(i) The $(\mathcal{D}_0, P)$-order sequence is $(0, j_2 - 1)$.

(ii) For a point $Q \neq P$ the $(\mathcal{D}_0, Q)$-order sequence is $(0, I(P, \mathcal{X} \cap \ell_{P,Q}))$, where $\ell_{P,Q}$ is the line joining P and Q.

(iii) The $\mathcal{D}_0$-order sequence of $\mathcal{X}$ is $(0, 1)$ as $\mathcal{X}$ is non-strange.

(vi) The degree of the ramification divisor $R^{\mathcal{D}_0}$ is

$$\deg(R^{\mathcal{D}_0}) = 2g - 2 + 2(d-1) \ . \tag{4.12}$$

Note that each point in $T_P(\mathcal{X}) \cap \mathcal{X}$ is a point of W_0. Assume that there exists $S \in W_0 \setminus (T_P(\mathcal{X}) \cap \mathcal{X})$, and let $\Delta' := \mathcal{O}_{G_P}(S)$. Then Δ' is an orbit in W_0 disjoint from $\{P\}$ and $\mathcal{O}_{G_P}(R_1) = (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$, which are are non-tame orbits under G_P. Hence by Lemma 4.1.7 we obtain

$$|G_P| \leq 2g - 2 + |\Delta'| < 2g - 2 + |W_0| \leq 2g - 2 + \deg(R^{\mathcal{D}_0}) < 4g + 2d \ .$$

Then (4.10) follows from Lemma 4.1.6. Therefore, we can assume that

$$W_0 = T_P(\mathcal{X}) \cap \mathcal{X} \ . \tag{4.13}$$

In particular, (4.13) means that any line passing through the point P other than the line $T_P(\mathcal{X})$ cannot be tangent at any point of $\mathcal{X}$.

(iia) $\mathbf{p \nmid (j_2 - 1)}$. As $\mathcal{X}$ is non-classical, by Theorem 5.0.25 $p \mid (d-1)$ holds. Therefore, $p \nmid j_2$; otherwise $p \mid d$ as $d = (h+1)j_2$. Then Theorem 5.0.26(ii) implies that $v_P(R^{\mathcal{D}_0}) = j_2 - 2$, whereas $v_{R_i}(R^{\mathcal{D}_0}) = j_2 - 1$ for each $i = 1, \ldots, h$. Therefore, by (4.13) we have

$$\deg(R^{\mathcal{D}_0}) = (j_2 - 2) + h(j_2 - 1) = d - h - 2 \ ;$$

but this contradicts (4.12).

(iib) $\mathbf{p} \mid (\mathbf{j_2}-\mathbf{1})$. Note that $h > 1$; otherwise $d = 2j_2$ and p divides both $2j_2 - 1$ and $j_2 - 1$. We now prove that

$$G_{P,R_1,R_2} \subseteq G_P^{(2)} \ . \tag{4.14}$$

Let α be a non-trivial element in G_{P,R_1,R_2}. As α fixes the line $T_P(\mathcal{X})$ pointwise, α is a central collineation with axis $T_P(\mathcal{X})$. Denote by C the center of α. Suppose that the center C does not lie on $T_P(\mathcal{X})$. Let $\ell_1 = \ell_{P,C}$ be the line joining P and C, and let ℓ_2 be a line through C such that ℓ_2 is not tangent to $\mathcal{X}$ at any point and the intersection point of ℓ_2 and $T_P(\mathcal{X})$ does not belong to $\mathcal{X}$. Note that since $W_0 \subseteq T_P(\mathcal{X})$, for $i = 1, 2$, $I(Q, \mathcal{X} \cap \ell_i) = 1$ for all $Q \in \mathcal{X} \cap \ell_i$. Furthermore, α cannot fix any point on $\ell_1 \cup \ell_2$ other than P and C. If $C \notin \mathcal{X}$, then α acts semiregularly on both $(\ell_1 \cap \mathcal{X}) \setminus \{P\}$ and $\ell_2 \cap \mathcal{X}$. This is impossible as the former set has size $d-1$, whereas the latter has size d. Similarly, if $C \in \mathcal{X}$, then α acts semiregularly both on a set of size $d-2$, namely $(\ell_1 \cap \mathcal{X}) \setminus \{P, C\}$, and on a set of size $d-1$, that is $(\ell_2 \cap \mathcal{X}) \setminus \{C\}$. This contradiction shows that α must be an elation with axis $T_P(\mathcal{X})$. By Proposition 4.1.4, α lies in $G_P^{(2)}$, proving that G_{P,R_1,R_2} is contained in $G_P^{(2)}$.

By taking into account of (4.14) we obtain

$$|G| = |W||G_P| \leq |W||G_{P,R_1}|h \leq |W||G_{P,R_1,R_2}|(h-1)h < |W||G_P^{(2)}|h^2 \ .$$

Then by (4.11) we have the following inequalities.

$$\begin{aligned} |G| &< [(1+\epsilon_2)(2g-2)+3d]\frac{2g+d-2}{d-2}\left(\frac{d}{j_2}\right)^2 \\ &< [(1+\epsilon_2)(2g-2+d)]\frac{2g+d-2}{d-2}\left(\frac{d}{j_2}\right)^2 \\ &< d(2g+d-2)^2 \\ &= 4dg^2+6dg+8g^2-10g-d+2 \ . \end{aligned}$$

In the third inequality we have used both $\frac{1+\epsilon_2}{j_2} \leq 1$ and $\frac{d}{(d-2)j_2} \leq 1$. As a result,

$$|G| < 4dg^2 + 6dg + 8g^2 \leq 8dg^2 \ .$$

□

As a consequence of Lemmas 4.2.17 and 4.2.18, from now on we assume that **the condition (C3) holds**. In other words, we assume that every p-element of G fixes precisely one point of W.

Lemma 4.2.19 *If $j_2 < d$, then* (4.10) *holds.*

Proof: Let $T_P(\mathcal{X}) \cap \mathcal{X} \setminus \{P\} = \{R_1, \ldots, R_h\}$. By condition (C3), $G_P^{(1)}$ acts semiregularly on $T_P(\mathcal{X}) \cap \mathcal{X} \setminus \{P\}$. Then $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ consists of either long or short tame orbits under G_P, and the order of $G_P^{(1)}$ divides h. Furthermore, in Proposition

4.1.4 we have seen that an element of $G_P^{(2)}$ fixes $T_P(\mathcal{X})$ pointwise; therefore $G_P^{(2)}$ must be trivial.

If $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ contains a long orbit of G_P, then $|G_P| < d$ and the claim follows from Lemma 4.1.6. Hence we can assume that $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ consists of short tame orbits. Now we distinguish three cases.

(i) $(\mathbf{T_P}(\mathcal{X}) \cap \mathcal{X}) \setminus \{\mathbf{P}\}$ **is the only short tame orbit of** $\mathbf{G_P}$. Let g' be the genus of $\mathcal{X}/G_P$. Then, by the Hurwitz genus formula

$$2g - 2 = |G_P|(2g' - 2) + (|G_P| - 1) + (|G_P^{(1)}| - 1) + h(|G_{P,R_1}| - 1) \ .$$

Since $h|G_{P,R_1}| = |G_P|$, we have

$$2g = 2g'|G_P| + |G_P^{(1)}| - h \ .$$

From the facts that $g > 2$ and $|G_P^{(1)}| \leq h$, the genus g' must be a positive integer. Then $2g \geq 2|G_P| - d$, implying that $|G_P| \leq g + \frac{d}{2}$. Then (4.10) follows from Lemma 4.1.6.

(ii) $(\mathbf{T_P}(\mathcal{X}) \cap \mathcal{X}) \setminus \{\mathbf{P}\}$ **is one of the** $\mathbf{s > 2}$ **short tame orbits of** $\mathbf{G_P}$. By Lemma 4.1.6, it is enough to prove that $|G_P| \leq 6(g-1)$. If $s \geq 3$, by Lemma 4.1.8 we have $|G_P| \leq 4(g-1)$. Hence we assume that $s = 2$. Let Δ_1 be the short tame orbit of G_P different from $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$. If Δ_1 has size less than d, then the assertion follows from Lemma 4.1.9. Therefore we can assume that $|\Delta_1| \geq d$. Arguing as in Lemma 4.1.9, we have

$$2g - 2 = |G_P|(d_1' + d_2' + d_3' - 2) \ ,$$

with $d_3' \geq 1$ and $d_2' \geq d_1' \geq 1/2$. If $d_1' \geq 2/3$ then $d_1' + d_2' + d_3' \geq 7/3$; so $|G_P| \leq 6(g-1)$. From now on we may assume $d_1' = 1/2$. Note that $d_2' = (|G_{P,R_1}| - 1)/|G_{P,R_1}|$. Therefore

$$2g - 2 \geq |G_P|\Big(\frac{|G_{P,R_1}| - 1}{|G_{P,R_1}|} - \frac{1}{2}\Big) \ . \tag{4.15}$$

If $|G_{P,R_1}| < 6$, then $|G_P| \leq 6(d-1) < 6(g-1)$; if $|G_{P,R_1}| \geq 6$, the same inequality follows from (4.15).

(iii) $\mathbf{G_P}$ **acts with at least 2 short orbits on** $(\mathbf{T_P}(\mathcal{X}) \cap \mathcal{X}) \setminus \{\mathbf{P}\}$. Clearly, the size of a short orbit of G_P contained in $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ is less than $d-1$. Then by Lemmas 4.1.8 and 4.1.9 it follows that $|G_P| \leq 6(g-1)$. By Lemma 4.1.6, (4.10) holds. □

Lemma 4.2.20 *If* $j_2 = d$*, then* (4.10) *holds.*

Proof: By (4.4), $G_P = G_P^{(1)} \ltimes H$, where H is a cyclic group of order prime to p. We consider the quotient curve $\mathcal{X}/G_P^{(1)}$. Let g' be the genus of $\mathcal{X}/G_P^{(1)}$. By Lemmas 4.1.5 and 4.1.6, $g' = 0$ can be assumed. Furthermore, by Proposition 4.1.4 either $|G_P^{(2)}| = d$ or $|G_P^{(2)}| = d - 1$. A number of cases will be considered.

(i) $\mathbf{G_P^{(1)}}$ **is cyclic**. As in the proof of Proposition 4.1.4, without loss of generality, we assume that $P = (0:0:1)$ and that $T_P(\mathcal{X}) = \ell_\infty$. Then a generator α of $G_P^{(1)}$ is equal to $M_{a,b,c}$ for some $a, b, c \in \mathbb{K}$. As $p > 2$, by straightforward computation we have

$$\alpha^p = M_{pa,pb,p\frac{p-1}{2}ab+pc} = id \ .$$

Therefore, $|G_P^{(1)}| = p$ holds. Since $G_P^{(2)}$ is non-trivial, $G_P^{(2)} = G_P^{(1)}$.

Assume that $\mathcal{X}$ is non-classical. Then $p \mid (d-1)$ by Theorem 5.0.25; therefore $|G_P^{(2)}| = p = d-1$ holds. By Theorem 5.0.26(iv), $\epsilon_2 = p$. Then this contradicts Theorem 5.0.28 as $\mathcal{X}$ is assumed not to be projectively equivalent to a Hermitian curve.

Then $\mathcal{X}$ is classical. By Theorem 5.0.26(iii),

$$|W| \leq \frac{6g-6+3d}{d-2} = 3d \ .$$

$G_P^{(2)} = G_P^{(1)}$ gives that $|G_P^{(1)}| \leq d$. Hence by the orbit stabilizer theorem we obtain

$$|G| = |G_P^{(1)}||H||W| \leq d(4g+2)3d \ .$$

If $d > 4$, then (4.10) holds. If $d = 4$, then $p = d$ cannot occur; hence, $|G_P^{(1)}| = d-1$, and (4.10) is obtained from $|G| = (d-1)|H||W|$.

(ii) $\mathbf{G_P^{(1)}}$ **is not cyclic**. As $|G_P^{(1)}| \geq |G_P^{(2)}| \geq d-1$ and $G_P^{(1)}$ acts semiregularly on $W \setminus \{P\}$, we have that $|W| \geq d$. If $|W| = d$, then

$$|W| - 1 = |G_P^{(1)}| = |G_P^{(2)}| = d-1 \ ;$$

therefore

$$|G| = |H||G_P^{(1)}||W| \leq (4g+2)(d-1)d < (12g^2+6g)d \ .$$

As a result we can assume that $|W| > d$. In addition, assume that $|G_P^{(2)}| = d$. Then $p|d$ and $\mathcal{X}$ is classical by Theorem 5.0.25. Then $|W| \leq \frac{6g-6+3d}{d-2} = 3d$. Since $G_P^{(1)}$ acts semiregularly on $W \setminus \{P\}$, d divides $|W|-1$. Therefore, $|W| \leq 2d+1$ and $|G_P^{(1)}| = d$. Then we have

$$|G| = |H||G_P^{(1)}||W| \leq (4g+2)d(2d+1) \leq (12g^2+6g)d \ .$$

From now on we assume that $|G_P^{(2)}| = d-1$. Note that all the hypotheses of Lemma 4.1.12 are satisfied, and we can apply Theorem 5.0.29 with $M = \{id\}$. Moreover, by the proof of Proposition 4.1.4, any non-trivial element of $G_P^{(2)}$ is an elation with axis $T_P(\mathcal{X})$ and center P. Therefore, for any point $R \in W \setminus \{P\}$, the line $\ell_{P,R}$ joining P and R is fixed by $G_P^{(2)}$, and as $G_P^{(2)}$ acts semiregularly on $W \setminus \{P\}$, the d distinct points of $\mathcal{X}$ in $\ell_{P,R}$ all belong to W. By Lemma 4.1.12, G acts 2-transitively on W; in particular the action of G is primitive on W. Let N be a minimal normal subgroup of G. Note that for any point $Q \in W$, $Q \neq P$, the two-point stabilizer $G_{P,Q}$ has size prime to p and is a subgroup of G_P; therefore it is a cyclic group. Then the Kantor-O'Nan-Seitz Theorem 5.0.30 applies to G. If N is abelian, then by Lemma 5.0.31 N is the only minimal normal subgroup of G, which contradicts Theorem 5.0.29. Therefore, Theorem 5.0.30 together with Theorem 5.0.29 imply that G is one of the following groups in their natural 2-transitive permutation representations:

1. $\mathrm{PSL}_2(p^a)$ with $p^a \geq 4$,

2. $\mathrm{PGL}_2(p^a)$ with $p^a \geq 4$,

3. ${}^2G_2(3^{2a+1})$ with $a \geq 0$, and

4. $\mathrm{PSU}_3(p^a)$ or $\mathrm{PGU}_3(p^a)$ with $p^a > 2$.

1. Suppose that G is $\mathrm{PSL}_2(p^a)$ in its natural 2-transitive permutation representation. Let $q = p^a$. Then the size of W is $q+1$, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q. Moreover, a complement H of $G_P^{(1)}$ in G_P is a cyclic group of order $(q-1)/2$ fixing a point $R \in W \setminus \{P\}$ and acting with two long orbits on $W \setminus \{P, R\}$. Note that H acts on $(\ell_{P,R} \cap \mathcal{X}) \setminus \{P, R\}$. Therefore $(q-1)/2 = d-2$ holds. Now take a point $Q \in W \setminus \ell_{P,R}$. It has already been noticed that on $\ell_{Q,R}$ there are $d-1$ points of W distinct from P. But then $|W| \geq 2d-1 = 2(d-2)+3 \geq q+2$, which contradicts $|W| = q+1$.

2. Suppose that G is $\mathrm{PGL}_2(p^a)$ in its natural 2-transitive permutation representation. Let $q = p^a$. Then the size of W is $q+1$, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q. Unlike the previous case, a complement H of $G_P^{(1)}$ in G_P is a cyclic group of order $(q-1)$ fixing a point $R \in W \setminus \{P\}$ and acting regularly on $W \setminus \{P, R\}$. Then H acts on $(\ell_{P,R} \cap \mathcal{X}) \setminus \{P, R\}$. Therefore $q = d-1$ holds. But this contradicts $q+1 = |W| > d$.

3. Suppose that G is ${}^2G_2(3^{2a+1})$, $p = 3$, in its natural 2-transitive permutation representation. Therefore the size of W is q^3+1, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q^3. Moreover, the commutator subgroup of $G_P^{(1)}$ has size q^2, whereas the center of $G_P^{(1)}$ has order q (see [16, Lemma 12.32]). By Lemma 4.1.12 $G_P^{(2)}$ is the center of $G_P^{(1)}$, whence $|G_P^{(2)}| = q$. On the other hand, in the proof of Lemma 4.1.12(iii) it has been shown that the commutator subgroup of $G_P^{(1)}$ is contained in $G_P^{(2)}$ (see (4.9)). Then $q^2 \leq |G_P^{(2)}|$, which is clearly a contradiction.

4. Suppose that G is either $\mathrm{PSU}_3(q)$ or $\mathrm{PGU}_3(q)$, $q = p^a > 2$, in its natural 2-transitive permutation representation. Therefore, the size of W is q^3+1, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q^3. Moreover, the center of $G_P^{(1)}$ has order q (see [16, Example A.9]). By Lemma 4.1.12, the center of $G_P^{(1)}$ is $G_P^{(2)}$; thus $|G_P^{(2)}| = q = d - 1$. Then the genus g of $\mathcal{X}$ is $\frac{q(q-1)}{2}$. As a result,

$$|G| \geq \frac{(q^3+1)q^3(q^2-1)}{3} > 16g^3 + 24g^2 + g\ .$$

By [16, Theorem 11.127] the unique curve of genus g with more than $16g^3 + 24g^2 + g$ automorphisms is the Hermitian curve. As we are assuming that $\mathcal{X}$ is not birationally equivalent to a Hermitian curve, a contradiction is obtained.

□

The proof of Theorem 4.0.1 is now complete.

CHAPTER 5

Appendix

5.0.1. Function Fields

In this section we give some facts related to function fields and for details we refer to [38].

Let F/K be a function field of genus g with full constant field K. For a divisor D of F denote by $\ell(D)$ the dimension of $\mathcal{L}(D)$, the Riemann-Roch space associated to D, then **Riemann-Roch theorem** states that

$$\ell(D) = \deg D + 1 - g + \ell(W - D) \ , \tag{5.1}$$

where W is a canonical divisor of F. (Note that here W is not the same as the one we used in Chapter 4 for the support of the ramification divisor.) Furthermore if $\deg D \geq 2g - 1$, then $\ell(D) = \deg D + 1 - g$; and therefore

$$\mathcal{L}(D + P) \setminus \mathcal{L}(D) \neq \emptyset$$

holds for any place P of F.

Let F'/F be a finite separable extension. Denote by K' and g' the full constant field and the genus of F', respectively. Then the **Hurwitz genus formula** relates the genus of F, the genus of F' and the different of F'/F as follows.

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathrm{Diff}(F'/F) \tag{5.2}$$

Kummer's Theorem is useful to determine all extensions of a place $P \in \mathbb{P}_F$ in F'. For convention denote by $\bar{F} := \mathcal{O}_P/P$ the residue class field of P. If $\varphi(T) = \sum c_i T^i$ is a polynomial with coefficients $c_i \in \mathcal{O}_P$, we set $\bar{\varphi}(T) = \sum \bar{c}_i T^i \in \bar{F}[T]$, where $\bar{c}_i = c_i$ mod P.

Theorem 5.0.21 (Kummer) Suppose that $F' = F(y)$, where y is integral over $\mathcal{O}_P$ with the minimal polynomial $\varphi(T) \in \mathcal{O}_P[T]$ such that $\bar{\varphi}(T)$ is a separable polynomial over $\bar{F}$. Write

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \psi_i(T) \ ,$$

where $\psi_i(T)$ is irreducible for all $i = 1, \ldots, r$. Choose $\varphi_i(T) \in \mathcal{O}_P[T]$ with

$$\bar{\varphi}_i(T) = \psi_i(T) \quad \text{and} \quad \deg \varphi_i(T) = \deg \psi_i(T) \ ,$$

then there exists a place $P_i \in \mathbb{P}_{F'}$ such that

$$P_i \mid P, \quad \varphi_i(y) \in P_i \quad \text{and} \quad f(P_i \mid P) = \deg \varphi_i(T) \ .$$

Furthermore, by the Fundamental Equality, there is no other place of F' lying over P.

Now we give formulas for ramification index and different exponent in two special types of Galois extensions, namely Kummer and Artin-Schreier extensions.

Theorem 5.0.22 (Kummer Extension) Let F/K be a function field, where K contains a primitive n-th root of unity and let $u \in F$ such that

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

Set $F' = F(y)$ with $y^n = u$. Then F'/F is Galois of degree n. Let $P \in \mathbb{P}_F$ and let $P' \in \mathbb{P}_{F'}$ lying above P, then the ramification index and the different exponent of $P' \mid P$ are given as follows.

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

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

Theorem 5.0.23 (Artin-Schreier Extension) Let F/K be a function field of characteristic $p > 0$. Suppose that there is an element $u \in F$ such that either $v_P(u) \geq 0$ or $v_P(u)$ is relatively prime to p for any place P of F. Define the integer m_P by

$$m_P := \begin{cases} m & \text{, if } v_P(u) = -m \text{ is relatively prime to } p \\ -1 & \text{, if } v_P(u) \geq 0 \ . \end{cases}$$

In addition suppose that there exists a place Q of F with $m_Q > 0$ and $\mathbb{F}_{p^r} \subseteq K$. Set $F' = F(y)$ with $y^{p^r} - y = u$. Then F'/F is a Galois extension of degree p^r. A place P of F is unramified if and only if $m_P = -1$. In the case of $m_P > 0$, P is totally ramified. Denote the unique place of F' lying over P by P', then the different exponent $d(P' \mid P)$ is given by

$$d(P' \mid P) = (p^r - 1)(m_P + 1) \ .$$

It is worth to note that in an extension F'/F if there exists a total ramification, then the full constant fields of F and F' are the same.

The following theorem gives the ramification and splitting behavior of a place in the compositum of function fields.

Theorem 5.0.24 Let F'/F be a finite separable extension of function fields. Suppose that $F' = F_1 \cdot F_2$ is the compositum of two intermediate fields $F_1, F_2 \supseteq F$.

(i) (Abhyankar's Lemma) For $P' \in \mathbb{P}_{F'}$ lying over $P \in \mathbb{P}_F$ set $P_i = P' \cap F_i$ for $i = 1, 2$. Assume that at least one of the extensions $P_1 \mid P$ or $P_2 \mid P$ is tame. Then the ramification index of $P' \mid P$ is given by

$$e(P' \mid P) = \operatorname{lcm}\{e(P_1 \mid P), e(P_2 \mid P)\},$$

where lcm denotes the least common multiple.

(ii) Suppose that $P \in \mathbb{P}_F$ such that P splits completely in F_1/F. Then every place $Q \in \mathbb{P}_{F_2}$ lying over P splits completely in F'/F_2. In particular, if P splits completely in both F_1/F and F_2/F, then P slits completely in F'/F. In this case if P is rational, then F' and F have the same full constant fields.

5.0.2. The Stöhr-Voloch Theory

The idea to investigate the local properties of a non-singular algebraic curve $\mathcal{X}$ using the intersection numbers $I(P, \mathcal{X} \cap \Pi)$ of $\mathcal{X}$ with hyperplanes Π through $P \in \mathcal{X}$ was developed for complex curves in the early nineteenth century; see for instance [35, Section 25]. In [40] the authors extended the classical treatment to curves defined over a field of positive characteristic. The original motivation was to find an upper bound for the number of $\mathbb{F}_q$-rational points of an algebraic curve defined over a finite field of order q. Here we use some of their results on ramification divisors of non-singular plane algebraic curves.

Assume that $\mathcal{X}$ is a non-singular plane curve. For a point $P \in \mathcal{X}$, the order sequence of $\mathcal{X}$ at P is the strictly increasing sequence

$$j_0(P) = 0 < j_1(P) = 1 < j_2(P)$$

such that each $j_i(P)$ is the intersection number $I(P, \mathcal{X} \cap \ell_i)$ of $\mathcal{X}$ and some line ℓ_i at P, see [40], and [16, Chapter 7.6]. For $i = 2$, such a line ℓ_2 is uniquely determined being the tangent line $T_P(\mathcal{X})$ to $\mathcal{X}$ at P. A point P for which $j_2(P) > 2$ is a flex (or an inflection point) of $\mathcal{X}$. The order sequence is the same for all but a finite number of points.

Definition 5.0.1 The curve $\mathcal{X}$ is said to be classical if the generic order sequence is $(\epsilon_0, \epsilon_1, \epsilon_2) = (0, 1, 2)$.

Theorem 5.0.25 (Corollary 2.2 in [28]) Assume that $p \geq 3$. If $\mathcal{X}$ is a non-classical curve of degree d, then $p|(d-1)$.

The concept of order sequence can be given for any linear series. Let $\mathcal{D}$ be a base-point-free linear series with degree d and dimension r. Let $\pi : \mathcal{X} \to PG(r, \mathbb{K})$, $\pi = (x_0 : x_1 : \ldots : x_r)$, be the morphism associated to $\mathcal{D}$. For a point P of $\mathcal{X}$, let γ_P be the branch of $\pi(\mathcal{X})$ corresponding to P via π. Then the $(\mathcal{D}, P)$-order sequence of $\mathcal{X}$ is the strictly increasing sequence

$$j_0^{\mathcal{D}}(P) = 0 < j_1^{\mathcal{D}}(P) < \ldots < j_r^{\mathcal{D}}(P)$$

such that each $j_i^{\mathcal{D}}(P)$ is the intersection number $I(\gamma_P, \mathcal{X} \cap H_i)$ of $\mathcal{X}$ and some hyperplane H_i at the branch γ_P. The $(\mathcal{D}, P)$-order sequence is the same, say $\epsilon_0^{\mathcal{D}} < \ldots < \epsilon_r^{\mathcal{D}}$, for all but finitely many points of $\mathcal{X}$. This constant sequence is the *$\mathcal{D}$-order sequence of* $\mathcal{X}$. The curve is *$\mathcal{D}$-classical* if $\epsilon_i^{\mathcal{D}} = i$ for each i.

The *ramification divisor* $R^{\mathcal{D}}$ of $\mathcal{D}$ is

$$R^{\mathcal{D}} = \text{div}(\det(D_\xi^{(\epsilon_i^{\mathcal{D}})} x_j)) + (\epsilon_0^{\mathcal{D}} + \ldots + \epsilon_r^{\mathcal{D}})\text{div}(d\xi) + (r+1)\sum e_P P,$$

where $e_P = -\min\{ord_P(x_0), \ldots, ord_P(x_r)\}$ and $D_\xi^{(\epsilon_i^{\mathcal{D}})}$ is the $\epsilon_i^{\mathcal{D}}$-th Hasse derivative with respect to a separating element ξ of $\mathbb{K}(\mathcal{X})$.

The support of $R^{\mathcal{D}}$ is the set of points of $\mathcal{X}$ whose $(\mathcal{D}, P)$-orders are different from $(\epsilon_0^{\mathcal{D}}, \ldots, \epsilon_r^{\mathcal{D}})$. Some of the properties of order sequences and ramification divisors are summarized in the following theorem. For a proof, see [16, Chapter 7].

Theorem 5.0.26 Let $\mathcal{D}$ be a base-point-free linear series with degree d and dimension r. Then we have

(i) $j_i^{\mathcal{D}}(P) \geq \epsilon_i^{\mathcal{D}}$ for each P and each i;

(ii) $v_P(R^{\mathcal{D}}) \geq \sum_i (j_i^{\mathcal{D}}(P) - \epsilon_i^{\mathcal{D}})$, and equality holds if and only if $\det(\binom{j_i^{\mathcal{D}}(P)}{\epsilon_j^{\mathcal{D}}}) \not\equiv 0 \mod p$;

(iii) $\deg(R^{\mathcal{D}}) = (2g-2)\sum_i \epsilon_i^{\mathcal{D}} + (r+1)d$; and

(iv) if $p \geq r$ and $\epsilon_i^{\mathcal{D}} = i$ for each $i = 0, 1, \ldots, r-1$, then either $\epsilon_r^{\mathcal{D}} = r$, or $\epsilon_r^{\mathcal{D}}$ is a power of p.

Definition 5.0.2 A projective irreducible plane curve $\mathcal{X}$ is said to be strange if there exists a point belonging to every tangent line at any non-singular point of $\mathcal{X}$.

Theorem 5.0.27 ([25]) A non-singular projective irreducible plane curve $\mathcal{X}$ is strange if and only if $\mathcal{X}$ is a conic in characteristic 2.

The following classification result due to Hefez [14] is a key lemma for Theorem 4.0.1.

Theorem 5.0.28 Let $\mathcal{X}$ be a non-singular non-strange plane curve of degree $d > 3$. If $d = \epsilon_2 + 1$, then $\mathcal{X}$ is projectively equivalent to the Hermitian curve.

5.0.3. Central Collineations

In this section we give some notions from Projective Geometry.

A *collineation* of a projective space $\mathrm{PG}(r, \mathbb{K})$ is an isomorphism from $\mathrm{PG}(r, \mathbb{K})$ to itself, that is, a bijection on the point sets mapping any subspace into a subspace. A collineation is *projective* if it is induced by a linear map of $\mathbb{K}^{r+1}$, that is, if it is an element of $\mathrm{PGL}_{r+1}(\mathbb{K})$, viewed as a permutation group acting on $\mathrm{PG}(r, \mathbb{K})$.

A collineation ϕ of $\mathrm{PG}(r, \mathbb{K})$, $r \geq 2$, is a *central* collineation if there is a hyperplane H (the *axis* of ϕ) and a point C (the *center* of ϕ) such that every point of H is a fixed point of ϕ and every line through C is a fixed line of ϕ.

If H is a hyperplane of $\mathrm{PG}(r, \mathbb{K})$ and C, P, P' are distinct collinear points of $\mathrm{PG}(r, \mathbb{K})$ with P, P' not in H, then there is precisely one central collineation of $\mathrm{PG}(r, \mathbb{K})$ with axis H and center C mapping P to P'. In particular, axis and center of a non-identical central collineation are uniquely determined.

A non-identical central collineation ϕ is an *elation* if its center is incident with its axis, and a *homology* if center and axis are not incident (the identity is considered both as homology and elation).

A collineation of $\mathrm{PG}(r, \mathbb{K})$, $r \geq 2$, is an *axial* collineation if there is a hyperplane H such that every point of H is a fixed point of ϕ. Each axial collineation is central [1, Lemma 3.1.9]. Each central collineation is a projective collineation [1, Theorem 3.6.1].

5.0.4. Some Results from Group Theory

(i) The projective linear group $\mathcal{G} = \mathrm{PGL}_2(p^a)$ has order $p^a(p^a - 1)(p^a + 1)$. It is the automorphism group of $\mathrm{PG}(1, p^a)$; equivalently, $\mathcal{G}$ acts on the set Ω of size $p^a + 1$ consisting of all $\mathbb{F}_{p^a}$-rational points of the projective line defined over $\mathbb{F}_{p^a}$. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $p^a(p^a - 1)$. The natural 2-transitive representation of $\mathrm{PSL}_2(p^a)$ is obtained when $\mathrm{PSL}_2(p^a)$ is viewed as a subgroup of $\mathrm{PGL}_2(p^a)$, see [20, Chapters II.7 and II.8] and [16, Appendix A, Example A.7]. For $p = 2$, $\mathrm{PGL}_2(p^a) = \mathrm{PSL}_2(p^a)$. For $p > 2$, $\mathrm{PSL}_2(p^a)$ has order $\frac{1}{2}p^a(p^a - 1)(p^a + 1)$. For $p^a \geq 4$, $\mathrm{PSL}_2(p^a)$ is a simple group and $\mathrm{PGL}_2(p^a)$ is a non-solvable group.

(ii) The projective unitary group $\mathcal{G} = \mathrm{PGU}_3(p^a)$ has order $(p^{3a} + 1)p^{3a}(p^{2a} - 1)$. It is the linear collineation group in the projective plane $\mathrm{PG}(2, p^{2a})$ preserving the classical unital Ω of size $p^{3a} + 1$ consisting of all absolute points of a non-degenerate unitary polarity of $\mathrm{PG}(2, p^{2a})$, see [19, Chapter II.8] and [16, Appendix A, Example A.9]. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $p^{3a}(p^{2a} - 1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the Hermitian curve, regarded as a non-singular plane curve defined over the finite field with p^{2a} elements $\mathbb{F}_{p^{2a}}$, acting on the set Ω of all its $\mathbb{F}_{p^{2a}}$-rational points. The special projective unitary group $\mathrm{PSU}_3(p^a)$ either coincides with $\mathrm{PGU}_3(p^a)$ or is a subgroup of $\mathrm{PGU}_3(p^a)$ of index 3 according as $\mu = 1$ or $\mu = 3$ with $\mu = \gcd(3, p^a + 1)$. In its action on Ω, $\mathrm{PSU}_3(p^a)$ is still 2-transitive, see [19, Chapter II.8] and [17]. For $p^a \geq 4$, $\mathrm{PSU}_3(p^a)$ is a simple group and $\mathrm{PGU}_3(p^a)$ is a non-solvable group.

(iii) The Suzuki group $\mathcal{G} = {}^2B_2(n)$ with $n = 2n_0^2$, $n_0 = 2^a$ and $a \geq 1$ has order $(n^2 + 1)n^2(n - 1)$. It is the linear collineation group of $\mathrm{PG}(3, n)$ preserving the Tits ovoid Ω of size $n^2 + 1$, see [21, Chapter XI.3] and [16, Appendix A, Example A.11]. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $n^2(n - 1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the DLS curve, regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$, acting on the set Ω of all its $\mathbb{F}_n$-rational points, see [10]. ${}^2B_2(n)$ is a simple group.

(iv) The Ree group $\mathcal{G} = {}^2G_2(n)$ with $n = 3n_0^2$, $n_0 = 3^a$ has order $(n^3+1)n^3(n-1)$. It is the linear collineation group of $\mathrm{PG}(6, n)$ preserving the Ree ovoid Ω of size n^3+1, see [21, Chapter XI.13] and [16, Appendix A, Example A.13]. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $n^3(n-1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the DLR curve, regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$, acting on the set Ω of all its $\mathbb{F}_n$-rational points, see [13] and [3], For $n > 3$, ${}^2G_2(n)$ is simple, while ${}^2G_2(3) \cong \mathrm{P\Gamma L}_2(8)$.

For each of the above linear groups, the structure of the 1-point stabilizer and its action in the natural 2-transitive permutation representation, as well as its automorphism group, are explicitly given in the papers quoted.

We now give classification results on finite groups with trivially intersecting Sylow p-subgroups.

Theorem 5.0.29 (Theorem 3.16 **in [11])** Let S be a Sylow p-subgroup of a finite group $\mathcal{G}$ with $S \subsetneq \mathcal{G}$. Set $I := N_{\mathcal{G}}(S)$ and $M := C(I)$. Suppose that $p > 2$, and

(i) $I = SH$, with H cyclic;

(ii) for $h \in \mathcal{G} \setminus I$, $S \cap h^{-1}Sh = \{id\}$.

Then

(i) M is a normal subgroup of $\mathcal{G}$;

(ii) $\mathcal{G}/M$ has a unique minimal normal subgroup, which is non-abelian simple and isomorphic to one of the following groups: $\mathrm{PSL}_2(p^a)$ with $a \geq 2$, $\mathrm{PSU}_3(p^a)$ with $p^a > 2$, and for $p = 3$ the Ree group ${}^2G_2(3^{2a+1})'$ with $a \geq 0$.

In particular, $\mathcal{G}$ acts 2-transitively on the set of Sylow p-subgroups of $\mathcal{G}$.

Theorem 5.0.30 (The Kantor-O'Nan-Seitz Theorem [23]) Let $\mathcal{G}$ be a finite 2-transitive permutation group whose 2-point stabiliser is cyclic. Then either $\mathcal{G}$ has an elementary abelian regular normal subgroup, or $\mathcal{G}$ is one of the following groups in their natural 2-transitive permutation representations: $\mathrm{PSL}_2(p^a)$, $p^a \geq 4$, $\mathrm{PGL}_2(p^a)$, $p^a \geq 4$, $\mathrm{PSU}_3(p^a)$ with $p^a > 2$, $\mathrm{PGU}_3(p^a)$ with $p^a > 2$, the Suzuki group ${}^2B_2(n)$, ${}^2G_2(3^{2a+1})$ with $a \geq 0$.

We end this section with a classical result on primitive permutation groups. For a proof, see e.g. [24, Corollary 2].

Lemma 5.0.31 If $\mathcal{G}$ is a finite primitive permutation group, then $\mathcal{G}$ contains at most 2 minimal normal subgroup and if $\mathcal{G}$ has an abelian normal subgroup then it has a unique minimal normal subgroup.

Bibliography

[1] A. Beutelspacher and U. Rosenbaum, *Projective Geometry: From Foundations to Applications*, *Cambridge University Press*, Cambridge, 1998.

[2] J. Bezerra, A. Garcia, H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. **589** (2005), 159-199.

[3] E. Çakçak and F. Özbudak, *Subfields of the function field of the Deligne–Lusztig curve of Ree type*, *Acta Arith.* **115** (2004), 133–180.

[4] I. Duursma, K.-H. Mak, *On lower bounds for the Ihara constants* A(2) *and* A(3), arXiv:1102.4127v2 [math. NT], 21 Mar 2011.

[5] N. D. Elkies, *Explicit towers of Drinfel'd modular curves*, in European Congress of Mathematics, vol. II (Barcelona 2000), ed. C. Casacuberta, R. M. Miró–Roig, J. Verdera, S. Xambó–Descamps, Progr. Math. **202**, Birkhäuser (2001), 189-198.

[6] N. D. Elkies, E. W. Howe, A. Kresch, B. Poonen, J. L. Wetherell, M. E. Zieve, *Curves of every genus with many points,* II*: Asymptotically good families*, Duke Math. J. **122** (2004), 399-422.

[7] A. Garcia, H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211-222.

[8] A. Garcia, H. Stichtenoth, M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl. **3** (1997), 257-274.

[9] G. van der Geer, M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34 (3)** (2002), 291-300.

[10] M. Giulietti, G. Korchmáros and F. Torres, *Quotient curves of the Deligne–Lusztig curve of Suzuki type*, *Acta Arith.* **122** (2006), 245–274.

[11] R. Guralnick, B. Malmskog and R. Pries, *The automorphism groups of a family of maximal curves*, arXiv:1105.3952.

[12] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics No. **52**.

[13] J.P. Hansen and J.P. Pedersen, *Automorphism group of Ree type, Deligne-Lusztig curves and function fields*, *J. Reine Angew. Math.* **440** (1993), 99–109.

[14] A. Hefez, *Non-reflexive curves*, *Composition Math.* **69** (1989), 3–35.

[15] H.W. Henn, *Funktionenkörper mit großer Automorphismengruppe*, *J. Reine Angew. Math.* **302** (1978), 96–115.

[16] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over finite fields*, Princeton University Press, Princeton and Oxford, 2008.

[17] A.R. Hoffer, *On unitary collineation groups*, *J. Algebra* **22** (1972), 211–218.

[18] E. Howe, K. Lauter, C. Ritzenthaler, G. van der Geer, *manYPoints - Table of Curves with Many Points*, http://www.manypoints.org

[19] D.R. Hughes and F.C. Piper, *Projective Planes*, Graduate Texts in Mathematics **6**, Springer, New York, 1973.

[20] B. Huppert, *Endliche Gruppen. I*, *Grundlehren der Mathematischen Wissenschaften* **134**, Springer, Berlin, 1967.

[21] B. Huppert and B.N. Blackburn, *Finite groups. III*, *Grundlehren der Mathematischen Wissenschaften* **243**, Springer, Berlin, 1982.

[22] 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), 721-724.

[23] W.M. Kantor, M. O'Nan and G.M. Seitz, *2-transitive groups in which the stabilizer of two points is cyclic*, *J. Algebra* **21** (1972), 17–50.

[24] M. W. Liebeck, C. E. Praeger and J. Saxl, *On the O'Nan-Scott Theorem for Finite Primitive Permutation Groups*, *J. Austral. Math. Soc. (Series A)* **44** (1988), 389–396.

[25] E. Lluis, *Variedades algebraicas con ciertas condiciones en sus tangentes*, *Bol. Soc. Mat. Mexicana (2)* **7** (1962), 47–56.

[26] H. Niederreiter, C. P. Xing, *Rational points on curves over finite fields*, vol. **285** of London Mathematical Society Lecture Note Series, Cambridge University Press, 2001.

[27] H. Niederreiter, C. P. Xing, *Algebraic geometry in coding theory and cryptography*, Princeton University Press, Princeton, NJ, 2009.

[28] R. Pardini, *Some remarks on plane curves over finite fields of finite characteristic*, *Compositio Math.* **60** (1986), 3–17.

[29] P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, *Math. Z.* **117** (1970), 157–163.

[30] B. Segre, *Sulle curve algebriche che ammettono come trasformata razionale una curva piana dello stesso ordine, priva di punti multipli*, *Math. Ann.* **109** (1933), 1–3.

[31] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer, New York, 1979.

[32] J.-P. Serre, *Nombres de points des courbes algébriques sur* $\mathbb{F}_q$, in Séminaire de Théorie des Nombres de Bordeaux 1982-1983, exposé n^o 22.

[33] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sc. Paris, Sér. I Math. **296** (1983), 397-402.

[34] J.-P. Serre, *Rational points on curves over finite fields*, Lectures given at Harvard University. Notes by F. Q. Gouvêa (1985).

[35] F. Severi, *Trattato di Geometria Algebrica*, Zanichelli, Bologna, 1926.

[36] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, *Arch. Math.* **24** (1973), 527–544.

[37] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern*, *Arch. Math.* **24** (1973), 615–631.

[38] H. Stichtenoth, *Algebraic function fields and codes*, 2$^{\text{nd}}$ Edition, Springer-Verlag, 2009. Graduate Texts in Mathematics No. **254**.

[39] H. Stichtenoth, *Curves with a prescribed number of rational points*, Finite Fields Appl., Vol.**17**, No **6** (2011), 552-559.

[40] K.O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fileds*, *Proc. London Math. Soc.* (3) **52** (1986), 1-19.

[41] J. Top, *Genus of genus 3 over small finite fields*, Indag. Mathem. **14(2)** (2003), 275-283.

[42] S. G. Vlăduţ, V. G. Drinfel'd, *The number of points of an algebraic curve*, Funct. Anal. Appl. **17** (1983), 53-54.

[43] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in Fundamentals of computation theory (Cottbus 1985), vol. **199** of Lecture Notes in Comp. Sc., pp. 503-511, Springer-Verlag, 1985.