



UNIVERSITÀ
DEGLI STUDI
FIRENZE



UNIVERSITÀ
DEGLI STUDI
DI PERUGIA



Università di Firenze, Università di Perugia, INdAM consorziate nel CIAFM

**DOTTORATO DI RICERCA
IN MATEMATICA, INFORMATICA, STATISTICA
CURRICULUM IN MATEMATICA
CICLO XXXVIII**

Sede amministrativa Università degli Studi di Firenze
Coordinatrice Prof.ssa Alessandra Sestini

**Automorphisms of algebraic
curves in positive characteristic
and their applications**

Settore Scientifico Disciplinare MATH -02/B

Dottoranda:
Arianna Dionigi

Supervisore
Prof. Massimo Giulietti
Co-Supervisori
Prof. Daniele Bartoli,
Prof.ssa Giuliana Fatabbi

Coordinatrice
Prof.ssa Alessandra Sestini

Contents

Introduction	VII
1 Background and Preliminary Results	1
1.1 Algebraic curves	1
1.1.1 Affine varieties	1
1.1.2 Projective varieties	6
1.1.3 Rational maps	8
1.1.4 DVR of an algebraic curve	10
1.1.5 Divisors, genus and Weierstrass semigroup of an algebraic curve	12
1.1.6 Coverings	18
1.2 Automorphism groups of algebraic curves	22
1.3 Maximal curves	27
1.4 Linear Codes	30
1.4.1 Algebraic-Geometric Codes	33
2 Algebraic curves with large automorphism groups	37
2.1 Automorphism groups of order greater than $4(g - 1)$	39
2.2 Cyclic groups	43
2.2.1 Proof of Theorem 2.5 when p divides N	45
2.2.2 Proof of Theorem 2.5 when p does not divide N	59
2.3 Abelian groups	66
2.4 Dihedral groups	82
2.5 Nilpotent groups	98
2.6 Non-perfect groups	99
2.7 Groups with a cyclic subgroup of index 2	104
2.7.1 Groups of size a multiple of p	109
2.7.2 Groups of size coprime to p	112

2.7.3	Classification results	122
3	Galois subcovers of the Hermitian curve	129
3.1	The function field of the Hermitian curve	131
3.2	Galois subcovers of $\mathbb{F}_{q^2}(\mathcal{H})$ of type (I) of Theorem (3.6)	135
3.3	Galois subcovers of $\mathbb{F}_{q^2}(\mathcal{H})$ of type (II) of Theorem (3.6) . . .	136
3.4	Galois subcovers of $\mathbb{F}_{q^2}(\mathcal{H})$ of type (III) of Theorem (3.6) . . .	138
3.5	Weierstrass semigroups and application to AG-codes	140
	Bibliography	145

Introduction

The study of algebraic curves $\mathcal{X}$ with numerous automorphisms in relation to their genus $g(\mathcal{X})$ is a classical and well-established area in Algebraic-Geometric, and it continues to be an active field of research. The Hurwitz bound on the order of the $\mathbb{K}$ -automorphism group $\text{Aut}(\mathcal{X})$ of an algebraic curve $\mathcal{X}$ of genus $g(\mathcal{X}) \geq 2$ defined over a field $\mathbb{K}$ with characteristic zero states that $|\text{Aut}(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1)$. When the characteristic p divides $|\text{Aut}(\mathcal{X})|$, the classical Hurwitz bound does not generally apply. Specifically, if $g(\mathcal{X}) \geq 2$, then $|\text{Aut}(\mathcal{X})| < 8g(\mathcal{X})^3$ except for four infinite families of curves; see [29] or [32, Theorem 11.127]. These results, which strictly relate the geometric complexity of the curve to the size of its automorphism group, have motivated a long line of studies aimed to determine classes of curves which have an automorphism group that is close to the upper bounds, as well as to classify curves whose automorphism group has a specific algebraic structure. In fact, stronger bounds for subgroups G of $\text{Aut}(\mathcal{X})$ under certain conditions have been established.

For instance, back in 1995 Irokawa and Sasaki [36] gave a complete classification of curves over $\mathbb{C}$ with an automorphism of order $N \geq 2g(\mathcal{X}) + 1$. The situation deeply changes when one considers the case of positive characteristic: in this context, the possibility of wild ramification has presented a few challenges to the investigation. On the other hand, if a subgroup G of $\text{Aut}(\mathcal{X})$ is dihedral, then in the complex case, $|G| \leq 4g(\mathcal{X}) + 4$, see [7]. More recently it has been shown that a tighter bound holds for G a generalized quasi-dihedral group ([31, Theorem 6.1]).

A central aspect of this thesis is the extension of several results known for the case of zero characteristic to the case of positive characteristic. In particular, we provide a complete classification of curves $\mathcal{X}$ admitting a cyclic automorphism group of size greater than $2g(\mathcal{X})$, as well as a complete classification of curves $\mathcal{X}$ with an automorphism group admitting a cyclic subgroup of index 2 and size greater than $2g(\mathcal{X}) + 1$.

Other results are obtained for abelian groups and for solvable groups, with the additional hypothesis that the characteristic p does not divide the size of the group. In this context, it should be noted that our proofs in the case where p does not divide $|G|$ use basically ramification theory, as well as the theory of finite permutation groups. Although one could alternatively appeal to the celebrated Abhyankar Conjecture, such proofs would not reflect the perspective adopted in this dissertation (for a survey on Abhyankar Conjecture and its consequences on the theory of automorphism groups of a curve see for instance [28]).

Understanding the behavior of automorphism groups in positive characteristic has not only a theoretical relevance, but also has important applications. In fact curves with many automorphisms, defined over finite field, are closely related to the construction of Algebraic-Geometric codes (AG-codes). It is well-known that *good* AG-codes can be constructed from curves defined over finite fields with many rational points with respect to their genus. Generally speaking, if a curve possesses many rational points, than also its quotient curve with respect to an automorphism group will do. This is certainly true for curves attaining the Hasse-Weil upper bound on the number of rational points, the so-called maximal curve. In fact, any quotient curve of a maximal curve over a field with q elements with respect to an automorphism group defined over the same field is a maximal curve.

In particular, a problem of current interest, is to find explicit equations for quotients of the maximal curve with the highest possible genus, namely the Hermitian curve. This has been done so far ad hoc, in particular in the cases where the Galois group has prime order and also when has order the square of the characteristic. Within this framework lie some of the results presented in this thesis, which aim to explicitly describe some families of maximal curves related to the Hermitian curve, with possible applications to coding theory.

Chapter 1 is a collection of preliminary definitions and results that will be used in the following chapters. The fundamental concepts of algebraic curves, function fields, morphisms, automorphism groups and coverings of curves, together with the notions of ramification, Hurwitz's theorem and behavior of extensions in positive characteristic are recalled. Furthermore, the notion of maximal curve over a finite field is introduced, and the main links with the theory of Algebraic-Geometric codes are presented.

In Chapter 2 curves with large automorphism group are investigated. In the first part of the chapter, curves with a cyclic automorphism group of order N at least $2g(\mathcal{X}) + 1$ in positive characteristic $p \neq 2$ are successfully classified,

offering the positive characteristic counterpart to the Irokawa-Sasaki result. Then curves with abelian, dihedral and non-perfect groups are studied. In the final part it will be tackled the case of groups with a cyclic subgroup of index 2. This in particular includes dihedral and quasi-dihedral groups, but also others more general structures. After recalling some known bounds, it will be proved that an analogous bound holds for these groups. In particular, we show that the upper bound for the size of a dihedral group of automorphisms holds for curves defined over an algebraically closed field of characteristic $p \neq 2$. Then we provide some classification results about (non-dihedral) groups of size larger than $4g(\mathcal{X}) + 4$ admitting a cyclic subgroup of index 2. This part of the thesis thus broadens the understanding of the behavior of large automorphism groups in positive characteristic, extending the picture known in characteristic zero.

Finally, Chapter 3 is focused on the study of some Galois subcovers of the Hermitian curve. The Hermitian curve represents a classical and well-known example of a maximal curve. To find new maximal curves and explicit equations is a problem of great interest both under the theoretical and practical side. In this chapter we obtain explicit equations of all Galois subcovers of the Hermitian curve with Galois group of order dp where p is the characteristic of $\mathbb{F}_{q^2}$ and d is a prime other than p . We also compute the generators of the Weierstrass semigroup at a special $\mathbb{F}_{q^2}$ -rational point of some of the curves, and discuss some possible positive impacts on the minimum distance problems of AG-codes.

Taken together the results presented in this thesis contribute to outlining a larger picture of the relationship between the structure of the automorphism group of a curve and its geometry, by extending several classical results to the case of positive characteristic.

On one side, the classifications obtained in Chapter 2 broaden the understanding of possible bounds on the size of the automorphism groups in this context; on the other side the study of Galois subcovers of the Hermitian curve shows how these structures can be used in order to construct curves with many symmetries and interesting properties.

Chapter 1

Background and Preliminary Results

1.1 Algebraic curves

In this first chapter all the definitions and preliminary results needed for the following chapters will be introduced. In particular the focus will be on algebraic curves and on all the objects that can be associated to them.

1.1.1 Affine varieties

Let $\mathbb{K}$ be an algebraically closed field and let $\mathbb{A}^n(\mathbb{K}) = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{K}\}$ be the n -dimensional affine space over $\mathbb{K}$.

Definition 1.1. Let I be an ideal of $\mathbb{K}[X_1, \dots, X_n]$, that is the polynomial ring in n indeterminates over $\mathbb{K}$, the subset of $\mathbb{A}^n(\mathbb{K})$ defined by

$$V(I) := \{(a_1, \dots, a_n) \in \mathbb{A}^n(\mathbb{K}) \mid f(a_1, \dots, a_n) = 0 \forall f \in I\}$$

is called *affine algebraic set associated with I* .

Since $\mathbb{K}[X_1, \dots, X_n]$ is a Noetherian ring, each of its ideals is finitely generated. Hence, if $I = \langle f_1, \dots, f_m \rangle$, it trivially follows that

$$V(I) := \{(a_1, \dots, a_n) \in \mathbb{A}^n(\mathbb{K}) \mid f_i(a_1, \dots, a_n) = 0 \forall i = 1, \dots, m\}.$$

Definition 1.2. Let $V \subset \mathbb{A}^n(\mathbb{K})$ be an affine algebraic set, the ideal of $\mathbb{K}[X_1, \dots, X_n]$ defined by

$$I(V) = \{f \in \mathbb{K}[X_1, \dots, X_n] \mid f(a_1, \dots, a_n) = 0 \ \forall (a_1, \dots, a_n) \in V\}$$

is called *ideal of V* .

Definition 1.3. An affine algebraic set $V \subseteq \mathbb{A}^n(\mathbb{K})$ is called *reducible* if there exist two affine algebraic sets V_1 and V_2 such that $V_1, V_2 \subsetneq V$ and $V = V_1 \cup V_2$. Otherwise V is called *irreducible*.

Definition 1.4. An affine algebraic set that is irreducible is called *affine variety*.

The main properties of affine algebraic sets and their ideals are summarized in the following proposition.

Proposition 1.5. 1 Let V_1 and V_2 be two affine algebraic sets, then $V_1 \cup V_2$ and $V_1 \cap V_2$ are affine algebraic sets.

2 Let J be an ideal of $\mathbb{K}[X_1, \dots, X_n]$, then $J \subset I(V(J))$.

3 (Hilbert's Theorem) Let J be an ideal of $\mathbb{K}[X_1, \dots, X_n]$, then $I(V(J)) = \sqrt{J}$ where

$$\sqrt{J} := \{f \in \mathbb{K}[X_1, \dots, X_n] \mid \exists m \in \mathbb{Z}, m \geq 1 \text{ such that } f^m \in J\}.$$

4 Let V be an affine algebraic set, then $V = V(I(V))$.

5 An affine algebraic set V is irreducible if and only if $I(V)$ is a prime ideal.

6 Each affine algebraic set V can be written as finite union of algebraic varieties.

To each affine variety V it is possible to associate a ring, denoted by $\mathbb{K}[V]$ and that is called *affine coordinate ring of V* , defined as follows

$$\mathbb{K}[V] := \mathbb{K}[X_1, \dots, X_n] / I(V).$$

A generic element of $\mathbb{K}[V]$ is of the form $\alpha = f + I(V)$ with $f \in \mathbb{K}[X_1, \dots, X_n]$.

Remark 1.6. Since V is irreducible, $I(V)$ is a prime ideal and then $\mathbb{K}[V]$ is an integral domain.

In a natural way, to each affine variety V , can also be associated a field, that is the field of fractions of $\mathbb{K}[V]$. It is called *field of rational functions of V* and it is denoted by $\mathbb{K}(V)$, hence

$$\mathbb{K}(V) := \left\{ \frac{f + I(V)}{g + I(V)} \mid f, g \in \mathbb{K}[X_1, \dots, X_n], g \notin I(V) \right\}.$$

Remark 1.7. $\mathbb{K}(V) = \mathbb{K}(\overline{x_1}, \dots, \overline{x_n})$ where $\overline{x_i} := x_i + I(V)$.

Definition 1.8. Let V be an affine variety and let $P = (a_1, \dots, a_n)$ be an element of V . A rational function $\alpha \in \mathbb{K}(V)$ is called *regular* (or *defined*) at P if there exist $f, g \in \mathbb{K}[X_1, \dots, X_n]$ such that $\alpha = \frac{f + I(V)}{g + I(V)}$ and $g(a_1, \dots, a_n) \neq 0$.

If a rational function α is defined at P , then it is well defined the value $\alpha(P) := \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)}$.

Definition 1.9. Let V be an affine variety, the *dimension* of V is the degree of transcendence of $\mathbb{K}(V)$ over $\mathbb{K}$, and it is denoted by $\dim(V)$.

Definition 1.10. An *affine curve* is an affine variety of dimension one.

Proposition 1.11. Let $V \subseteq \mathbb{A}^2(\mathbb{K})$, if $V = V(\langle f \rangle)$, with f an irreducible polynomial, then V is an affine variety and $\dim(V) = 1$.

After the definition of regular functions, it is possible to associate a local ring to each affine variety V . Recall that a *local ring* R is a commutative ring with unity which satisfies one of the following equivalent conditions

- 1 the set of non-invertible elements of R is an ideal
- 2 there exists a unique proper maximal ideal of R which contains each other proper ideal of R

and the ideal of non-invertible elements is exactly the unique proper maximal ideal.

Definition 1.12. Let $V \subseteq \mathbb{A}^n(\mathbb{K})$ be an affine variety and let P be a point of V . The *local ring of V in P* is

$$\mathbb{K}[V]_P := \{ \alpha \in \mathbb{K}(V) \mid \alpha \text{ is regular at } P \}.$$

Proposition 1.13. $\mathbb{K}[V]_P$ is a local Noetherian domain and its ideal of non invertible elements, denoted by $M_P(V)$, is

$$M_P(V) = \{\alpha \in \mathbb{K}[V]_P \mid \alpha(P) = 0\}.$$

Definition 1.14. Let V be an affine variety and let $P = (a_1, \dots, a_n)$ be a point of V .

- 1 The *tangent space to V at P* , denoted by $T_P(V)$, is defined as the linear subspace

$$T_P(V) = \bigcap_{f \in I(V)} \left(\sum_{i=1}^n \frac{\partial f}{\partial X_i}(P)(X_i - a_i) = 0 \right).$$

- 2 The *cotangent space to V at P* is defined as the linear subspace $M_P(V)/M_P^2(V)$ where $M_P^2(V)$ is the ideal generated by $\{fg \mid f, g \in M_P\}$.

Definition 1.15. A point P of an affine variety V is called *singular* if $\dim(T_P(V)) > \dim(V)$ and *non-singular* (or *simple*) if $\dim(T_P(V)) = \dim(V)$.

From now on an affine curve will be denoted by $\mathcal{X}$.

Proposition 1.16. Let P be a non-singular point of an affine curve $\mathcal{X}$, then $M_P(\mathcal{X})$ is a principal ideal.

Definition 1.17. Let P be a non-singular point of an affine curve $\mathcal{X}$. A *local parameter* of $\mathcal{X}$ at P is a generator of $M_P(\mathcal{X})$.

Recall that a *discrete valuation ring* A is an integral domain such that

- 1 A is not a field,
- 2 A is local,
- 3 A is Noetherian,
- 4 the maximal ideal of A is principal.

Proposition 1.18. Let P be a non-singular point of an affine curve $\mathcal{X}$, then $\mathbb{K}[V]_P$ is a discrete valuation ring.

To each non singular point of an affine curve it is possible to associate a valuation function in the following way.

Proposition 1.19. *Let P be a non singular point of an affine curve $\mathcal{X}$ and let t be a local parameter of $\mathcal{X}$ at P . Then for all $\alpha \in \mathbb{K}[\mathcal{X}]_P$, $\alpha \neq 0$, there exists a unique $m \in \mathbb{Z}$, $m \geq 0$, and a unique $u \in (\mathbb{K}[\mathcal{X}]_P \setminus M_P(\mathcal{X}))$ such that $\alpha = ut^m$. Furthermore for all $\alpha \in \mathbb{K}(\mathcal{X})$, $\alpha \neq 0$, there exists a unique $m \in \mathbb{Z}$, and a unique $u \in (\mathbb{K}[\mathcal{X}]_P \setminus M_P(\mathcal{X}))$ such that $\alpha = ut^m$.*

Definition 1.20. Let P be a non-singular point of an affine curve $\mathcal{X}$ and let $\alpha \in \mathbb{K}(\mathcal{X})$, $\alpha \neq 0$. The *order* of α at P , denoted by $\text{ord}_P(\alpha)$, is defined as the unique integer m such that $\alpha = ut^m$, where $u \in (\mathbb{K}[\mathcal{X}]_P \setminus M_P(\mathcal{X}))$ and t is a local parameter of $\mathcal{X}$ at P . For $\alpha = 0$ assume $\text{ord}_P(\alpha) = \infty$.

It can be noticed that

$$\mathbb{K}[\mathcal{X}]_P = \{\alpha \in \mathbb{K}(\mathcal{X}) \mid \text{ord}_P(\alpha) \geq 0\} \text{ and } M_P = \{\alpha \in \mathbb{K}(\mathcal{X}) \mid \text{ord}_P(\alpha) > 0\}.$$

In the next proposition there are the main properties of the order of functions at a point.

Proposition 1.21. *Let $\mathcal{X}$ be an affine curve and let P be a non-singular point of $\mathcal{X}$. Then*

- 1 $\text{ord}_P(\alpha\beta) = \text{ord}_P(\alpha) + \text{ord}_P(\beta)$ for all $\alpha, \beta \in \mathbb{K}(\mathcal{X})$;
- 2 $\text{ord}_P(\alpha+\beta) \geq \min\{\text{ord}_P(\alpha), \text{ord}_P(\beta)\}$ for all $\alpha, \beta \in \mathbb{K}(\mathcal{X})$, if $\text{ord}_P(\alpha) \neq \text{ord}_P(\beta)$ then the equality holds;
- 3 $\text{ord}_P(a) = 0$ for all $a \in \mathbb{K}$.

Definition 1.22. Let P be a point of a non-singular (that is there are no singular point) affine curve $\mathcal{X}$ and let $\alpha \in \mathbb{K}(\mathcal{X})$. P is called *zero of multiplicity m* for α if $\text{ord}_P(\alpha) = m > 0$, whereas it is called *pole of multiplicity m* for α if $\text{ord}_P(\alpha) = m < 0$.

At this point the Proposition 1.16 can be reversed.

Proposition 1.23. *Let $\mathcal{X}$ be an affine curve and let P be a point of $\mathcal{X}$. If $\mathbb{K}[\mathcal{X}]_P$ is a discrete valuation ring, that is if $M_P(\mathcal{X})$ is principal, then P is a non-singular point.*

1.1.2 Projective varieties

Let $\mathbb{P}^n(\mathbb{K})$ be the n -dimensional projective space over $\mathbb{K}$.

Definition 1.24. Let I be a homogeneous ideal of $\mathbb{K}[X_0, \dots, X_n]$, the subset of $\mathbb{P}^n(\mathbb{K})$ defined by

$$V(I) := \{P \in \mathbb{P}^n(\mathbb{K}) \mid F(P) = 0 \ \forall F \in I \text{ such that } F \text{ is homogeneous}\}$$

is called *projective algebraic set associated with I* .

Definition 1.25. Let $V \subseteq \mathbb{P}^n(\mathbb{K})$ be a projective algebraic set, the homogeneous ideal of $\mathbb{K}[X_0, \dots, X_n]$ denoted by $I(V)$ and generated by

$$\{F \in \mathbb{K}[X_0, \dots, X_n] \mid F \text{ is homogeneous and } F(P) = 0 \ \forall P \in V\}$$

is called *homogeneous ideal of V* .

Definition 1.26. A projective algebraic set $V \subseteq \mathbb{P}^n(\mathbb{K})$ is called *reducible* if there exists two projective algebraic sets V_1 and V_2 such that $V_1, V_2 \subsetneq V$ and $V = V_1 \cup V_2$. Otherwise V is called *irreducible*.

Definition 1.27. A projective algebraic set that is irreducible is called *projective variety*.

Proposition 1.28. A projective algebraic set V is irreducible if and only if $I(V)$ is a prime ideal.

As in the previous subsection, for each projective variety V it can be defined the *projective coordinate ring of V* as

$$\mathbb{K}[V] := \mathbb{K}[X_0, \dots, X_n] / I(V)$$

and the *field $\mathbb{K}(V)$ of rational functions of V* as

$$\left\{ \frac{F + I(V)}{G + I(V)} \mid F, G \in \mathbb{K}[X_0, \dots, X_n] \text{ are homogeneous, } \deg F = \deg G, G \notin I(V) \right\}.$$

Definition 1.29. Let V be a projective variety and let P be an element of V . A rational function $\alpha \in \mathbb{K}(V)$ is called *defined* (or *regular*) at P if there exist $F, G \in \mathbb{K}[X_0, \dots, X_n]$, two homogeneous polynomials of the same degree, such that $\alpha = \frac{F + I(V)}{G + I(V)}$ and $G(P) \neq 0$

Hence, in the same way as in the previous subsection, it can be defined the *local ring* of a projective variety V at a point P , still denoted by $\mathbb{K}[V]_P$, and, as in the affine case, it is a local Noetherian domain and its ideal of non-invertible elements is denoted by $M_P(V)$.

Remark 1.30. *The affine space $\mathbb{A}^n(\mathbb{K})$ can be seen as a subset of the projective space $\mathbb{P}^n(\mathbb{K})$ via the maps $\varphi_i : \mathbb{A}^n(\mathbb{K}) \longrightarrow U_i$ where*

$$U_i := \{(X_0, \dots, X_n) \in \mathbb{P}^n(\mathbb{K}) \mid X_i \neq 0\},$$

defined by

$$\varphi_i(a_1, \dots, a_n) = (a_1, \dots, a_{i-1}, 1, a_i, \dots, a_n)$$

(For simplicity of the notation it will be fixed $i = 0$).

The next definition clarifies the connection between affine and projective algebraic sets.

Definition 1.31. Let $V \subseteq \mathbb{A}^n(\mathbb{K})$ be an affine variety. The projective algebraic set $\overline{V} := V(I)$ where I is the homogeneous ideal of $\mathbb{K}[X_0, \dots, X_n]$ generated by $\{F^* \mid F \in I(V)\}$, where F^* is the homogenization of F , is called *projective closure* of V .

The correspondence

$$V \longmapsto \overline{V}$$

defines a bijection between the set of the affine varieties of $\mathbb{A}^n(\mathbb{K})$ and the set of the projective varieties of $\mathbb{P}^n(\mathbb{K})$ that are not contained in $H_0 := \{(X_0, \dots, X_n) \mid X_0 = 0\}$.

Proposition 1.32. *Let V be an affine variety. Then*

1 $\overline{V}$ is irreducible;

2 $V = \overline{V} \cap \mathbb{A}^n(\mathbb{K})$;

3 *The map $\varphi : \mathbb{K}(\overline{V}) \longrightarrow \mathbb{K}(V)$, defined by $\varphi\left(\frac{F + I(\overline{V})}{G + I(\overline{V})}\right) = \frac{F_* + I(V)}{G_* + I(V)}$, where F_* and G_* are the dehomogenizations of F and G , is well defined. Furthermore, φ is an isomorphism that induces a ring isomorphism between $\mathbb{K}[\overline{V}]_P$ and $\mathbb{K}[V]_P$ if $P \in V$.*

Definition 1.33. Let V be a projective variety, the *dimension* of V is the transcendence degree of $\mathbb{K}(V)$ over $\mathbb{K}$, and it is denoted by $\dim(V)$.

Definition 1.34. A *projective curve* is a projective variety of dimension one.

Definition 1.35. A point P of a projective variety V is called *singular* (respectively *non-singular*) if and only if it is singular (respectively non-singular) for any of its affine parts.

As in the previous subsection, the following result holds.

Proposition 1.36. A point P of a projective curve $\mathcal{X}$ is non-singular if and only if $M_P(\mathcal{X})$ is a principal ideal.

1.1.3 Rational maps

Definition 1.37. Let $V_1 \subseteq \mathbb{P}^n(\mathbb{K})$ be a projective variety. A *rational map* from V_1 to $\mathbb{P}^m(\mathbb{K})$ is an element $\varphi = (\alpha_0 : \cdots : \alpha_m) \in \mathbb{P}^m(\mathbb{K}(V_1))$.

Let us notice that a rational map of V_1 in $\mathbb{P}^m(\mathbb{K})$ is not necessarily defined on each point of V_1 . Furthermore, sometimes, it is possible to evaluate $\varphi(P)$ at points P of V_1 where certain α_i are not regular by replacing α_i with $\lambda\alpha_i$ for a suitable $\lambda \in \mathbb{K}(V_1)$.

Definition 1.38. A rational map $\varphi : V_1 \longrightarrow \mathbb{P}^m(\mathbb{K})$, $\varphi = (\alpha_0, \dots, \alpha_m)$ is called *regular* (or *defined*) at $P \in V_1$ if there exists $\lambda \in \mathbb{K}(V_1)$ such that

- 1 each $\lambda\alpha_i$ is regular in P ;
- 2 for some $i_0 \in \{0, \dots, m\}$ $(\lambda\alpha_{i_0})(P) \neq 0$.

If such a λ exists, then $\varphi(P) := ((\lambda\alpha_0)(P) : \cdots : (\lambda\alpha_m)(P))$.

Note that for different points it may be necessary to consider different λ .

Definition 1.39. Given two projective varieties $V_1 \subseteq \mathbb{P}^n(\mathbb{K})$ and $V_2 \subseteq \mathbb{P}^m(\mathbb{K})$, a *rational map* from V_1 to V_2 ($\varphi : V_1 \longrightarrow V_2$) is a rational map φ of V_1 in $\mathbb{P}^m(\mathbb{K})$ such that, for each P where φ is regular, $\varphi(P) \in V_2$.

Definition 1.40. A rational map $\varphi : V_1 \longrightarrow V_2$ that is regular at each $P \in V_1$ is called *morphism* from V_1 to V_2 .

In a natural way it can be defined the composition of rational maps.

Definition 1.41. Let V_1, V_2 and V_3 be three projective varieties, let $\varphi = (\alpha_0 : \dots : \alpha_m)$ be a rational map of V_1 in V_2 and let $\psi = (\beta_0 : \dots : \beta_r)$ be a rational map of V_2 in V_3 . Let F_i, G_i be polynomials such that $\beta_i = \frac{F_i + I(V_2)}{G_i + I(V_2)}$, if $G_i(\alpha_0 : \dots : \alpha_m) \neq 0$ for each $i = 0, \dots, r$, set $\psi \circ \varphi = (\gamma_0 : \dots : \gamma_r)$ where $\gamma_i = \frac{F_i(\alpha_0, \dots, \alpha_m)}{G_i(\alpha_0, \dots, \alpha_m)}$. If $G_{i_0}(\alpha_0, \dots, \alpha_m) = 0$ for some i_0 , then $\psi \circ \varphi$ is not defined.

Definition 1.42. Let V_1 and V_2 be two projective varieties, a rational map $\phi : V_1 \longrightarrow V_2$ is called *birational* if there exists a rational map $\psi : V_2 \longrightarrow V_1$ such that $\psi \circ \phi = id_{V_1}$ and $\phi \circ \psi = id_{V_2}$. A birational map is called *isomorphism* if both ϕ and $\phi^{-1} := \psi$ are morphisms.

Definition 1.43. Two varieties V_1 and V_2 are said to be *birationally equivalent* (respectively *isomorphic*) if there exists a birational map (respectively an isomorphism) of V_1 in V_2 .

Definition 1.44. A rational map $\phi : V_1 \longrightarrow V_2$ is called *dominant* if there does not exist a proper algebraic subset of V_2 that contains the image set of ϕ .

Proposition 1.45. *The composition of two dominant rational maps is still a dominant rational map.*

To a dominant rational map between two projective varieties V_1 and V_2 it can be related a field homomorphism of $\mathbb{K}(V_2)$ in $\mathbb{K}(V_1)$.

First of all, note that, for a given projective variety V , there exists a bijection

$$h_V : \mathbb{K}(V) \longrightarrow \left\{ \varphi : V \longrightarrow \mathbb{P}^1(\mathbb{K}) \mid \varphi \text{ is a rational map and } \varphi \neq (0 : 1) \right\}$$

defined by $h_V(\alpha) = (0 : \alpha)$.

Definition 1.46. Let $\phi : V_1 \longrightarrow V_2$ be a dominant rational map and let $\beta \in \mathbb{K}(V_2)$. The *pull-back* of β by ϕ , denoted by $\phi^*(\beta)$, is defined as $\phi^*(\beta) = h_{V_1}^{-1}(h_{V_2}(\beta) \circ \phi)$.

Note that $\phi^*(\beta)$ is an element of $\mathbb{K}(V_1)$, in particular, if $\phi = (\alpha_0, \dots, \alpha_m)$ and $\beta = \frac{F + I(V_2)}{G + I(V_2)}$, then $\phi^*(\beta) = \frac{F(\alpha_0, \dots, \alpha_m)}{G(\alpha_0, \dots, \alpha_m)}$.

Proposition 1.47. *Let $\phi : V_1 \longrightarrow V_2$ be a dominant rational map, the pull-back $\phi^* : \mathbb{K}(V_2) \longrightarrow \mathbb{K}(V_1)$ is a non-trivial field homomorphism. Furthermore, if V_2 is not contained in the hyperplane H_0 , then $\phi = (1 : \alpha_1 : \cdots : \alpha_m)$ and ϕ^* is the unique field homomorphism of $\mathbb{K}(V_2)$ into $\mathbb{K}(V_1)$ that fixes $\mathbb{K}$ element by element and such that $\phi^*(\bar{x}_i) = \alpha_i \ \forall i = 1, \dots, m$, where $\bar{x}_i = \frac{X_i + I(V)}{X_0 + I(V)}$.*

Conversely, to a given field homomorphism $\gamma : \mathbb{K}(V_2) \longrightarrow \mathbb{K}(V_1)$ that fixes $\mathbb{K}$ element by element it can be related a dominant rational map $\phi : V_1 \longrightarrow V_2$ such that $\gamma = \phi^*$; indeed, suppose for simplicity that V_2 is not contained in H_0 , so $\mathbb{K}(V_2) = \mathbb{K}(\bar{x}_1, \dots, \bar{x}_m)$, then, as ϕ , it can be considered the rational map $(1 : \gamma(x_1) : \cdots : \gamma(x_n))$.

Proposition 1.48. *Let id_V be the identity of a projective variety V and let $\phi : V_1 \longrightarrow V_2$ and $\psi : V_2 \longrightarrow V_3$ be two dominant rational maps.*

1 $(id_V)^*$ is the identity automorphism of $\mathbb{K}(V)$;

2 $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.

Proposition 1.49. *Two varieties V_1 and V_2 are birationally equivalent if and only if the related function field $\mathbb{K}(V_1)$ and $\mathbb{K}(V_2)$ are $\mathbb{K}$ -isomorphic.*

Proposition 1.50. *Let $\phi : V_1 \longrightarrow V_2$, $\phi = (\alpha_0 : \cdots : \alpha_m)$, be a dominant rational map. Given $P \in V_1$ and $Q \in V_2$ the following conditions are equivalent:*

1 ϕ is defined at P and $\phi(P) = Q$;

2 $\mathbb{K}[V_1]_P \supseteq \phi^*(\mathbb{K}[V_2]_Q)$ and $M_P \supseteq \phi^*(M_Q)$.

Proposition 1.51. *Let $\phi : V_1 \longrightarrow V_2$ be an isomorphism between two projective varieties. For each $P \in V_1$ it holds that $\phi^*(\mathbb{K}[V_2]_{\phi(P)}) = \mathbb{K}[V_1]_P$ and $\phi^*(M_{\phi(P)}) = M_P$. In particular the local rings at P and at $\phi(P)$ are isomorphic.*

1.1.4 DVR of an algebraic curve

From now on, given an algebraic curve $\mathcal{X}$, a DVR (discrete valuation ring) of $\mathbb{K}(\mathcal{X})$ will be a DVR contained in $\mathbb{K}(\mathcal{X})$, that contains $\mathbb{K}$ and such that its field of fractions is $\mathbb{K}(\mathcal{X})$. From Proposition 1.18 it is known that for each non-singular point of $\mathcal{X}$ there exists a DVR of $\mathbb{K}(\mathcal{X})$, in general these are not all the possible DVR of the rational function field of a curve, more precisely the following theorem holds.

Theorem 1.52. *Let $\mathcal{O}$ be a DVR of $\mathbb{K}(\mathcal{X})$ and let M be the maximal ideal of $\mathcal{O}$. Then*

- 1 *there exists a unique point $P \in \mathcal{X}$ such that $\mathbb{K}[\mathcal{X}]_P \subseteq \mathcal{O}$, $\mathbb{K}[\mathcal{X}]_P \cap M = M_P$ and the point P is called the center of the DVR $\mathcal{O}$;*
- 2 *if P is a non singular point of $\mathcal{X}$, then $\mathbb{K}[\mathcal{X}]_P$ is the unique DVR of $\mathbb{K}(\mathcal{X})$ that is centered at P .*

Therefore for each $\mathcal{O}$ DVR of $\mathbb{K}(\mathcal{X})$ there exists a point that is its center, on the other hand, each point of a projective curve $\mathcal{X}$ is a center of at least one DVR of $\mathbb{K}(\mathcal{X})$, in particular it can be proved that a point P is the center of the DVR $\mathbb{K}[\mathcal{X}]_P$. Furthermore it can be proved that the number of DVR that are centered at a fixed point P is finite.

An important consequence of the previous theorem is that if $\mathcal{X}$ is a non-singular curve then the correspondence

$$P \longmapsto \mathbb{K}[\mathcal{X}]_P$$

defines a bijection between the set of points of $\mathcal{X}$ and the DVR of $\mathbb{K}(\mathcal{X})$.

The following results show how the pull-back of a rational map works on DVR of function fields of curves.

Proposition 1.53. *Let $\mathcal{X}$ and $\mathcal{Y}$ be two projective curves and let $\phi : \mathcal{X} \longrightarrow \mathcal{Y}$ be a non-constant dominant rational map. Then $\mathbb{K}(\mathcal{X}) : \phi^*(\mathbb{K}(\mathcal{Y}))$ is a finite field extension.*

Proposition 1.54. *Let $\phi : \mathcal{X} \longrightarrow \mathcal{Y}$ be a dominant rational map. Then for each $\mathcal{O}$ DVR of $\mathbb{K}(\mathcal{X})$ the ring $\hat{\phi}(\mathcal{O}) := (\phi^*)^{-1}(\mathcal{O} \cap \phi^*(\mathbb{K}(\mathcal{Y}))) \subseteq \mathbb{K}(\mathcal{Y})$ is a DVR of $\mathbb{K}(\mathcal{Y})$ whose maximal ideal $M_{\hat{\phi}(\mathcal{O})}$ is such that $M_{\hat{\phi}(\mathcal{O})} = (\phi^*)^{-1}(M_{\mathcal{O}} \cap \phi^*(\mathbb{K}(\mathcal{Y})))$ where $M_{\mathcal{O}}$ is the maximal ideal of $\mathcal{O}$.*

Proposition 1.55. *Let $\phi : \mathcal{X} \longrightarrow \mathcal{Y}$ be a dominant rational map, then, ϕ is regular at each non-singular point P of $\mathcal{X}$.*

Proposition 1.56. *Let P be a non-singular point of $\mathcal{X}$ and let Q be a point of $\mathcal{Y}$. Then $\phi(P) = Q$ if and only if $\hat{\phi}(\mathbb{K}[\mathcal{X}]_P)$ is a DVR of $\mathbb{K}(\mathcal{Y})$ centered at Q .*

Proposition 1.57. *Let $\mathcal{X}$ be a projective curve and let $\phi : \mathcal{X} \longrightarrow \mathbb{P}^m(\mathbb{K})$ be a non-constant rational map, then there exists a projective curve $\mathcal{Y} \subseteq \mathbb{P}^m(\mathbb{K})$ such that ϕ is a dominant rational map of $\mathcal{X}$ in $\mathcal{Y}$.*

1.1.5 Divisors, genus and Weierstrass semigroup of an algebraic curve

Throughout this subsection it will be considered a non-singular algebraic curve $\mathcal{X}$, hence the points of $\mathcal{X}$ and the DVR of $\mathbb{K}(\mathcal{X})$ will be identified. $\mathcal{P}$ will denote the set of DVR of $\mathbb{K}(\mathcal{X})$ and, based on what was said before, P will denote both a point of $\mathcal{X}$ or a DVR of $\mathbb{K}(\mathcal{X})$.

Definition 1.58. A *divisor* D of $\mathcal{X}$ is a finite formal sum of elements of $\mathcal{P}$, that is $D = \sum_{P \in \mathcal{P}} n_P P$, where $n_P \in \mathbb{N}$ for all $P \in \mathcal{P}$ and $n_P \neq 0$ just for a finite number of P . The set $\text{supp}(D) := \{P \in \mathcal{P} \mid, n_P \neq 0\}$ is called *support* of D and the *degree* of D is defined as $\deg(D) := \sum_{P \in \mathcal{P}} n_P$.

Let $D = \sum_{P \in \mathcal{P}} n_P P$ and $D' = \sum_{P \in \mathcal{P}} n'_P P$ it can be defined the sum $D + D'$ as $D + D' := \sum_{P \in \mathcal{P}} (n_P + n'_P) P$.

Proposition 1.59. The divisors of $\mathcal{X}$ form a group, that will be denoted by $\text{Div}(\mathcal{X})$, where the identity element is the divisor with all coefficients equal to zero.

It is possible to define a partial order relation on the group of divisors, that is, given two divisors $D = \sum_{P \in \mathcal{P}} n_P P$ and $D' = \sum_{P \in \mathcal{P}} n'_P P$

$$D \leq D' \iff n_P \leq n'_P \quad \forall P \in \mathcal{P}.$$

Definition 1.60. A divisor $D = \sum_{P \in \mathcal{P}} n_P P$ is called *positive* or *effective* if $n_P \geq 0$ for all $P \in \mathcal{P}$ and it will be denoted as $D \geq 0$.

Furthermore it is possible to relate a divisor to each rational function $f \in \mathbb{K}(\mathcal{X})$ that is

$$(f) := \sum_{P \in \mathcal{P}} \text{ord}_P(f) P$$

and this result to be the zero divisor if and only if f is a constant. The divisors of this type are called *principal divisors*. If f is non constant then the divisor (f) can be written as

$$(f) = (f)_0 - (f)_\infty$$

where

$$(f)_0 := \sum_{P \in \mathcal{P} \mid \text{ord}_P(f) > 0} \text{ord}_P(f) P$$

and

$$(f)_\infty := \sum_{P \in \mathcal{P} \mid \text{ord}_P(f) < 0} -\text{ord}_P(f)P$$

are two effective divisors respectively called *zero divisor of f* and *pole divisor of f* .

Definition 1.61. Two divisors D and D' are said to be *linearly equivalent* if there exists a rational function $f \in \mathbb{K}(\mathcal{X})$ such that $D - D' = (f)$.

Given a divisor D it can be defined a vector space related to D , denoted by $\mathcal{L}(D)$, that is

$$\mathcal{L}(D) := \{f \in \mathbb{K}(\mathcal{X}) \mid (f) + D \geq 0\} \cup \{0\}.$$

$\mathcal{L}(D)$ is called *Riemann-Roch space* of D and the dimension of $\mathcal{L}(D)$ is denoted by $\ell(D)$.

The main properties of the divisors of a curve $\mathcal{X}$ are summarized in the next proposition.

Proposition 1.62. 1 If two divisors D and D' are linearly equivalent, then the relative Riemann-Roch spaces $\mathcal{L}(D)$ and $\mathcal{L}(D')$ are isomorphic.

2 $\mathcal{L}(0) = \mathbb{K}$, where 0 denotes the divisor with all zero coefficients.

3 If D is an effective divisor, then $\ell(D) \leq \deg(D) + 1$.

4 If a divisor D can be written as $D = D_1 - D_2$, where D_1 and D_2 are two effective divisors, then $\ell(D) \leq \deg(D_1) + 1$.

5 Let $f \in \mathbb{K}(\mathcal{X}) \setminus \mathbb{K}$, then $\deg((f)_0) = [\mathbb{K}(\mathcal{X}) : \mathbb{K}(x)]$.

6 For all principal divisors the degree is zero.

7 Two linearly equivalent divisors have the same degree.

8 Let $D \in D_{\mathcal{X}}$ such that $\deg(D) < 0$, then $\mathcal{L}(D) = \{0\}$.

9 Let $D \in D_{\mathcal{X}}$ such that $\deg(D) \geq 0$, then $\ell(D) \leq \deg(D) + 1$.

At this point, the most important birational invariant of algebraic curves can be introduced, that is the genus of a curve.

Theorem 1.63 (Riemann's Theorem). *There exists a non-negative integer γ , which depends only on $\mathcal{X}$, such that for each $D \in D_{\mathcal{X}}$ $\ell(D) \geq \deg(D) + 1 - \gamma$ holds.*

Definition 1.64. The *genus* g of a curve $\mathcal{X}$ is defined as

$$g := \max \{ \deg(D) - \ell(D) + 1 \mid D \text{ is a divisor of } \mathbb{K}(\mathcal{X}) \}.$$

It trivially follows that the genus of a curve is a non-negative integer.

Theorem 1.65. *Let $\mathcal{X}$ be an algebraic curve of genus g , then there exists an integer $c(\mathcal{X})$, depending only on $\mathbb{K}(\mathcal{X})$, such that for each $D \in D_{\mathcal{X}}$ with $\deg(D) \geq c(\mathcal{X})$ $\ell(D) = \deg(D) + 1 - g$ holds.*

In the special case of non-singular plane curves, the genus is completely determined by the order (that is the degree) of the curve.

Lemma 1.66. *Let $\beta \in \mathbb{K}(\mathcal{X})$, if β is defined at each point of $\mathcal{X}$ then β is polynomial.*

Theorem 1.67. *Let $\mathcal{X} = V(\langle F(X_0, X_1, X_2) \rangle)$ be a non-singular plane projective algebraic curve of order d and genus g . Then*

$$g = \frac{(d-1)(d-2)}{2}.$$

To each point P of a non-singular curve $\mathcal{X}$ can be associated a semigroup and in order to introduce it, a special class of divisors must be taken into account, that is the class of *one-point* divisors. A one-point divisor D is a divisor of the form $D = mP$ where P is a point of $\mathcal{X}$ and m is a positive integer. For this type of divisors the Riemann-Roch space can be written as follows

$$\mathcal{L}(mP) = \{ f \in \mathbb{K}(\mathcal{X}) \mid (f)_{\infty} = lP \text{ with } l \leq m \}.$$

Definition 1.68. The set of non-negative integers

$$H(P) := \{ l \mid \exists f \in \mathbb{K}(\mathcal{X}) \text{ with } (f)_{\infty} = lP \}$$

is trivially a semigroup with respect to the sum and it is called *Weierstrass semigroup at P* . Furthermore the elements of $H(P)$ are called *non-gaps of P* , whereas the elements of $\mathbb{N} \setminus H(P)$ are called *gaps of P* .

The main results about the Weierstrass semigroups are summarized in the next proposition.

Proposition 1.69. *Let P be a point of $\mathcal{X}$. Then*

- 1 *An integer i is a non-gap at P if and only if $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$.*
- 2 *An integer i is a non-gap at P if and only if $\ell((i-1)P) = \ell(iP) - 1$.*
- 3 *The dimension of $\mathcal{L}(mP)$ coincides with the number of non-gaps at P that are smaller than or equal to m .*
- 4 *Let $i_0 = 0, i_1, \dots, i_r$ be all the non-gaps at P that are smaller than or equal to m and let $f_0, \dots, f_r \in \mathbb{K}(\mathcal{X})$ be rational functions such that $(f_j)_\infty = i_j P$. Then $\{f_0, \dots, f_r\}$ is a basis of $\mathcal{L}(mP)$.*
- 5 *The number of gaps at each point of $\mathcal{X}$ coincides with the genus of $\mathcal{X}$.*
- 6 *If the genus of $\mathcal{X}$ is greater than or equal to 1 then there exists at least one gap at each point P of $\mathcal{X}$ and 1 is a gap at each P .*
- 7 *If i is an integer greater than or equal to two times the genus of $\mathcal{X}$ then i is a non-gap at each point P of $\mathcal{X}$.*

Corollary 1.70. *Let D be a one-point divisor. If $\deg(D) \geq 2g - 1$, then $\ell(D) = \deg(D) - g + 1$.*

In order to define another particular type of divisors it is useful to introduce a new object: the differentials. Let R be a commutative ring which contains $\mathbb{K}$ and let F be the free R -module generated by the elements $[x]$ with $x \in R$, where $[x]$ is just a symbol associated to the element x ; then an element of F is of the type $\sum a_i [x_i]$ with $a_i \in R$. Let N be submodule of F generated by these sets: $\{[x+y] - [x] - [y] \mid x, y \in R\}$, $\{[\lambda x] - \lambda[y] \mid \lambda \in \mathbb{K}, x \in R\}$ and $\{[xy] - x[y] - y[x] \mid x, y \in R\}$ and let $\Omega_K(R)$ be the quotient module F/N .

Definition 1.71. $\Omega_K(R)$ is called *module of differentials of R over $\mathbb{K}$* .

The image in F/N of the element $[x] \in F$ is denoted by dx and it can be considered the map $d : R \longrightarrow \Omega_K(R)$ which maps x to dx . The differentials can be also related to algebraic curves and their function fields. Assume $R = \mathbb{K}[x_1, \dots, x_n]$, it can be proved that the R -module $\Omega_K(R)$ is generated by the differentials $dx_1, \dots, dx_n$; furthermore if $L = \mathbb{K}(x_1, \dots, x_n)$ it can be proved that $\Omega_K(L)$ is generated, as L -vector space, by the differentials $dx_1, \dots, dx_n$.

Proposition 1.72. *Let $L = \mathbb{K}(\mathcal{X})$, then $\Omega_K(L)$ is non trivial and*

- (1) if $x \in \mathbb{K}(\mathcal{X}) \setminus \mathbb{K}$ is such that $\mathbb{K}(\mathcal{X}) : \mathbb{K}(x)$ is separable then $dx \neq 0$;
- (2) if $t \in \mathbb{K}(\mathcal{X})$ is a local parameter then $dt \neq 0$.

Proposition 1.73. *Let $L = \mathbb{K}(\mathcal{X})$, then $\Omega_K(L)$ is a vector space over L of dimension 1.*

From this proposition it follows that, if x is a separating element or a local parameter, then for all $\alpha \in \mathbb{K}(\mathcal{X})$ there exists a unique $v \in \mathbb{K}(\mathcal{X})$ such that $d\alpha = vdx$, such v is called *derivative of α with respect to x* and it will be denoted by $v = d\alpha/dx$. By this way it is possible to define the order of a differential at a DVR of $\mathbb{K}(\mathcal{X})$.

Definition 1.74. Let $\omega \in \Omega_K(R)$, $\omega \neq 0$, let P be a DVR of $\mathcal{X}$ and let t be a local parameter of P . Let α be the unique element of $\mathbb{K}(\mathcal{X})$ such that $\omega = \alpha dt$, then the *order of ω at P* is define as $\text{ord}_P(\omega) = \text{ord}_P(\alpha)$.

It can be trivially proved that this definition does not depend on the choice of the local parameter t .

Proposition 1.75. *Let O be a DVR of $\mathbb{K}(\mathcal{X})$ and let t be a local parameter of O . If $\alpha \in O$ then $\frac{d\alpha}{dt} \in O$.*

Proposition 1.76. *Each local parameter is separating in $\mathbb{K}(\mathcal{X})$.*

Lemma 1.77. *Let $\omega \in \Omega_K(\mathbb{K}(\mathcal{X}))$, $\omega \neq 0$, then $\text{ord}_P(\omega) \neq 0$ at most for a finite number of DVR P of $\mathbb{K}(\mathcal{X})$.*

Also to a differential it can be associated a divisor, in particular, if $\omega \in \Omega_K(\mathbb{K}(\mathcal{X}))$, $\omega \neq 0$, the divisor associated to ω , denoted by $\text{div}(\omega)$, is defined as $\text{div}(\omega) = \sum_{P \in \mathcal{P}} \text{ord}_P(\omega)P$.

Definition 1.78. Let $\omega \in \Omega_K(\mathbb{K}(\mathcal{X}))$, $\omega \neq 0$, then $W = \text{div}(\omega)$ is called *canonical divisor* of $\mathbb{K}(\mathcal{X})$.

Proposition 1.79. *Two canonical divisors differ by a principal divisor.*

Proposition 1.80. *A divisor which differs from a canonical divisor by a principal divisor is canonical.*

Assume now that $\mathcal{X}$ is a non-singular plane curve and that it is not the line $X_0 = 0$. Let $f(X, Y) = 0$, with $\deg(f) = d \geq 3$, be an equation of $\mathcal{X}$. Suppose that $X + \langle f \rangle \neq 0$ is a separating element in $\mathbb{K}(x, y)$ and that the points of $\mathcal{X}$ on the line $X_0 = 0$ are d distinct points $P_1, \dots, P_d$.

Proposition 1.81. *The divisor $\overline{W} = (d - 3)(P_1 + \cdots + P_d)$ is a canonical divisor.*

Theorem 1.82. *Let $\mathcal{X}$ be a curve of genus g . The degree of a canonical divisor W is $2g - 2$ and $\ell(W) \geq g$*

Theorem 1.83. *Let $\mathcal{X}$ be a plane curve, let $P_1, \dots, P_r$ be the singular points of $\mathcal{X}$. If each P_i is ordinary, then*

$$g = \frac{(d-1)(d-2)}{2} - \sum_{i=1}^r \frac{r_i(r_i-1)}{2}$$

where r_i denotes the multiplicity of P_i .

Theorem 1.84 (Riemann-Roch Theorem). *Let D be a divisor of an algebraic curve $\mathcal{X}$,*

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

where W is an arbitrary canonical divisor.

In general, the computation of $\ell(W - D)$ is non trivial, but, if the degree of D is sufficiently large, then $\ell(W - D) = 0$.

Corollary 1.85. *If D is a divisor such that $\deg(D) \geq 2g - 1$, then $\ell(D) = \deg(D) + 1 - g$.*

Lemma 1.86. *If D is a divisor such that $\deg(D) = 0$, then $\ell(D) \leq 1$.*

The genus and the automorphism group of a curve are two of the most important birational invariants of a curve. Another birational invariant can be defined through the group of divisors in the following way. Let

$$\text{Div}^0(\mathcal{X}) = \left\{ \sum_{P \in \mathcal{X}} n_P P \mid \sum_{P \in \mathcal{X}} n_P = 0 \right\},$$

that is the group of divisors of $\mathcal{X}$ of degree zero; it can be proved that the principal divisors

$$\text{Princ}(\mathcal{X}) = \{(f) \mid f \in \mathbb{K}(\mathcal{X})^*\}$$

form a subgroup of $\text{Div}^0(\mathcal{X})$.

Definition 1.87. The *Picard group* of $\mathcal{X}$, denoted by $\text{Pic}^0(\mathcal{X})$, is the factor group $\text{Pic}^0(\mathcal{X}) = \text{Div}^0(\mathcal{X}) / \text{Princ}(\mathcal{X})$.

Definition 1.88. Let ℓ be a prime, then

$$\mathrm{Pic}^0(\mathcal{X})[\ell] := \{x \in \mathrm{Pic}^0(\mathcal{X}) \mid \ell x = 0\}.$$

Theorem 1.89. *The following claims hold:*

- $\mathrm{Pic}^0(\mathcal{X})[\ell]$ is finite;
- if $\mathrm{char}(\mathbb{K}) \neq \ell$ then $|\mathrm{Pic}^0(\mathcal{X})[\ell]| = \ell^{2g}$ and $\mathrm{Pic}^0(\mathcal{X})[\ell]$ is isomorphic to the elementary abelian group $\mathbb{Z}_\ell^{2g}$;
- if $\mathrm{char}(\mathbb{K}) = \ell$ then $|\mathrm{Pic}^0(\mathcal{X})[\ell]| = \ell^\gamma$ with $\gamma \leq g$ and $\mathrm{Pic}^0(\mathcal{X})[\ell]$ is isomorphic to the elementary abelian group $\mathbb{Z}_\ell^\gamma$.

Definition 1.90. The integer γ of Theorem 1.89 is called *p-rank* or *Hasse-Witt invariant* of $\mathcal{X}$.

1.1.6 Coverings

Let $\Phi : \mathcal{X} \rightarrow \mathcal{Y}$ be a non constant rational map and let $\Phi^* : \mathbb{K}(\mathcal{Y}) \rightarrow \mathbb{K}(\mathcal{X})$ be its pull-back.

Definition 1.91. Let O be a DVR of $\mathbb{K}(\mathcal{X})$ and let O' be the DVR of $\mathbb{K}(\mathcal{Y})$ such that $\Phi^*(O') = O \cap \Phi^*(\mathbb{K}(\mathcal{Y}))$, that is the unique DVR of $\mathbb{K}(\mathcal{X})$ such that $\Phi^*(O') \subseteq O$ (this will also be denoted by $O|O'$). We will say that O' is *covered* by O .

Remark 1.92. If $O = \mathbb{K}[\mathcal{X}]_P$ and $O' = \mathbb{K}[\mathcal{Y}]_Q$ with P and Q non-singular points, then the condition O' covered by O is equivalent to $\Phi(P) = Q$.

Lemma 1.93. Let O be a DVR of $\mathbb{K}(\mathcal{X})$ and let O' be the DVR of $\mathbb{K}(\mathcal{Y})$ such that $\Phi^*(O') = O \cap \Phi^*(\mathbb{K}(\mathcal{Y}))$. There exists a positive integer, denoted by e_O , such that, for each $\alpha \in \mathbb{K}(\mathcal{Y})$, $\mathrm{ord}_O(\Phi^*(\alpha)) = e_O \cdot \mathrm{ord}_{O'}(\alpha)$.

Definition 1.94. The integer e_O is called *ramification index* of O over O' . If $e_O > 1$ we will say that $O|O'$ is *ramified*.

Proposition 1.95. For each DVR O' of $\mathbb{K}(\mathcal{Y})$ there exists at least one, and in any case a finite number of DVR O of $\mathbb{K}(\mathcal{X})$ such that $\Phi^*(O') \subset O$.

Theorem 1.96 (Fundamental equality). Let $n = [\mathbb{K}(\mathcal{X}) : \Phi^*(\mathbb{K}(\mathcal{Y}))]$, let O' be a DVR of $\mathbb{K}(\mathcal{Y})$ and let $O_1, \dots, O_m$ be the DVR of $\mathbb{K}(\mathcal{X})$ such that $O_i|O'$. Then $n = \sum_{i=1}^m e_{O_i}$.

Lemma 1.97. *For each $\alpha, x \in \mathbb{K}(\mathcal{Y})$ with $dx \neq 0$ we have*

$$d\alpha = udx \text{ in } \Omega_K(\mathbb{K}(\mathcal{Y})) \implies d\Phi^*(\alpha) = \Phi^*(u)d\Phi^*(x) \text{ in } \Omega_K(\mathbb{K}(\mathcal{X})).$$

Corollary 1.98. *Let $\Phi : \mathcal{X} \longrightarrow \mathcal{Y}$ be a separable rational map. If $\alpha \in \mathbb{K}(\mathcal{Y})$ is such that $d\alpha \neq 0$ in $\Omega_K(\mathbb{K}(\mathcal{Y}))$, then $d(\Phi^*(\alpha)) \neq 0$ in $\Omega_K(\mathbb{K}(\mathcal{X}))$.*

Now we are ready to state and prove a key theorem about coverings, that is the Riemann-Hurwitz theorem.

Theorem 1.99 (Riemann-Hurwitz Theorem). *Let $\mathcal{X}$ and $\mathcal{Y}$ be two projective algebraic curves. Let g be the genus of $\mathcal{X}$ and let g' be the genus of $\mathcal{Y}$. Let $\Phi : \mathcal{X} \longrightarrow \mathcal{Y}$ be a non-constant, separable, rational map of degree n . Then*

$$2g - 2 = n(2g' - 2) + \text{Diff}$$

where

$$\text{Diff} = \sum_{O \in \mathcal{P}} \text{ord}_O \frac{d\Phi^*(t')}{dt}$$

with t (respectively t') local parameter in O (respectively O').

Proof. Let x be a separating element for $\mathbb{K}(\mathcal{Y})$ (then $\Phi^*(x)$ is a separating element for $\mathbb{K}(\mathcal{X})$). Then

$$\begin{aligned} 2g - 2 &= \sum_{O \in \mathcal{P}} \text{ord}_O d(\Phi^*(x)) = \sum_{O \in \mathcal{P}} \text{ord}_O \left(\frac{d(\Phi^*(x))}{dt_O} \right) = \\ &= \sum_{O \in \mathcal{P}} \text{ord}_O \left(\frac{d(\Phi^*(x))}{d(\Phi^*(t_{O'}))} \frac{d(\Phi^*(t_{O'}))}{dt_O} \right) = \\ &= \sum_{O \in \mathcal{P}} \text{ord}_O \left(\frac{d(\Phi^*(x))}{d(\Phi^*(t_{O'}))} \right) + \sum_{O \in \mathcal{P}} \text{ord}_O \left(\frac{d(\Phi^*(t_{O'}))}{dt_O} \right) = \\ &= \sum_{O \in \mathcal{P}} \text{ord}_O \left(\frac{d(\Phi^*(x))}{d(\Phi^*(t_{O'}))} \right) + \text{Diff} \end{aligned}$$

where t_O (respectively $t_{O'}$) is a local parameter of O (respectively O') in $\mathbb{K}(\mathcal{X})$ (respectively $\mathbb{K}(\mathcal{Y})$). Note that, since $dt_{O'} \neq 0$, then $d(\Phi^*(t_{O'})) \neq 0$. Recall that $\frac{d(\Phi^*(x))}{d(\Phi^*(t_{O'}))}$ is the pull back of $dx/dt_{O'}$. We have

$$\begin{aligned} \sum_{O \in \mathcal{P}} \text{ord}_O \left(\frac{d(\Phi^*(x))}{d(\Phi^*(t_{O'}))} \right) &= \sum_{O' \in \mathcal{P}'} \sum_{\substack{O \in \mathcal{P} \\ O|O'}} \text{ord}_O \left(\frac{d(\Phi^*(x))}{d(\Phi^*(t_{O'}))} \right) = \\ &= \sum_{O' \in \mathcal{P}'} \sum_{\substack{O \in \mathcal{P} \\ O|O'}} \text{ord}_{O'} \left(\frac{dx}{dt_{O'}} \right) e_O = n \cdot \deg(\text{div}(dx)) = n(2g' - 2) \end{aligned}$$

where $\mathcal{P}'$ is the set of DVR of $\mathbb{K}(\mathcal{Y})$. Hence

$$2g - 2 = n(2g' - 2) + \text{Diff}.$$

□

When the characteristic of $\mathbb{K}$ is 0 or it does not divide any ramification index, the integer Diff has a simpler expression.

Proposition 1.100. *Let t (respectively t') be a local parameter in O (respectively O'), then $\text{ord}_O\left(\frac{d\Phi^*(t')}{dt}\right) \geq e_O - 1$. Furthermore, if $\text{char}(\mathbb{K}) = 0$ or it does not divide e_O for every $O \in \mathcal{P}$, then $\text{ord}_O\left(\frac{d\Phi^*(t')}{dt}\right) = e_O - 1$.*

As a direct consequence, also the Riemann-Hurwitz formula has a simpler expression.

Corollary 1.101. *If $\text{char}(\mathbb{K}) = 0$ or it does not divide e_O for every $O \in \mathcal{P}$, then*

$$2g - 2 = n(2g' - 2) + \sum_{O \in \mathcal{P}} (e_O - 1).$$

Corollary 1.102. *Let $\Phi : \mathcal{X} \rightarrow \mathcal{Y}$ be a non constant separable rational map. Let $n = [\mathbb{K}(\mathcal{X}) : \Phi^*(\mathbb{K}(\mathcal{Y}))]$. Then for each O' DVR of $\mathbb{K}(\mathcal{Y})$, except possibly finitely many, $\#\{O \text{ DVR of } \mathbb{K}(\mathcal{X}) \mid O|O'\} = n$ holds.*

Now, recall that, for each $M : L$ finite and separable extension, it can be defined the group

$$\Gamma(M, L) = \{\sigma : M \rightarrow M \mid \sigma \text{ is an automorphism, } \sigma(l) = l \forall l \in L\}.$$

In general we have that $|\Gamma(M, L)| \leq [M : L]$, the extension is called *Galois extension* if $|\Gamma(M, L)| = [M : L]$.

Let $\Phi : \mathcal{X} \rightarrow \mathcal{Y}$ be a non constant rational map and let $\Phi^* : \mathbb{K}(\mathcal{Y}) \rightarrow \mathbb{K}(\mathcal{X})$ be its pull-back. We denote by $\Gamma(\mathcal{X}, \mathcal{Y}) = \Gamma(\mathbb{K}(\mathcal{X}), \Phi^*(\mathbb{K}(\mathcal{Y})))$, that is

$$\Gamma(\mathcal{X}, \mathcal{Y}) = \{\sigma : \mathbb{K}(\mathcal{X}) \rightarrow \mathbb{K}(\mathcal{X}) \mid \sigma \text{ automorphism, } \sigma(\alpha) = \alpha \forall \alpha \in \Phi^*(\mathbb{K}(\mathcal{Y}))\}.$$

Definition 1.103. A rational map $\Phi : \mathcal{X} \rightarrow \mathcal{Y}$ is called a *Galois map* if the extension $\mathbb{K}(\mathcal{X}) : \Phi^*(\mathbb{K}(\mathcal{Y}))$ is a Galois extension, that is if $\mathbb{K}(\mathcal{X}) : \Phi^*(\mathbb{K}(\mathcal{Y}))$ is separable and $|\Gamma(\mathcal{X}, \mathcal{Y})|$ is equal to the degree of Φ . If Φ is a Galois rational map, $\mathcal{Y}$ is called *quotient curve* of $\mathcal{X}$ with respect to the group $\Gamma(\mathcal{X}, \mathcal{Y})$.

On the other hand each finite group of automorphism of $\mathbb{K}(\mathcal{X})$ is $\Gamma(\mathcal{X}, \mathcal{Y})$ for a suitable Galois map $\Phi : \mathcal{X} \longrightarrow \mathcal{Y}$.

Theorem 1.104. *Let G be a finite group of $\mathbb{K}$ -automorphism of $\mathbb{K}(\mathcal{X})$. Let $L = \{\alpha \in \mathbb{K}(\mathcal{X}) \mid \sigma(\alpha) = \alpha \ \forall \sigma \in G\}$. Then the extension $\mathbb{K}(\mathcal{X}) : L$ is a Galois extension and $\Gamma(\mathbb{K}(\mathcal{X}), L) = G$.*

Corollary 1.105. *The quotient curves of $\mathcal{X}$ are in bijection with the finite subgroups of automorphisms of $\mathbb{K}(\mathcal{X})$.*

For a given finite group of automorphism of $\mathbb{K}(\mathcal{X})$, say G , the quotient curve of $\mathcal{X}$ with respect to the Galois covering induced by G will be denoted by $\mathcal{X}/G$.

Lemma 1.106. *Let O be a DVR of $\mathbb{K}(\mathcal{X})$, let O' be a DVR of $\mathbb{K}(\mathcal{Y})$ such that $O|O'$ and let $\sigma \in \Gamma(\mathcal{X}, \mathcal{Y})$. Then*

- (1) $\sigma(O)$ is a DVR of $\mathbb{K}(\mathcal{X})$;
- (2) $\text{ord}_{\sigma(O)}(\alpha) = \text{ord}_O((\sigma^{-1})(\alpha))$;
- (3) $\sigma(O)|O$;
- (4) $e_{\sigma(O)} = e_O$.

Lemma 1.107. *Let $\mathbb{K}(\mathcal{X}) : \Phi^*(\mathbb{K}(\mathcal{Y}))$ be a Galois extension. Then*

$$\Phi^*(\mathbb{K}(\mathcal{Y})) = \{\alpha \in \mathbb{K}(\mathcal{X}) \mid \sigma(\alpha) = \alpha \ \forall \sigma \in \Gamma(\mathcal{X}, \mathcal{Y})\}.$$

Theorem 1.108. *Let $\Phi : \mathcal{X} \longrightarrow \mathcal{Y}$ be a Galois map. Let O' be a DVR of $\mathbb{K}(\mathcal{Y})$ and let O_1 and O_2 be DVR of $\mathbb{K}(\mathcal{X})$ such that $O_1|O'$ and $O_2|O'$. Then there exists $\sigma \in \Gamma(\mathcal{X}, \mathcal{Y})$ such that $O_2 = \sigma(O_1)$.*

Corollary 1.109. *Let $\Phi : \mathcal{X} \longrightarrow \mathcal{Y}$ be a Galois map of degree n and let O be a DVR of $\mathbb{K}(\mathcal{X})$. Then e_O coincides with the size of the stabilizer of O in $\Gamma(\mathcal{X}, \mathcal{Y})$.*

Let us denote by $\Gamma(\mathcal{X}, \mathcal{Y})_O$ the stabilizer of O in $\Gamma(\mathcal{X}, \mathcal{Y})$, by Corollary 1.101 and Corollary 1.109, in the case where the characteristic of $\mathbb{K}$ does not divide the order of the stabilizer of any point, the genus of the quotient curve $\mathcal{Y}$ is completely determined by the action of the group $\Gamma(\mathcal{X}, \mathcal{Y})$ on the set of DVR of $\mathbb{K}(\mathcal{X})$. Whereas, in the general case, the different depends on the so called higher ramification subgroups of $|\Gamma(\mathcal{X}, \mathcal{Y})|$.

Definition 1.110. Let $O|O'$ and let t be a local parameter at O . Then, for each integer $i \geq 0$

$$\Gamma(\mathcal{X}, \mathcal{Y})_i(O|O') = \{\sigma \in \Gamma(\mathcal{X}, \mathcal{Y}) \mid \text{ord}_O(\sigma(t) - t) \geq i + 1\}$$

is called *i-th ramification subgroup of $O|O'$* .

This definition does not depend on the choice of t .

Theorem 1.111 (Hilbert's Different Theorem). *Let $\phi : \mathcal{X} \rightarrow \mathcal{Y}$ be a Galois rational map. Let $O|O'$ and let t (respectively t') be a local parameter at O (respectively O'). Then*

$$\text{ord}_O \frac{d\phi^*(t')}{dt} = \sum_{i=0}^{\infty} (|\Gamma(\mathcal{X}, \mathcal{Y})_i(O|O')| - 1).$$

1.2 Automorphism groups of algebraic curves

In this section we collect some useful results about the automorphism groups of algebraic curves.

From now on we will denote by $\text{Aut}(\mathcal{X})$ the automorphism group of $\mathcal{X}$. With a slight abuse of notation, automorphisms of $\mathcal{X}$ will be identified with $\mathbb{K}$ -automorphisms of the function field $\mathbb{K}(\mathcal{X})$. If G is a finite subgroup of $\text{Aut}(\mathcal{X})$, we will consider the Galois extension $\mathbb{K}(\mathcal{X})$ over the fixed field of G . If P is a simple point of $\mathcal{X}$, then P will be identified with the DVR consisting of the rational functions defined at P . When this point of view is adopted, we will denote the i -th ramification group of $\mathcal{X}$ at P by $G_P^{(i)}$; according to Definition 1.110, for t a local parameter at P we have

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

Here, $G_P^{(0)} = G_P$. The structure of G_P is well understood; see, for example, [59, Chapter IV, Corollary 4] or [32, Theorem 11.49, Theorem 11.60].

Theorem 1.112. *The stabilizer G_P of a point $P \in \mathcal{X}$ in G has the following properties:*

- (i) $G_P^{(1)}$ is the unique Sylow p -subgroup of G_P ;
- (ii) For $i \geq 1$, $G_P^{(i)}$ is a normal subgroup of G_P and the quotient group $G_P^{(i)} / G_P^{(i+1)}$ is an elementary abelian p -group;

(iii) $G_P = G_P^{(1)} \rtimes U$, where U is a cyclic group whose order is prime to p .

A subgroup of $\text{Aut}(\mathcal{X})$ is a p' -group (or a prime-to- p group) if its order is prime to p . A subgroup G of $\text{Aut}(\mathcal{X})$ is *tame* if the stabilizer of any point in G is a p' -group. Otherwise, G is *non-tame* (or *wild*). Whereas every p' -subgroup of $\text{Aut}(\mathcal{X})$ is tame, the converse is not always true.

If a curve has genus 0 it is called *rational* and its automorphism group is isomorphic to $\text{PGL}(2, \mathbb{K})$. The following result is a consequence of Dickson's classification of finite subgroups of $\text{PGL}(2, \mathbb{K})$ (see [13]; also [32, Theorem 11.91]).

Proposition 1.113. *Any non-trivial tame automorphism of a rational curve that fixes a point has exactly two fixed points.*

We will also use additional information on automorphisms of elliptic curves, i.e. curves of genus 1. Let $\mathcal{E}$ be a non-singular plane cubic curve viewed as a birational model of an elliptic curve. For an inflection point O of $\mathcal{E}$, the set of points of $\mathcal{E}$ can be equipped by an operation $\oplus$ to form an abelian group G_O with zero-element O , which is isomorphic to the zero Picard group of $\mathcal{E}$; see for instance [32, Theorem 6.107]. The translation τ_P associated with $P \in \mathcal{E}$ is the permutation on the points of $\mathcal{E}$ with equation $\tau_P : X \mapsto X \oplus P$. Since there exists an automorphism in $\text{Aut}(\mathcal{E})$ which acts on $\mathcal{E}$ as τ_P does, translations of $\mathcal{E}$ can be viewed as elements of $\text{Aut}(\mathcal{E})$. They form the translation group T of $\mathcal{E}$ which acts faithfully on $\mathcal{E}$ as a sharply transitive permutation group. For every prime r , the elements of order r in T are called r -torsion points. They together with the identity form an elementary abelian r -group of rank k . Here $k = 2$ for $r \neq p$, whereas k equals the p -rank of $\mathcal{E}$ for $r = p$, that is, $k = 0, 1$ according as $\mathcal{E}$ is supersingular or ordinary.

Proposition 1.114. *If $\mathcal{E}$ is an elliptic curve, the translation group T is a normal subgroup of $\text{Aut}(\mathcal{E})$, and $\text{Aut}(\mathcal{E}) = T \rtimes \text{Aut}(\mathcal{E})_P$ for every $P \in \mathcal{E}$.*

Concerning automorphisms of elliptic curves fixing a point, the following result holds.

Theorem 1.115 ([61, Theorem 10.1], [32, Theorem 11.94]). *Let $\mathcal{E}$ be an elliptic curve. If G is a subgroup of $\text{Aut}(\mathcal{E})$ and $P \in \mathcal{E}$, then*

$$|G_P| = \begin{cases} 2, 4, 6 & \text{when } p \neq 2, 3, \\ 2, 4, 6, 12 & \text{when } p = 3, \\ 2, 4, 6, 8, 12, 24 & \text{when } p = 2. \end{cases} \quad (1.1)$$

Proposition 1.116. *Let $\mathcal{E}$ be an elliptic curve defined over a field of characteristic $p > 2$, and let α be an automorphism of $\mathcal{E}$ of finite order $o(\alpha)$.*

- (a) *If $o(\alpha) = p^h$, then either $\mathcal{E}$ is not ordinary, $p^h = 3$, and α does not act semiregularly on $\mathcal{E}$, or $\mathcal{E}$ is ordinary and α acts semiregularly on $\mathcal{E}$.*
- (b) *If $(o(\alpha), p) = 1$ and α does not act semiregularly on $\mathcal{E}$, then α has order in $\{2, 3, 4, 6\}$. Specifically:*
 - *If $o(\alpha) = 2$, then α fixes 4 points and acts semiregularly on the other points of $\mathcal{E}$.*
 - *If $o(\alpha) = 3$, then α fixes 3 points and acts semiregularly on the other points of $\mathcal{E}$.*
 - *If $o(\alpha) = 4$, then α fixes 2 points, and the only other short orbit has size 2.*
 - *If $o(\alpha) = 6$, then α fixes 1 point, and the only other short orbits are two orbits of sizes 2 and 3.*

Proof. (a) If $\mathcal{E}$ is not ordinary, then $\langle \alpha \rangle$ fixes a point and acts semiregularly on the other points. By [32, Theorem 11.94], we have $h = 1$ and $p = 3$.

Assume now that $\mathcal{E}$ is ordinary. Then, by Proposition 1.115, $\langle \alpha \rangle T / T \cong \langle \alpha \rangle / (\langle \alpha \rangle \cap T)$ is either trivial or a p -group and is isomorphic to a subgroup of the stabilizer of O . Note that p does not divide the size of the stabilizer of O ; this follows directly from [32, Theorem 11.94] for $p > 3$. For $p = 3$, it can be checked that 3 divides the size of the stabilizer of O only if the curve is not ordinary. Therefore, $\langle \alpha \rangle = \langle \alpha \rangle \cap T$ and α belongs to T , acting semiregularly on $\mathcal{E}$.

- (b) Let $m = o(\alpha)$. Since α does not act semiregularly on $\mathcal{E}$, the genus of the quotient curve $\mathcal{E} / \langle \alpha \rangle$ is 0. Applying the Riemann-Hurwitz genus formula for the group generated by α , with $\Omega_1, \dots, \Omega_n$ denoting the short orbits under the action of α , we have:

$$0 = -2m + \sum_{i=1}^n (m - |\Omega_i|) \geq -2m + \frac{m}{2}n.$$

Thus, $3 \leq n \leq 4$. If $n = 3$, then:

$$m = |\Omega_1| + |\Omega_2| + |\Omega_3|.$$

Considering the equation $\frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} = 1$, where e_i is the size of the stabilizer of a point in Ω_i and assuming $e_1 \leq e_2 \leq e_3$, and using [32, Theorem 11.94], the possible values for e_i are $\{2, 3, 4, 6\}$. If $e_i = 3$ or 6 for some i , then $p > 3$. The only possibilities are:

- $e_1 = 2, e_2 = e_3 = 4$; hence, $4 \mid m$, and an element of order 2 in $\langle \alpha \rangle$ fixes m points. By [32, Lemma 11.107], we get $m = 4$.
- $e_1 = e_2 = e_3 = 3$; hence, $3 \mid m$, and an element of order 3 in $\langle \alpha \rangle$ fixes m points. By [32, Lemma 11.106], this implies $m = 3$.
- $e_1 = 2, e_2 = 3, e_3 = 6$; hence, $6 \mid m$, and the elements of orders 2, 3, and 6 in α fix $\frac{2m}{6}, \frac{m}{3} + \frac{m}{6},$ and $\frac{m}{6}$ points respectively. By [32, Lemma 11.106], this implies $m = 6$.

If $n = 4$, then:

$$2m = |\Omega_1| + |\Omega_2| + |\Omega_3| + |\Omega_4|.$$

The only possibility is $|\Omega_i| = m/2$ for each i , and hence the element of order 2 in α fixes $2m$ points. By [32, Lemma 11.107], this implies $m = 2$. $\square$

We need the following corollary to Theorem 1.5 from [49]. Although stated for the algebraic closure of a finite field, this result holds for every algebraically closed field of positive characteristic p .

Proposition 1.117. *Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) = q - 1$, where q is a power of p . If $\text{Aut}(\mathcal{X})$ contains an elementary abelian subgroup E_q of order q , then, up to birational equivalence over $\mathbb{K}$, one of the following holds:*

(a) $\mathcal{X}$ has an affine equation

$$L_1(y) = ax + \frac{1}{x},$$

where $a \in \mathbb{K}^*$ and $L_1(T) \in \mathbb{K}[T]$ is a separable p -linearized polynomial of degree q . Furthermore, $\mathcal{X}$ is ordinary and $|\text{Aut}(\mathcal{X})| = 4q$.

(b) If $p \neq 3$, then $\mathcal{X}$ has an affine equation

$$L_2(y) = x^3 + bx,$$

where $b \in \mathbb{K}$ and $L_2(T) \in \mathbb{K}[T]$ is a separable p -linearized polynomial of degree q . Furthermore, the p -rank of $\mathcal{X}$ is equal to zero.

We now prove a basic result on Kummer extensions that will be used throughout the thesis.

Proposition 1.118. *The number of branch points of a Kummer extension is different from 1.*

Proof. Let $\mathbb{K}(\mathcal{X})/\mathbb{K}(\mathcal{Y})$ be a Kummer extension of degree N ; that is $\mathbb{K}(\mathcal{X}) = \mathbb{K}(\mathcal{Y})(y)$ with

$$y^N - \alpha = 0 \quad \text{and} \quad \alpha \in \mathbb{K}(\mathcal{Y}).$$

From Kummer theory (see e.g. [64, Proposition 3.7.3 (b)]), the branch points of this extension are the points P of $\mathcal{Y}$ for which $\text{GCD}(\text{ord}_P(\alpha), N) < N$, i.e., $N \nmid \text{ord}_P(\alpha)$. Suppose by contradiction that there is a unique branch point P_0 . Then,

$$0 = \deg(\text{div}(\alpha)) = \text{ord}_{P_0}(\alpha) + \sum_{P \neq P_0} \text{ord}_P(\alpha).$$

Thus,

$$-\text{ord}_{P_0}(\alpha) = \sum_{P \neq P_0} \text{ord}_P(\alpha), \tag{1.2}$$

which is a contradiction because N divides the right-hand side of (1.2) but not the left-hand side. $\square$

From now on, $\mathcal{X}$ is a non-singular algebraic curve of genus $g(\mathcal{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \neq 2$ and G is a subgroup of the full automorphism group $\text{Aut}(\mathcal{X})$ of $\mathcal{X}$. It is a classical result that $\text{Aut}(\mathcal{X})$ is finite if the genus $g(\mathcal{X})$ of $\mathcal{X}$ is at least two; see, for example, [32, Chapter 11]

Theorem 1.119. *Let G be a finite automorphism group of a curve of genus $g \geq 2$. If $\text{char}(K) = 0$ or if $p = \text{char}(K) > 0$ does not divide $|G|$, then*

$$|G| < 84(g - 1).$$

Theorem 1.120. *Let G be such that the characteristic of $\mathbb{K}$ does not divide $|G|$. Then $|G| = 84(g - 1)$ if and only if G acts with 3 short orbits of size $|G|/2$, $|G|/3$ and $|G|/7$.*

Theorem 1.121. *[32, Theorem 11.60] If G is a subgroup of $\text{Aut}(\mathcal{X})$ that fixes a point and $p \nmid |G|$, then*

$$|G| \leq 4g(\mathcal{X}) + 2.$$

Theorem 1.122. [32, Theorem 11.79] *If G is an abelian subgroup of $\text{Aut}(\mathcal{X})$, then*

$$|G| \leq \begin{cases} 4g(\mathcal{X}) + 4, & \text{if } p \neq 2, \\ 4g(\mathcal{X}) + 2, & \text{if } p = 2. \end{cases}$$

We conclude this section with two preliminary results about ramification points in the extension $\mathcal{X}$ over $\mathcal{X}/G$, for G a cyclic group.

Proposition 1.123. *Let G be a cyclic group of order N . If $N \geq 2g(\mathcal{X}) + 1$, the extension $\mathcal{X}$ over $\mathcal{X}/G$ ramifies.*

Proof. Suppose by contradiction that the extension is unramified. Then, by the Riemann-Hurwitz formula applied to G we have

$$2g(\mathcal{X}) - 2 = N(2g_0 - 2),$$

where g_0 is the genus of $\mathcal{X}/G$. If $g_0 > 1$ then $2g(\mathcal{X}) - 2 \geq 2N$ that is $N \leq g(\mathcal{X}) - 1$ against $N \geq 2g(\mathcal{X}) + 1$; if $g_0 = 1$ then $2g(\mathcal{X}) - 2 = 0$ that is $g(\mathcal{X}) = 1$ against $g(\mathcal{X}) \geq 2$; if $g_0 = 0$ then $2g(\mathcal{X}) - 2 = -2N$, again a contradiction. $\square$

Proposition 1.124. *Let G be a cyclic group of order N . Let d be a divisor of N and H be the subgroup of G of order d . Denote by $\mathcal{Y}$ and $\mathcal{Z}$ the quotient curves $\mathcal{X}/H$ and $\mathcal{X}/G$, respectively. For a point $P \in \mathcal{X}$, let $Q \in \mathcal{Y}$ and $R \in \mathcal{Z}$ be the points lying under P with respect to the coverings $\mathcal{X} \rightarrow \mathcal{Y}$ and $\mathcal{X} \rightarrow \mathcal{Z}$. Then, R is a branch point for the covering $\mathcal{Y} \rightarrow \mathcal{Z}$ if and only if $|G_P| \nmid d$.*

Proof. Assume that $e_P = |G_P| \mid d$. Then, H contains a unique subgroup of order e_P , and this subgroup is G_P . Therefore, $G_P = H_P$ must hold, and hence the covering $\mathcal{Y} \rightarrow \mathcal{Z}$ is not ramified over R . On the other hand, if $e_P \nmid d$, H has no subgroups of order e_P , thus $G_P \not\subseteq H$. Therefore, H_P is properly contained in G_P , and so $\mathcal{Y} \rightarrow \mathcal{Z}$ ramifies over R . $\square$

1.3 Maximal curves

In the study of curves with many $\mathbb{F}_q$ -rational points the main problem is to determine the largest number of $\mathbb{F}_q$ -rational points of an irreducible $\mathbb{F}_q$ -rational curve. A fundamental result in this sense is the next theorem.

Theorem 1.125 (Hasse-Weil Bound). *Let $\mathcal{X}$ be an irreducible non-singular algebraic curve of genus g defined over $\mathbb{F}_q$ and let $\mathcal{X}(\mathbb{F}_q)$ be the set of the $\mathbb{F}_q$ -rational points of $\mathcal{X}$. Then*

$$q + 1 - 2g\sqrt{q} \leq \#\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

Definition 1.126. If

$$\#\mathcal{X}(\mathbb{F}_q) = q + 1 + 2g\sqrt{q}$$

then $\mathcal{X}$ is called $\mathbb{F}_q$ -maximal.

One of the most known examples of $\mathbb{F}_{q^2}$ -maximal curve is the Hermitian curve. The Hermitian curve $\mathcal{H}_q$ is a non-singular plane curve of genus $g = \frac{1}{2}(q^2 - q)$ with exactly $q^3 + 1 = q^2 + 1 + 2gq$ points in $PG(2, q^2)$. Two equivalent equations for $\mathcal{H}_q$ are

$$X^{q+1} - Y^q - Y = 0$$

and

$$\omega X^{q+1} + Y^q - Y = 0$$

with $\omega \in \mathbb{F}_q$ such that $\omega^{q+1} = -1$.

Also, the automorphism group of the Hermitian curve is completely known, indeed

$$\text{Aut}(\mathcal{H}_q) \cong \text{PGU}(3, q).$$

Now we collect some useful results about the function field of the Hermitian curve and its Galois subcovers. For more details, the reader is referred to [33, 35].

Result 1.127. [32, Theorem 12.24(iv), Proposition 11.30] $\text{Aut}(\mathbb{F}(\mathcal{H}_q)) = \text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q)) \cong \text{PGU}(3, q)$. Moreover, $\text{Aut}(\mathbb{F}(\mathcal{H}_q))$ acts on the set of all $\mathbb{F}_{q^2}$ -rational points of $\mathcal{H}_q$ as $\text{PGU}(3, q)$ in its natural doubly transitive permutation representation of degree $q^3 + 1$ on the isotropic points of the unitary polarity of the projective plane $PG(2, \mathbb{F}_{q^2})$.

The maximal subgroups of $\text{PGU}(3, q)$ were determined by Mitchell in 1911, see Hoffer [33]. Let S_p be a Sylow p -subgroup of $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q)) = \text{PGU}(3, q)$. From Result 1.127, it may be assumed up to conjugacy that the unique fixed point of S_p is the point at infinity Y_∞ of $\mathcal{H}_q$. The following result describes the structure of the stabilizer of Y_∞ in $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$.

Result 1.128. *Let the Hermitian function field be given by its canonical form $\mathbb{F}_{q^2}(x, y)$ with $y^q + y - x^{q+1} = 0$. Then the stabilizer G of Y_∞ in $\text{Aut}(\mathbb{F}(\mathcal{H}_q))$ consists of all maps*

$$\psi_{a,b,\lambda} : (x, y) \mapsto (\lambda x + a, a^q \lambda x + \lambda^{q+1} y + b) \quad (1.3)$$

where

$$a \in \mathbb{F}_{q^2}, \lambda \in \mathbb{F}_{q^2}^*, b^q + b = a^{q+1}. \quad (1.4)$$

In particular, $G = S_p \rtimes C$ where $S_p = \{\psi_{a,b,1} | b^q + b = a^{q+1}, a, b \in \mathbb{F}_{q^2}\}$ and $C = \{\psi_{0,0,\lambda} | \lambda \in \mathbb{F}_{q^2}^*\}$.

A direct computation by induction on i shows that for $1 \leq i \leq p$

$$\psi_{a,b,1}^i = \psi_{ia, a^{q+1}(i^2-i)/2+ib, 1}. \quad (1.5)$$

For more about Result 1.128 see [23], Section 4.

Remark 1.129. Changes of the generators x, y of the Hermitian function field $\mathbb{F}_{q^2}(x, y)$, $y^q + y - x^{q+1} = 0$ provide another canonical form. For our purpose, a useful change is $\tau : (x, y) \rightarrow (\omega x, -\omega y)$ where $\omega^{q-1} = -1$, and the arising canonical form is $y^q - y + \omega x^{q+1} = 0$. Then the elements in the stabilizer G of Y_∞ in $\text{Aut}(\mathbb{F}(\mathcal{H}_q))$ are of the form:

$$\varphi_{a,b,\lambda} : (x, y) \mapsto (\lambda x + a, a^q \lambda \omega x + \lambda^{q+1} y + b) \quad (1.6)$$

where (1.4) is replaced by

$$a \in \mathbb{F}_{q^2}, \lambda \in \mathbb{F}_{q^2}^*, b^q - b = -\omega a^{q+1}.$$

A direct computation by induction on i shows that for $1 \leq i \leq p$

$$\varphi_{a,b,1}^i = \varphi_{ia, a^{q+1}\omega(i^2-i)/2+ib, 1}. \quad (1.7)$$

For more about Result 1.129 see [23], Section 4.

From Result 1.128, S_p is the (unique) Sylow p -subgroup of the stabilizer of Y_∞ in $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$.

Result 1.130. S_p has the following properties.

- (I) The center $Z(S_p)$ of S_p has order q and it consists of all maps $\psi_{0,b,1}$ with $b^q + b = 0, b \in \mathbb{F}_{q^2}$. Also, $Z(S_p)$ is an elementary abelian group of order p .

- (II) The non-trivial elements of S_p form two conjugacy classes in the stabilizer of Y_∞ in $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$, one comprises all non-trivial elements of $Z(S_p)$, the other does the remaining $q^3 - q$ elements.
- (III) The elements of G other than those in $Z(S_p)$ have order p , or $p^2 = 4$ according as $p > 2$ or $p = 2$.

The following result follows from [57, Lemma 1].

Result 1.131. All $\mathbb{F}_{q^2}$ -maximal curves have zero Hasse-Witt invariant.

The following result is commonly attributed to Serre.

Result 1.132. [32, Theorem 10.2] For every subgroup G of $\text{Aut}_{\mathbb{F}_{q^2}}(\mathcal{X})$, the quotient curve $\mathcal{X}/G$ is also $\mathbb{F}_{q^2}$ -maximal.

1.4 Linear Codes

Definition 1.133. A linear code C of length n is a vector subspace $C \subseteq \mathbb{F}_q^n$. For a linear code C the dimension k is $k = \dim_{\mathbb{F}_q}(C)$ and the minimum distance d is $d = \min \{d(a, b) \mid a, b \in C, a \neq b\}$ where, if $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$, $d(a, b) = \#\{i \mid a_i \neq b_i\}$.

A linear code C of length n , dimension k and minimum distance d over $\mathbb{F}_q$ is called $[n, k, d]_q$ -code. The minimum distance d can also be expressed as $d = \min \{\|a\| \mid a \in C, a \neq 0\}$, where $\|a\| = \#\{i \mid a_i \neq 0\}$, that is the weight of a .

Definition 1.134. A generator matrix of an $[n, k, d]_q$ -code C is a $k \times n$ matrix over $\mathbb{F}_q$ whose rows form a basis for C .

Remark 1.135. If G is a generator matrix of an $[n, k, d]_q$ -code C , then $C = \{x \cdot G \mid x \in \mathbb{F}_q^k\}$.

Definition 1.136. Let C be an $[n, k, d]_q$ -code. The dual code $C^\perp$ of C is the code of length n defined as $C^\perp = \{a \in \mathbb{F}_q^n \mid \langle a, x \rangle = 0 \ \forall x \in C\}$, where $\langle \cdot, \cdot \rangle$ denotes the standard inner product.

Remark 1.137. If G is a generator matrix of an $[n, k, d]_q$ -code C , then $C^\perp = \{x \in \mathbb{F}_q^n \mid G \cdot x^T = 0\}$.

It can be proved that $\dim_{\mathbb{F}_q}(C^\perp) = n - k$ and that $(C^\perp)^\perp = C$.

Definition 1.138. A *parity-check matrix* of an $[n, k, d]_q$ -code C is a $(n - k) \times n$ matrix over $\mathbb{F}_q$ that is a generator matrix of the dual code $C^\perp$.

Remark 1.139. If H is a parity-check matrix of an $[n, k, d]_q$ -code C , then $C = \{x \in \mathbb{F}_q^n \mid H \cdot x^T = 0\}$.

Proposition 1.140. Let H be a parity-check matrix of an $[n, k, d]_q$ -code C . Then d is the minimum number of linearly dependent columns of H .

The next result shows the relationship between two generator matrices of the same code.

Proposition 1.141. Let $G = (g_{i,j})$ and $G' = (g'_{i,j})$ be two generator matrices of two $[n, k, d]_q$ -codes C and C' . Then $C = C'$ if and only if there exists $N \in GL(k, q)$ such that $G' = NG$.

An analogous result holds for the parity-check matrices.

Proposition 1.142. Let $H = (h_{i,j})$ and $H' = (h'_{i,j})$ be two parity-check matrices of two $[n, k, d]_q$ -codes C and C' . Then $C = C'$ if and only if there exists $N \in GL(n - k, q)$ such that $H' = NH$.

Even though all the k -dimensional vector subspaces of $\mathbb{F}_q^n$ are isomorphic, the $[n, k, d]_q$ -codes are not all equivalent, since, in general, a linear isomorphism does not preserve the weight of a vector. The isomorphisms that are regarded as equivalences of $[n, k, d]_q$ -codes are the restrictions of those automorphisms of $\mathbb{F}_q^n$ represented by monomial matrices, which are the invertible matrices containing exactly one nonzero entry in each row and in each column or, equivalently, the matrices obtained as the product of a permutation matrix and a diagonal matrix.

Note that, if M is a monomial matrix, then $x \in \mathbb{F}_q^n$ and $x \cdot M$ have the same weight and, if B is a matrix with n columns over $\mathbb{F}_q^n$, then the columns of BM are proportional to those of B , possibly permuted.

Let $\mathcal{A}$ be the group of automorphisms of $\mathbb{F}_q^n$ represented by monomial matrices.

Definition 1.143. Two $[n, k, d]_q$ -codes C and C' are called *equivalent* if there exists $A \in \mathcal{A}$ such that $C' = A(C)$.

Lemma 1.144. *Two $[n, k, d]_q$ -codes C and C' are equivalent if and only if their duals are equivalent.*

Proposition 1.145. *Let G and G' be two generator matrices of two $[n, k, d]_q$ -codes C and C' . Then C and C' are equivalent if and only if there exist an $n \times n$ monomial matrix M and an $k \times k$ invertible matrix N such that $G' = NGM$.*

Proposition 1.146. *Let H and H' be two parity-check matrices of two $[n, k, d]_q$ -codes C and C' . Then C and C' are equivalent if and only if there exist an $n \times n$ monomial matrix M and an $(n - k) \times (n - k)$ invertible matrix N such that $H' = NHM$.*

Definition 1.147. Let C be a $[n, k, d]_q$ -code. The *automorphism group* of C , denoted by $\text{Aut}(C)$, is the group of the elements $A \in \mathcal{A}$ such that $A(C) = C$.

For fixed n and k , the best linear codes are those with the largest possible minimum distance d . The next proposition provides an upper bound for d , known as *Singleton bound*.

Proposition 1.148. *Let C be an $[n, k, d]_q$ -code. Then*

$$d \leq n - k + 1.$$

Definition 1.149. An $[n, k, d]_q$ -code which attains the Singleton bound is called *optimal* or *MDS* (*Maximum Distance Separable*).

Proposition 1.150. *An $[n, k, d]_q$ -code is MDS if and only if every set of k columns of a generator matrix forms a set of linearly independent vectors of $\mathbb{F}_q^k$.*

Proposition 1.151. *The dual code of an $[n, k, d]_q$ -code that is MDS, is still MDS.*

Definition 1.152. Let C be an $[n, k, d]_q$ -code, the integer $\Delta_C = n - k + 1 - d$ is called *Singleton defect*. The codes with $\Delta_C = 1$ are called *Almost MDS* (*AMDS*).

For fixed n and k , the best codes are those with the lowest Singleton defect; on the other hand, for a fixed Singleton defect, the codes generally considered best are those with larger n .

We now define two particular classes of codes: cyclic codes and quasi-cyclic codes.

Definition 1.153. Let C be a linear code of length n over $\mathbb{F}_q$. Let

$$c = (c_1, c_2, \dots, c_n)$$

denote a codeword in C . If

$$c' = (c_n, c_1, c_2, \dots, c_{n-1})$$

also belongs to C , then C is called a *cyclic code* over $\mathbb{F}_q$ of length n .

Definition 1.154. Let C be a linear code of length ln_0 over $\mathbb{F}_q$. Let

$$c = (c_{1,1}, c_{1,2}, \dots, c_{1,l}, c_{2,1}, c_{2,2}, \dots, c_{2,l}, \dots, c_{n_0,1}, c_{n_0,2}, \dots, c_{n_0,l})$$

denote a codeword in C . If

$$c' = (c_{1,l}, c_{1,1}, \dots, c_{1,l-1}, c_{2,l}, c_{2,1}, \dots, c_{2,l-1}, \dots, c_{n_0,l}, c_{n_0,1}, \dots, c_{n_0,l-1})$$

belongs to C then C is called a quasi-cyclic (QC) code over $\mathbb{F}_q$ of length ln_0 , index n_0 and co-index l .

1.4.1 Algebraic-Geometric Codes

Let $\mathcal{X}$ be an algebraic curve defined over $\mathbb{F}_q$, let $\text{Div}(\mathcal{X})$ be the group of divisors of $\mathcal{X}$ and, for $G \in \text{Div}(\mathcal{X})$, let $\deg(G)$ denote the degree of G , let $\mathcal{L}(G)$ denote the Riemann-Roch space of G and $\ell(G) = \dim(\mathcal{L}(G))$.

Let $P_1, \dots, P_n$ be n different $\mathbb{F}_q$ -rational points of $\mathcal{X}$ and let $D = P_1 + \dots + P_n$ and $G = \sum n_P P \in \text{Div}(\mathcal{X})$ such that $n_{P_i} = 0$ for each $i \in \{1, \dots, n\}$.

Let

$$\begin{aligned} e = e_{P_1, \dots, P_n} : \mathcal{L}(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \dots, f(P_n)) \end{aligned}$$

note that $e_{P_1, \dots, P_n}$ is $\mathbb{F}_q$ -linear.

Definition 1.155. The *Goppa code* associated with D and G is $C_{D,G} = e(\mathcal{L}(G))$.

Lemma 1.156. Let $k = \dim(C_{D,G})$ and let d be the minimum distance of $C_{D,G}$. Then

- (1) $k = \ell(G) - \ell(G - D)$;
- (2) $d \geq n - \deg(G)$.

Proposition 1.157. *Let $C_{D,G}$ be an $[n, k, d]_q$ -Goppa code and let g be the genus of $\mathcal{X}$. Then*

- (1) *If $n > \deg(G)$, then $k = \ell(G)$. In particular $k \geq \deg(G) + 1 - g$. Furthermore, a generator matrix of $C_{D,G}$ is*

$$M = \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_k(P_1) & \cdots & f_k(P_n) \end{pmatrix}$$

where $f_1, \dots, f_k$ form a basis of $\mathcal{L}(G)$ over $\mathbb{F}_q$;

- (2) *If $n > \deg(G) > 2g - 2$, then $k = \deg(G) + 1 - g$.*

Note that the Singleton bound (Proposition 1.148) together with Proposition 1.157 (1) imply, for a Goppa code $C_{D,G}$ with $n > \deg(G)$, that

$$n + 1 - g \leq d + k \leq n + 1$$

in particular, if the genus of $\mathcal{X}$ is 0, then $C_{D,G}$ is MDS.

Actually the definition of $C_{D,G}$ can be slightly generalized in order to omit the condition $v_{P_i}(G) = 0$. Let $P_1, \dots, P_n$ be n distinct $\mathbb{F}_q$ -rational points of $\mathcal{X}$ and let $G \in \text{Div}_q(\mathcal{X})$. Let

$$e^* = e_{P_1, \dots, P_n}^* : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n$$

$$f \mapsto (t_1^{b_1} f(P_1), \dots, t_n^{b_n} f(P_n)),$$

where t_i is a local parameter at P_i and $b_i = -v_{P_i}(G)$. Set $D = P_1 + \dots + P_n$. Let $C_{D,G}^* = e^*(\mathcal{L}(G))$. Clearly if $v_{P_i}(G) = 0$ for all $i = 1, \dots, n$ then $C_{D,G} = C_{D,G}^*$. The equations $n = \deg(D)$, $k = \ell(G) - \ell(G - D)$ and $d \geq n - \deg(G)$ hold for $C_{D,G}^*$ as well, see [66]. The definition of $C_{D,G}^*$ depends on the choice of the local parameters $t_1, \dots, t_n$. Nevertheless, codes corresponding to different local parameters are equivalent (one is obtained from the other via a monomial transformation), and therefore their monomial automorphism groups are isomorphic. The investigation of the automorphism groups of Goppa codes was initiated by Stichtenoth [65]. Given a code $C_{D,G}$, let $\text{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X})$ be the following automorphism group of the underlying curve $\mathcal{X}$:

$$\text{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X}) = \left\{ \sigma \in \text{Aut}_{\mathbb{F}_q}(\mathcal{X}) : \sigma(D) = D, \sigma(G) \approx_D G \right\},$$

where $\sigma(G) \approx_D G$ if and only if there exists an element $0 \neq u \in \mathbb{F}_q(\mathcal{X})$ such that $G' - G = \text{div}(u)$ and $u(P_i) = 1$ for $i = 1, \dots, n$. Among other results, Stichtenoth proved that any $\sigma \in \text{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X})$ induces a permutation automorphism of $C_{D, G}$; furthermore, if $n > 2g + 2$ then $\text{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X})$ can be identified with a subgroup of $\text{PAut}(C_{D, G})$. The problem of establishing whether the whole permutation automorphism group of a Goppa code coincides with $\text{Aut}_{\mathbb{F}_q, D, G}$ has been investigated by several authors, especially for the case of one-point Goppa codes, see [19, 39, 67, 68].

Chapter 2

Algebraic curves with large automorphism groups

The aim of this chapter is to investigate algebraic curves, defined over algebraically closed field of arbitrary characteristic, through the properties of their automorphism group.

In the case where the base field is the complex field, it is well known that the concept of an algebraic curve corresponds to that of a compact and connected Riemann surface. Generally speaking, numerous authors have studied curves over the complex field (or, equivalently, Riemann surfaces) that admit automorphism groups of specific type and of relatively large order compared to their genus. These investigations often involve classifying such surfaces and analyzing the structural conditions under which they can possess "large" symmetry groups. This typically requires tools from group theory, complex geometry, and topology. However, in the case of positive characteristic, the available methods are more limited. When similar results are obtained in this setting, the approach must rely entirely on algebraic techniques.

The goal of this chapter is to extend results that are somehow classical for the theory of Riemann surfaces to the case of positive characteristic, the difficulty is that topological methods cannot be used and a purely algebraic approach is needed. Our notation and terminology are standard; see [32, Chapter 11] for details. Let $\mathcal{X}$ denote a projective, geometrically irreducible, nonsingular algebraic curve defined over an algebraically closed field $\mathbb{K}$ of characteristic p of genus $g \geq 2$. Let G be a finite subgroup of $\text{Aut}(\mathcal{X})$, let $\bar{\mathcal{X}}$ be a non-singular model of $\mathbb{K}(\mathcal{X})^G$, that is, the quotient curve of $\mathcal{X}$ by G and it will be also denoted by $\mathcal{X}/G$. The field extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$ is Galois of

degree $|G|$. Let Φ denote the associated rational map $\mathcal{X} \rightarrow \bar{\mathcal{X}}$.

We recall that a point $P \in \mathcal{X}$ is called a ramification point of G if the stabilizer G_P of P in G is non-trivial; the ramification index e_P at P is given by $|G_P|$. A point $\bar{Q} \in \bar{\mathcal{X}}$ is a branch point of G if there is a ramification point $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$.

The G -orbit of $P \in \mathcal{X}$ is the subset of $\mathcal{X}$

$$o = \{R \mid R = g(P), g \in G\},$$

and it is called *long* if $|o| = |G|$; otherwise, o is *short*. For a point $\bar{Q}$, the G -orbit o lying over $\bar{Q}$ consists of all points $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$. If $P \in o$ then $|o| = |G|/|G_P|$ and hence $\bar{Q}$ is a branch point if and only if o is a short G -orbit. Note that it is possible for G to have no short orbits, which occurs if and only if every non-trivial element of G is fixed-point-free on $\mathcal{X}$, meaning the cover Φ is unramified. On the other hand, $\mathcal{X}$ has a finite number of short G -orbits.

If $\Omega_1, \dots, \Omega_k$ denote the short orbits under the action of G and n_i (suppose, without loss of generality, $n_1 \leq \dots \leq n_k$) denotes the size of the stabilizer in G of an arbitrary point of Ω_i , then

$$(n_1, \dots, n_k)$$

is called *signature* of the action of G on $\mathcal{X}$.

Definition 2.1. Let G be a finite group of automorphisms of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic p . Then G is called *tame* if no element of order p fixes a point of $\mathcal{X}$.

As mentioned in the introduction, when the characteristic p divides $|\text{Aut}(\mathcal{X})|$, the classical Hurwitz bound does not generally hold. Algebraic curves defined over fields of positive characteristic can have many more automorphisms than predicted by the Hurwitz bound, stronger bounds for subgroups G of $\text{Aut}(\mathcal{X})$ under certain conditions have been established. For instance,

- for solvable groups G and odd p , $|G| \leq 34(g(\mathcal{X}) + 1)^{3/2}$; see [42];
- for solvable groups G , even $g(\mathcal{X})$, and $p = 2$, $|G| \leq 35(g(\mathcal{X}) + 1)^{3/2}$; see [48];
- for abelian groups, $|G| \leq 4g(\mathcal{X}) + 4$; see Theorem 1.122;

- for subgroups of prime power order d with $d = p$, $|G| \leq 4(g(\mathcal{X}) - 1)$; see [52];
- for subgroups of prime power order d , p odd, and $d \neq p$, $|G| \leq 9(g(\mathcal{X}) - 1)$; see [41];
- for groups G fixing a point, $|G| \leq \frac{4pg(\mathcal{X})^2}{p-1} \left(\frac{2g(\mathcal{X})}{p-1} + 1 \right)$; see [62, Theorem 2.1]. See also [26, 44] for other bounds on automorphism groups fixing a point.

2.1 Automorphism groups of order greater than $4(g - 1)$

In [43] R. Kulkarni investigates Riemann surfaces which admit automorphism groups of large order with respect to their genus, in particular the author studies the cases where the order of the group is near the Hurwitz bound $84(g - 1)$. The paper provides a classification and a detailed analysis of the structural conditions for which these surfaces can have "large" symmetry groups, by using tools from both group theory and complex geometry. In particular, Kulkarni analyzes compact Riemann surfaces of genus $g \geq 2$ admitting automorphism groups G of order

$$|G| > 4(g - 1).$$

The proof can be easily extended to the case of curves defined over a field of any characteristic p , under the assumption that the group is tame.

Theorem 2.2. *Let G be a finite tame automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$. If $|G| > 4(g - 1)$ then G acts with 3 or 4 short orbits and the quotient curve $\mathcal{X}/G$ is rational. Furthermore, one of the following possibilities for the signature of the action of G on $\mathcal{X}$ holds:*

- $(2, 2, 2, n)$, $n \geq 3$
- $(2, 2, 3, n)$, $3 \leq n \leq 5$
- $(2, m, n)$, $n \geq m \geq 5$
- $(2, 3, n)$, $n \geq 7$

- $(2, 4, n), n \geq 5$
- $(3, 3, n), n \geq 4$
- $(3, 4, n), n \geq 4$
- $(3, 5, n), n \geq 5$
- $(3, 6, n), n \geq 6$
- $(3, 7, n), 41 \leq n \leq 7$
- $(3, 8, n), 23 \leq n \leq 8$
- $(3, 9, n), 17 \leq n \leq 9$
- $(3, 10, n), 14 \leq n \leq 10$
- $(3, 11, n), 13 \leq n \leq 11$
- $(4, 4, n), n \geq 4$
- $(4, 5, n), 19 \geq n \geq 5$
- $(4, 6, n), 11 \geq n \geq 6$
- $(4, 7, n), 9 \geq n \geq 7$
- $(5, 5, n), 9 \geq n \geq 5$
- $(5, 6, n), 7 \geq n \geq 6$.

Proof. Let r denote the number of short orbits under the action of G and let $e_1 \leq e_2 \leq \dots \leq e_r$ be the sizes of the stabilizers of the points in such orbits.

Let g' be the genus of $\mathcal{X}/G$, from Corollary 2.3 and Corollary 1.109 we know that

$$2g - 2 = |G|(2g' - 2) + \sum_{O \in \mathcal{P}} (|G_O| - 1)$$

where G_O denotes the stabilizer of O in G . We can also write

$$2g - 2 = |G|(2g' - 2) + \sum_{E \text{ orbit under } G} \left(\sum_{O \in E} (|G_O| - 1) \right).$$

Hence

$$2g - 2 = |G|(2g' - 2) + \sum_{E \text{ orbit under } G} \left(\sum_{O \in E} (|G|/|E| - 1) \right) = |G|(2g' - 2) + \sum_{E \text{ orbit under } G} (|G| - |E|),$$

and so

$$2g - 2 = |G| \left(2g' - 2 + \sum_{E \text{ orbit under } G} \left(1 - \frac{|E|}{|G|} \right) \right).$$

Let $E_1, \dots, E_r$ be the orbits of DVR under the action of G of size smaller than $|G|$. Let

$$d_i = \frac{e_i - 1}{e_i} = \left(1 - \frac{|E_i|}{|G|} \right).$$

Thus

$$2g - 2 = |G| \left(2g' - 2 + \sum_{i=1}^r d_i \right).$$

(If there are no short orbits assume $\sum_{i=1}^r d_i = 0$).

Since $|E_i|$ properly divides $|G|$, we have that $d_i \geq \frac{1}{2}$.

1. If $g' \geq 2$ then $|G| \leq g - 1$, against $|G| > 4(g - 1)$.
2. If $g' = 1$ then $2g - 2 = |G| \sum_{i=1}^r d_i$. Since $g \geq 2$ necessarily $\sum_{i=1}^r d_i > 0$ and so $\sum_{i=1}^r d_i \geq \frac{1}{2}$. Thus $|G| \leq 4(g - 1)$ against $|G| > 4(g - 1)$.
3. If $g' = 0$, then

$$2g - 2 = |G| \left(-2 + \sum_{i=1}^r d_i \right). \tag{2.1}$$

Hence we must have $\sum_{i=1}^r d_i > 2$, and so, since $d_i < 1$, necessarily $r > 2$.

If $r \geq 5$ then $\sum_{i=1}^r d_i \geq 5/2$ and so $|G| \leq 4(g - 1)$, a contradiction. Then $r < 5$.

Therefore we can conclude that $\mathcal{X}/G$ is rational and that $r \in \{3, 4\}$.

Thus, from 2.1, $|G| > 4g - 4$ implies

$$2 < \sum_{i=1}^r d_i < \frac{5}{2}.$$

Let us focus on the case $r = 4$.

Necessarily $e_4 > 2$ and $e_2 = 2$; furthermore $(2, 2, 2, n)$ is admissible for each $n \geq 3$, while $(2, 2, 3, n)$ is admissible just for $3 \leq n \leq 5$.

Let us now consider the case $r = 3$.

We have $e_1 \leq 5$.

If $e_1 = 2$ then $e_2 > 2$ and $(2, m, n)$ with $m \geq 5$ and $n \geq m$ is admissible, while $(2, 3, n)$ is admissible just for $n \geq 7$ and $(2, 4, n)$ just for $n \geq 5$.

If $e_1 = 3$ then $3 \leq e_2 \leq 11$, furthermore $(3, 3, n)$ and $(3, 4, n)$ are admissible for $n \geq 4$, $(3, 5, m)$ for $m \geq 5$, $(3, 6, m)$ for $m \geq 6$, $(3, 7, m)$ for $7 \leq m \leq 41$, $(3, 8, m)$ for $8 \leq m \leq 23$, $(3, 9, m)$ for $9 \leq m \leq 17$, $(3, 10, m)$ for $10 \leq m \leq 14$ and $(3, 11, m)$ for $11 \leq m \leq 13$.

If $e_1 = 4$ then the admissible combinations are $(4, 4, m)$ for $4 \leq m$, $(4, 5, m)$ for $5 \leq m \leq 19$, $(4, 6, m)$ for $6 \leq m \leq 11$ and $(4, 7, m)$ for $7 \leq m \leq 9$.

If $e_1 = 5$ then the admissible combinations are $(5, 5, m)$ for $5 \leq m \leq 9$ and $(5, 6, m)$ for $6 \leq m \leq 7$.

□

Note that the bound of Theorem 2.2 is sharp, in the sense that there exists an infinite number of examples of groups of order $4g - 4$ which act on curves of genus g with 5 short orbits (see Example 2.42).

Let us now consider a classical result, valid in the complex case (cited, for example, in [43]), whose extension to the case of positive characteristic will be given in one of the next sections for the case where G is abelian.

Theorem 2.3. *Let G be a finite automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over $\mathbb{C}$. Suppose that the quotient curve $\mathcal{X}/G$ is rational and let $\Omega_1, \dots, \Omega_k$ denote the short orbits under the action of G . Let G_i be the stabilizer in G of an arbitrary point of Ω_i and let g_i be a generator of the cyclic group G_i . Then G is generated by $k - 1$ elements arbitrarily chosen in $\{g_i \mid i = 1, \dots, k\}$.*

In the case of arbitrary characteristic we recall the next result (proved, for example, in [60, Proposition 4.4.6]).

Theorem 2.4. *Let G be a finite tame automorphism group of an algebraic curve $\mathcal{X}$ of genus $g \geq 2$ defined over an algebraically closed field of characteristic $p > 0$. Suppose that the quotient curve $\mathcal{X}/G$ is rational. Let $\Omega_1, \dots, \Omega_k$ denote the short orbits under the action of G . For a fixed integer i_0 between 1 and k , G is the group generated by the stabilizers of the points of Ω_i with $i \neq i_0$.*

Proof. For a fixed integer i_0 between 1 and k consider the subgroup H of G generated by all the subgroups G_P (that is the stabilizer of P in G) with

$$P \in \bigcup_{\substack{i=1, \dots, k \\ i \neq i_0}} \Omega_i.$$

Note that H is normal in G : in fact, given $g \in G_P$ with $P \in \Omega_i$, every conjugate of g belongs to the stabilizer of another point of Ω_i .

Suppose, by contradiction, that H is a proper subgroup of G and consider the quotient curve $\mathcal{X}/H$. The factor group G/H acts on $\mathcal{X}/H$. The action of G/H on the orbits under the action of H that are contained in Ω_i for $i \neq i_0$ is free: let Γ be an orbit under the action of H that is fixed by an element $g \in G \setminus H$; then, for the Stabilizer Index Theorem, the stabilizer in G of a point of Γ strictly contains the stabilizer in H of the same point and this can happen only for the points of Ω_{i_0} .

Thus G/H acts on $\mathcal{X}/H$ with at most one short orbit.

By recalling that $\mathcal{X}/G$ is rational, the Riemann-Hurwitz formula for G/H is

$$2g(\mathcal{X}/H) - 2 = -2 \frac{|G|}{|H|} + \frac{|G|}{|H|} - m = -\frac{|G|}{|H|} - m$$

where m is a divisor of $\frac{|G|}{|H|}$. This contradicts $\frac{|G|}{|H|} > 1$. $\square$

By combining Theorem 2.2 and Theorem 2.3 we have that in the complex case every automorphism group of size greater than $4(g-1)$ is generated by 3 elements.

2.2 Cyclic groups

The aim of this section is to characterize projective, geometrically irreducible, non singular algebraic curves defined over an algebraically closed field of positive and odd characteristic p , admitting a cyclic automorphism group G

of order $N \geq 2g + 1$, the results presented in this section are the subject of the paper [17]. In the complex case, if G is a cyclic group, then $|G| \leq 4g(\mathcal{X}) + 2$. A complete characterization of algebraic curves over $\mathbb{C}$ with an automorphism of order at least $2g(\mathcal{X}) + 1$ was given by Irokawa and Sasaki [36]. They proved that if $\mathcal{X}$ is a curve of genus at least 2 and its automorphism group contains a cyclic subgroup G of order $N \geq 2g(\mathcal{X}) + 1$, then $\mathcal{X}$ is either isomorphic to the curve

$$y^N = x^r(1 - x)^s,$$

for some $r, s \geq 1$, with $r + s \leq N - 1$ and $\text{GCD}(r, s, N) = 1$, or to the curve

$$y^2 = (x^{g(\mathcal{X})+1} - 1)(x^{g(\mathcal{X})+1} - \lambda),$$

where $\lambda \in \mathbb{K} \setminus \{0, 1\}$. In the first case, $\mathcal{X}$ is a quotient of the Fermat curve of degree N , whereas in the second case, it is a hyperelliptic curve.

As a matter of terminology, we say that $\mathcal{X}$ is an N -curve if it admits an automorphism group of size N . In arbitrary characteristic, so far only the prime order case has been thoroughly investigated: Homma [34] proved that if $N = q$ is a prime, then either $q \leq g(\mathcal{X}) + 1$ or $q = 2g(\mathcal{X}) + 1$ and provided a classification for the latter case; more recently, Arakelian and Speziali [3] classified $(g(\mathcal{X}) + 1)$ -curves, and fully characterized the automorphism groups of q -curves for $q = 2g(\mathcal{X}) + 1$ and for $q = g(\mathcal{X}) + 1$.

In this section, we tackle the problem of classifying N -curves with $N \geq 2g(\mathcal{X}) + 1$ in positive characteristic. The challenge in this context, compared to the complex case, arises from the potential for wild ramification, particularly due to the presence of p -elements in G that fix a point on $\mathcal{X}$. We achieve success for $p \neq 2$, and our main result is as follows.

Theorem 2.5. *Let $p \geq 3$, and let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ with a cyclic automorphism group G of order $N \geq 2g(\mathcal{X}) + 1$. Then, up to birational equivalence, one of the following holds:*

(I) $p \nmid N$, and either

$$\mathcal{X} : y^N = x^r(1 - x)^s,$$

for some natural numbers r and s such that $r + s \leq N - 1$ and $\text{GCD}(r, s, N) = 1$, or $\mathcal{X}$ is a hyperelliptic curve

$$\mathcal{X} : y^2 = \left(x^{\frac{N}{2}} - 1\right)\left(x^{\frac{N}{2}} - \lambda\right),$$

where $\lambda \in \mathbb{K} \setminus \{0, 1\}$ and $N \equiv 2 \pmod{4}$;

(II) $N = pm$ with $m > 1$, $(p, m) = 1$, and $p \neq 3$; also, either $g(\mathcal{X}) = \frac{(p-1)(m-1)}{2}$ and

$$\mathcal{X} : y^p - y = a(x^m - b)$$

for some $a, b \in \mathbb{K}$, or $g(\mathcal{X}) = p - 1$ and

$$\mathcal{X} : by^p + cy = ax + \frac{1}{x}$$

for some $a, b, c \in \mathbb{K}$.

(III) $N = p$, and

$$\mathcal{X} : y^p - y = x^2.$$

Due to the possible occurrence of wild ramification, we will divide the proof into two subsections: Subsection 2.2.1 and Subsection 2.2.2, according to whether $|G|$ is divisible by p or not.

2.2.1 Proof of Theorem 2.5 when p divides N

In this subsection $\mathcal{X}$ is a non-singular algebraic curve of genus $g(\mathcal{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \neq 2$. Also, σ is an automorphism of $\mathcal{X}$ of order N and $G = \langle \sigma \rangle$ is the subgroup of $\text{Aut}(\mathcal{X})$ generated by σ .

We assume that $N \geq 2g(\mathcal{X}) + 1$ and that p divides N . Our goal in this Subsection is to prove that either (II) or (III) of Theorem 2.5 holds. To this end, we distinguish the cases $N = p^h$ and $N = p^h m$ with $(p, m) = 1$, $m > 1$.

The case $N = p^h$

First, we show that that $h \leq 2$ holds under the weaker condition $N \geq 2g(\mathcal{X}) - 1$.

Proposition 2.6. *If $N = p^h$ with $p \geq 3$ and $N \geq 2g(\mathcal{X}) - 1$, then $h \leq 2$.*

Proof. If $p > 3$ then the p -rank $\gamma(\mathcal{X})$ of $\mathcal{X}$ is equal to zero by [32, Theorem 11.84]. Actually, we may assume $\gamma(\mathcal{X}) = 0$ also for $p = 3$. In fact, by [25, Proposition 3.3], if $\gamma(\mathcal{X}) > 0$ and $3^h > 2g(\mathcal{X}) - 2$ then $h = 1$.

Therefore, by [32, Lemma 11.129] and [32, Remark 11.128] G fixes one point $P_0 \in \mathcal{X}$ and acts semiregularly on the other points of the curve. By the Riemann-Hurwitz formula applied to G ,

$$2g(\mathcal{X}) - 2 = p^h(2g_0 - 2) + \sum_{i=0}^{\infty} (|G_{P_0}^{(i)}| - 1),$$

where g_0 is the genus of $\mathcal{X}/G$. Since $G = G_{P_0}^{(0)} = G_{P_0}^{(1)}$ is cyclic, by (iii) of [32, Theorem 11.74] we have that the factor group $G_{P_0}^{(i)}/G_{P_0}^{(i+1)}$ is either trivial or a cyclic group of order p . Also, by (v) of [32, Lemma 11.75] the integers k for which $G_{P_0}^{(k)}/G_{P_0}^{(k+1)}$ is non-trivial are all congruent modulo p .

Assume that $h \geq 3$. Then

$$\sum_{i=0}^{\infty} (|G_{P_0}^{(i)}| - 1)$$

is at least

$$2(p^h - 1) + p(p^{h-1} - 1) + p(p^{h-2} - 1) + \dots + p(p - 1)$$

that is

$$2p^h - 2 + p^h + p^{h-1} + \dots + p^2 - (h-1)p.$$

As $p^h \geq 2g(\mathcal{X}) - 1$

$$2g(\mathcal{X}) - 2 \geq p^h + p^{h-1} + \dots + p^2 - (h-1)p - 2 \geq 2g(\mathcal{X}) - 1 + p^{h-1} + \dots + p^2 - (h-1)p - 2$$

which implies

$$p^{h-1} + \dots + p^2 - (h-1)p - 1 \leq 0,$$

a contradiction. □

Now, the case $N = p^2$ is considered. We are going to show that it is not possible that $p^2 \geq 2g(\mathcal{X}) + 1$. Our first step is to rule out all possibilities but $p^2 = 2g(\mathcal{X}) + p$.

Proposition 2.7. *If $N = p^2$ with $p \geq 3$ and $N \geq 2g(\mathcal{X}) + 1$, then $p^2 = 2g(\mathcal{X}) + p$. Also, there is a unique short orbit $\Omega = \{P_0\}$ of $\mathcal{X}$ under the action of G , and*

$$|G_{P_0}^{(0)}| = |G_{P_0}^{(1)}| = p^2, \quad |G_{P_0}^{(2)}| = \dots = |G_{P_0}^{(p+1)}| = p, \quad |G_{P_0}^{(p+2)}| = 1.$$

Moreover, the quotient curve $\mathcal{X}/G_{P_0}^{(2)}$ is rational.

Proof. By the proof of Proposition 2.6, G fixes one point $P_0 \in \mathcal{X}$ and acts semiregularly on the other points of the curve. Also, there exist two positive integers $v \geq 2$ and w such that $|G_{P_0}^{(v-1)}| = p^2$ and

$$p = |G_{P_0}^{(v)}| = |G_{P_0}^{(v+1)}| = \dots = |G_{P_0}^{(wp+v-1)}| \neq |G_{P_0}^{(wp+v)}| = 1.$$

Let $T = G_{P_0}^{(v)}$. Clearly $T_{P_0}^{(i)} = T$ for each $i \leq wp + v - 1$. Write the Riemann-Hurwitz genus formula for T :

$$2g(\mathcal{X}) - 2 = p(2g(\mathcal{X}/T) - 2) + (wp + v)(p - 1).$$

Then

$$p^2 - 3 \geq 2g(\mathcal{X}) - 2 = p(2g(\mathcal{X}/T) - 2) + (wp + v)(p - 1)$$

implies $g(\mathcal{X}/T) = 0$, and hence

$$p^2 - 3 \geq 2g(\mathcal{X}) - 2 = -2p + (wp + v)(p - 1),$$

which can be read

$$p^2 - 1 \geq 2(-p + 1) + (wp + v)(p - 1),$$

and hence

$$p + 1 \geq wp + v - 2.$$

Then $w = 1$ and either $v = 2$ or $v = 3$. Actually, the latter case cannot occur. Indeed, the Riemann-Hurwitz formula for G gives

$$p^2 - 3 \geq 2g(\mathcal{X}) - 2 = -2p^2 + 3(p^2 - 1) + p(p - 1)$$

and hence $p(p - 1) \leq 0$, a contradiction. $\square$

Theorem 2.8. *If $N = p^h \geq 2g(\mathcal{X}) + 1$, then $h = 1$ and $\mathcal{X} : y^2 = x^p - x$.*

Proof. By Proposition 2.6, $h \leq 2$ holds. Assume by contradiction that $h = 2$. By Proposition 2.7, the subgroup of G of order p fixes a point P_0 , coincides with $G_{P_0}^{(2)}$, and acts semiregularly on the other points of $\mathcal{X}$. Also, the quotient curve $\mathcal{X}/G_{P_0}^{(2)}$ is rational.

By [32, Theorem 12.5], an equation for $\mathcal{X}$ is

$$y^p - y = B(x)$$

with B a polynomial of degree d coprime to p . By [32, Lemma 12.1(b)] the genus of $\mathcal{X}$ is $(p - 1)(d - 1)/2$. Then, by Proposition 2.7, $d = p + 1$ holds.

This means that $\mathcal{X}$ is a non-singular plane curve and therefore the group G consists of linear transformations fixing the points of $\mathcal{X}$; see [32, Theorem 11.29]. Clearly G must fix the point at infinity of the Y -axis and the tangent

line of $\mathcal{X}$ at that point, namely the ideal line. It was noticed in [1] that for a p -element in the projective linear group $\mathrm{PGL}(3, \mathbb{K})$ represented by a matrix

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

with $a, b, c \in \mathbb{K}$, the equation

$$A^p = A_{pa, pb, p^{\frac{p-1}{2}}ab+pc} = I_3,$$

holds for $p > 2$. Then, there cannot exist an element of G of order p^2 . Thus $h = 1$ and by [34] an equation of $\mathcal{X}$ is $y^2 = x^p - x$. $\square$

Remark 2.9. In [47] it is shown that $2g(\mathcal{X})p/(p-1)$ is an upper bound for the size of an abelian p -group of automorphisms of a curve $\mathcal{X}$. By the result of the present section, the bound can be improved in the cyclic case whenever $g(\mathcal{X}) > \frac{p-1}{2}$.

The case $N = p^h m$ with $m > 1$ and $(p, m) = 1$

Let M be the subgroup of G of order m and let S be the subgroup of G of order p^h . Also, let H be the factor group G/M . Then H is a cyclic group of order p^h acting on the quotient curve $\mathcal{X}/M$.

Proposition 2.10. Assume that $N = p^h m \geq 2g(\mathcal{X}) + 1$ with $p \geq 3$, $m > 1$, and $(p, m) = 1$. If $\mathcal{X}/M$ is elliptic, then $p = 3$, $h = 1$, the p -rank of $\mathcal{X}/M$ is zero, and H does not act semiregularly on $\mathcal{X}/M$.

Proof. By Proposition 1.116 it is enough to show that $\mathcal{X}/M$ is not ordinary. Assume by contradiction that the p -rank of $\mathcal{X}/M$ is equal to 1. Then by Proposition 1.116, H acts semiregularly on $\mathcal{X}/M$. Therefore, also $\mathcal{X}/G$ is elliptic and the Riemann-Hurwitz genus formula applied to G gives

$$2g(\mathcal{X}) - 2 = \sum_{i=1}^r (N - \ell_i),$$

where r is the number of short orbits under G and ℓ_i denote their sizes. As $N - \ell_i \geq N/2$ we have that if $r \geq 2$ then

$$2g(\mathcal{X}) - 2 \geq N,$$

a contradiction. Therefore, $r = 1$ holds. Moreover, no p -element of G fixes a point in $\mathcal{X}$ and therefore $\ell_1 = p^h m'$ with $m' < m$ a divisor of m .

Note that $\mathcal{X}/S$ is a cyclic extension of $\mathcal{X}/G$ of order m , and hence it is a Kummer extension with Galois group G/S . However, there is only one short orbit of $\mathcal{X}/S$ under the action of G/S . This is impossible by Proposition 1.118. $\square$

Proposition 2.11. *Assume that $N = p^h m$ with $p \geq 3$, $m > 1$, and $(p, m) = 1$. If $N \geq 2g(\mathcal{X}) + 1$, then $h \leq 2$.*

Proof. Recall that H is a cyclic group of order p^h acting on the quotient curve $\mathcal{X}/M$. Let $\hat{g}$ be the genus of $\mathcal{X}/M$. Three cases are distinguished.

- $\hat{g} = 0$. By the classification of subgroups of $\mathrm{PGL}(2, \mathbb{K})$ it follows that $h = 1$ holds in this case.
- $\hat{g} = 1$. By Proposition 2.10 we have $h = 1$.
- $\hat{g} \geq 2$. By the Riemann-Hurwitz genus formula applied to M we have

$$2g(\mathcal{X}) - 2 \geq m(2\hat{g} - 2),$$

that is

$$(2\hat{g} - 2) \leq \frac{2g(\mathcal{X}) - 2}{m} = \frac{2g(\mathcal{X}) + 1 - 3}{m} \leq p^h - \frac{3}{m},$$

and hence

$$|H| \geq 2\hat{g}(\mathcal{X}) - 2 + \frac{3}{m}$$

which implies

$$|H| \geq 2\hat{g} - 1;$$

finally, Proposition 2.6 applies. $\square$

Proposition 2.12. *Assume that $N = p^h m \geq 2g(\mathcal{X}) + 1$ with $p \geq 3$, $m > 1$, and $(p, m) = 1$. Let S be the subgroup of G of order p^h . Then $h = 1$ and one of the following holds:*

- (i) $\gamma(\mathcal{X}/M) = 0$ and $g(\mathcal{X}/S) \leq 1$; also, the only non-tame orbit Ω under the action of G has size $|\Omega| \leq 3$ for $g(\mathcal{X}/S) = 1$ and $|\Omega| \leq 2$ for $g(\mathcal{X}/S) = 0$. If $g(\mathcal{X}/S) = 1$, then $m \in \{2, 3, 4, 6\}$.

(ii) $\gamma(\mathcal{X}/M) = g(\mathcal{X}/M) = 2$ and $p = 3$; the group G/M of order 3 fixes two points on $\mathcal{X}/M$ and acts semiregularly on the other points. Also, up to birational equivalence $\mathcal{X}/M$ has affine equation

$$by^3 + cy = ax + 1/x,$$

where $a, b, c \in \mathbb{K}^*$, H consists of the maps

$$y \mapsto y + v, \quad x \mapsto x,$$

where v runs over the roots of $bY^3 + cY$, and $|\text{Aut}(\mathcal{X}/M)| = 12$.

Proof. By the proof of Proposition 2.11, the quotient curve $\mathcal{X}' = \mathcal{X}/M$ of genus $\hat{g}$ admits a cyclic automorphism group H of size p^h with $p^h \geq 2\hat{g} - 1$.

Assume that the p -rank of $\mathcal{X}'$ is greater than zero. From $p^h \geq 2\hat{g} - 1$ it follows by [52, Theorem 1] that either $\hat{g} = 1$ or $\hat{g} \geq 2$ and $p = 3$. The former case is ruled out by Proposition 2.10. In the latter case, it has already been noticed in the proof of Proposition 2.6 that $p^h = 3$ holds and therefore $\hat{g} = 2$. Then, (ii) holds by Proposition 1.117.

Assume now that the p -rank of $\mathcal{X}'$ is zero. Then H fixes one point $\bar{P}$ of $\mathcal{X}'$ and acts semiregularly on the other points. Let Ω be the orbit of $\mathcal{X}$ under the action of M corresponding to the point $\bar{P}$ of $\mathcal{X}'$. Clearly Ω is the only non-tame orbit under the action of G .

Moreover, Ω is both an M -orbit and a G -orbit, as $s(\bar{P}) = \bar{P}$ for each $s \in S$. This means that for each point $P \in \Omega$ we have

$$|\Omega| = \frac{p^h m}{|G_P|} = \frac{m}{|M_P|}$$

which implies that $p^h \mid |G_P|$ and $p^h = |G_P^{(1)}|$, that is, $G_P = H \times M_P$. Let $m' = \frac{m}{|\Omega|} = |M_P|$.

We apply the Riemann-Hurwitz genus formula to H and we denote by $\tilde{g}$ the genus of $\mathcal{X}/S$.

First, we show that the case $h = 2$ cannot actually occur. Assume that $|S| = |H| = p^2$. Since G_P is abelian and $G_P/G_P^{(1)}$ has order m' , by [32, Lemma 11.75 (iv)] we have that there exist positive integers v and w such that

$$S = G_P^{(1)} = G_P^{(2)} = \dots = G_P^{(vm')},$$

and

$$|G_P^{(vm'+1)}| = \dots = |G_P^{((v+w)m')}| = p,$$

and $|G_P^{((v+w)m'+1)}| = 1$.

Taking into account [32, Lemma 11.75 (v)], we have

$$vm' \equiv (v+w)m' \pmod{p}$$

and since $(m', p) = 1$ we have that p divides w . Therefore, $w \geq p$ yields

$$2g(\mathcal{X}) - 2 \geq p^2(2\tilde{g} - 2) + |\Omega|(m'p^2 - m' + p^2 - 1 + p^2m' - pm')$$

and hence

$$p^2m - 3 \geq -2p^2 + 2mp^2 - m(p+1) + |\Omega|(p^2 - 1)$$

whence

$$2p^2 - 3 \geq m(p^2 - p - 1) + |\Omega|(p^2 - 1) \geq 2(p^2 - p - 1) + p^2 - 1$$

and

$$p^2 - 2p \leq 0$$

a contradiction.

Therefore, $h = 1$ can be assumed. By the Riemann-Hurwitz genus formula applied to S , taking into account (iv) of [32, Lemma 11.75] we have

$$mp - 3 \geq 2g(\mathcal{X}) - 2 \geq p(2\tilde{g} - 2) + |\Omega|((m' + 1)(p - 1))$$

and hence

$$m \geq p(2\tilde{g} - 2) + 3 + |\Omega|(p - 1).$$

Note that this is a contradiction with the bound on the size of an abelian subgroup of the automorphism group of $\mathcal{X}/S$ (see [32, Theorem 11.79]), unless $\tilde{g} \leq 1$ or $p = 3$, $\tilde{g} = 2$, and $|\Omega| = 1$. However, by [32, Theorem 11.60], the latter case cannot actually occur taking into account that M fixes a point.

Therefore, either $\tilde{g} = 0$ or $\tilde{g} = 1$.

Observe that $m > |\Omega|$ holds with the only exception $m = |\Omega| = 2$ for $\tilde{g} = 0$.

To investigate $|\Omega|$ we first assume that $\tilde{g} = 0$. Then G/S is a cyclic group of order m coprime with p acting on the projective line on an algebraically closed field of characteristic p . Therefore, if a non-trivial element of G/S fixes a point, then it has precisely two fixed points on $\mathcal{X}/S$ and acts semiregularly on the other points. It has already been noticed that either $m > |\Omega|$ or $m = |\Omega| = 2$. Assume that $m > |\Omega|$. As each point in Ω is fixed by S , there

exist $|\Omega|$ points on the projective line fixed by some elements in G/S ; therefore $|\Omega| \leq 2$.

If $\tilde{g} = 1$, then $m > |\Omega|$ and hence G/S admits a non-trivial (cyclic) subgroup of size $m' = m/|\Omega| > 1$ fixing each point of $\mathcal{X}/S$ corresponding to a point in Ω . Then G/S does not act semiregularly on $\mathcal{X}/S$ and by Proposition 1.116 we have $m \in \{2, 3, 4, 6\}$. As $m = m'|\Omega|$ one of the following holds:

- (e1) $m = m' = 2, |\Omega| = 1$;
- (e2) $m = m' = 3, |\Omega| = 1$;
- (e3) $m = m' = 4, |\Omega| = 1$;
- (e4) $m = 4, m' = 2, |\Omega| = 2$;
- (e5) $m = m' = 6, |\Omega| = 1$;
- (e6) $m = 6, m' = 2, |\Omega| = 3$;
- (e7) $m = 6, m' = 3, |\Omega| = 2$.

□

Proposition 2.13. *Assume that $N = pm \geq 2g(\mathcal{X}) + 1$ with $p \geq 3$, $m > 1$, and $(p, m) = 1$. Let S be the subgroup of G of order p and M the subgroup of G of order m . If $\mathcal{X}/M$ is not rational then $p = 3$ and $g(\mathcal{X}/M) \in \{1, 2\}$.*

Proof. Let $\hat{g}$ denote $g(\mathcal{X}/M)$ and let $H = G/M$. By Proposition 2.12, either $\mathcal{X}/M$ has p -rank equal to zero, or $p = 3$, $\hat{g} = 2$, and we are in case (ii) of Proposition 2.12. Assume that the former case holds, and as in the proof of Proposition 2.12 let Ω be the only non-tame orbit under the action of G . First, we prove that the extension $\mathcal{X}$ over $\mathcal{X}/M$ ramifies. Assume by contradiction that the extension is unramified; then, in particular, $m = |\Omega|$ holds. From the proof of Proposition 2.12, we have that $m = 2$ and $\mathcal{X}/S$ is rational. Also,

$$2p - 3 \geq 2g(\mathcal{X}) - 2 = 4\hat{g} - 4.$$

Then $p \geq 2\hat{g} - \frac{1}{2}$. As $g(\mathcal{X}) \geq 2$ we have that $\hat{g} \geq 2$ as well. By [34], $p = 2\hat{g} + 1$ and hence $2g(\mathcal{X}) - 2 = 2(p - 3)$. This yields $g(\mathcal{X}) + 2 = p$ which is impossible by [34].

Since the extension is a Kummer extension, by Proposition 1.118 it is not possible that Ω is the only short orbit of $\mathcal{X}$ under the action of M . Therefore,

there exists a short orbit $\Omega' \neq \Omega$ under the action of M . If $\hat{g} > 2$ or $\hat{g} = 2$ and $p > 3$ then Ω' is not fixed by S (see the proof of Proposition 2.12). A proper subgroup M' of M fixes each point in Ω' . On the other hand, S acts on the set of fixed points by M' semiregularly, since $S(\Omega') \neq \Omega'$. Therefore, M has at least p short orbits of size Ω' , other than Ω .

Hence,

$$pm - 3 \geq 2g(\mathcal{X}) - 2 \geq m(2\hat{g} - 2) + m - |\Omega| + p(m - |\Omega'|).$$

Therefore,

$$p \geq \frac{m}{|\Omega'|}(2\hat{g} - 2) + \frac{m + 3 - |\Omega|}{|\Omega'|}$$

Note that $\frac{m+3-|\Omega|}{|\Omega'|}$ is strictly greater than 1 as, for $m > |\Omega|$ we have

$$\frac{m + 3 - |\Omega|}{|\Omega'|} \geq \frac{m + 3 - \frac{m}{2}}{\frac{m}{2}},$$

whereas $m = |\Omega|$ yields $m = 2$ and hence $\frac{m+3-|\Omega|}{|\Omega'|} = 3$.

Then,

$$p \geq \frac{m}{|\Omega'|}(2\hat{g} - 2) + 2 \geq 4\hat{g} - 2 > 2\hat{g} + 1.$$

By [34], $\hat{g} \leq 1$ holds and by Proposition 2.10 we have that $\hat{g} = 1$ implies $p = 3$. $\square$

Proposition 2.14. *Let $p \geq 3$. Let G be a cyclic group of automorphisms acting on a curve $\mathcal{X}$ of genus $g(\mathcal{X}) \geq 2$ of order N greater than or equal to $2g(\mathcal{X}) + 1$. If $|G| = p^h m$ with $h \geq 1$, $m > 1$, and $(p, m) = 1$ then $|G| = pm$. Also, for S the subgroup of G of order p and M the subgroup of G of order m , one of the following holds:*

- (Ia) $g(\mathcal{X}/M) = g(\mathcal{X}/S) = 0$, $g(\mathcal{X}) = \frac{1}{2}(p-1)(m-1)$, and S fixes exactly one point;
- (Ib) $g(\mathcal{X}/M) = g(\mathcal{X}/S) = 0$, $m = 2$, $g(\mathcal{X}) = p-1$, and S fixes exactly two points.

Proof. Recall that G/S is cyclic group of order $m = N/p$ acting on $\mathcal{X}/S$. Also, points of $\mathcal{X}/S$ are either fully ramified or unramified with respect to the covering $\mathcal{X} \rightarrow \mathcal{X}/S$.

We first prove that the p -rank $\gamma(\mathcal{X}/M)$ of $\mathcal{X}/M$ is equal to 0. Assume on the contrary that $\gamma(\mathcal{X}/M) > 0$. Then, by Proposition 2.12, we are in the following setting: $p = 3$ and $\mathcal{X}/M$ is an ordinary curve of genus 2; the group G/M of order 3 fixes two points on $\mathcal{X}/M$ and acts semiregularly on the other points.

We are going to show that actually such situation cannot occur. As $g(\mathcal{X}/M) = 2$ and $3m \geq 2g(\mathcal{X}) + 1$, the Riemann-Hurwitz formula applied to M gives

$$3m - 3 \geq 2g(\mathcal{X}) - 2 = 2m + \sum_{i=1}^n (m - |\Omega_i|) \geq 2m + n \frac{m}{2},$$

where $\Omega_1, \dots, \Omega_n$ are the short orbits of M on $\mathcal{X}$. Therefore, $n \leq 1$ holds. However, by Proposition 1.118, we have $n = 0$, and hence $g(\mathcal{X}) = m + 1$. Now, let $\bar{P}_1, \bar{P}_2$ be the two points on $\mathcal{X}/M$ fixed by G/M . Then, S fixes each point from the two (long) M -orbits, say Ω_1 and Ω_2 , lying over $\bar{P}_1$ and $\bar{P}_2$. This means that S fixes at least $2m$ points of $\mathcal{X}$. However, by [32, Lemma 11.106] the maximum number of fixed points of S is

$$2 + \frac{2g(\mathcal{X})}{|S| - 1} = m + 3,$$

which yields $m = 2$. However, for $m = 2$, $p = 3$, and $g(\mathcal{X}) = 3$, we have that $pm \geq 2g(\mathcal{X}) + 1$ does not hold.

So, from now on we assume that the p -rank of $\mathcal{X}/M$ is zero. Then, by Propositions 2.10, 2.12 and 2.13 we have the following information:

- $g(\mathcal{X}/M) \leq 1$. Moreover, $g(\mathcal{X}/M) = 1$ implies $p = 3$;
- $g(\mathcal{X}/S) \leq 1$;
- there exists a unique non-tame orbit Ω under the action of G on $\mathcal{X}$.

Clearly, fully ramified points of $\mathcal{X}/S$ correspond to the points of Ω , and with a slight abuse of notation they will be identified with the points of Ω . If a point $\bar{P} \in \mathcal{X}/S$ not in Ω is fixed by an element $\bar{\alpha}$ in G/S , then the element of M of the same order, say α , fixes all the p points over $\bar{P}$ with respect to the covering $\mathcal{X} \rightarrow \mathcal{X}/S$. On the other hand, if $\bar{P} \in \Omega$ then α fixes the only point over $\bar{P}$. Now, let v be the number of points fixed by M in $\mathcal{X}$. We distinguish two cases according to whether $g(\mathcal{X}/S) = 0$ or $g(\mathcal{X}/S) = 1$.

CASE 1: $g(\mathcal{X}/S) = 0$.

In this case, either G/S doesn't fix any point of $\mathcal{X}/S$, or it fixes two points and acts semiregularly on the other points of $\mathcal{X}/S$. Note also that in the latter case these two points cannot be both in Ω , as Ω is an M -orbit (see the proof of Proposition 2.12). Taking into account that when $g(\mathcal{X}/S) = 0$ then $|\Omega| \leq 2$, by the discussion above we have

$$v \in \{0, p+1, 2p\},$$

and $v = 2p$ can occur only when $|\Omega| = m = 2$.

We now show that $g(\mathcal{X}/M) = 0$. If on the contrary $g(\mathcal{X}/M) = 1$, then $p = 3$, and by the Riemann-Hurwitz formula applied to M we have

$$2g(\mathcal{X}) - 2 = v(m-1) \in \{0, 4(m-1), 6\},$$

a contradiction.

Then $g(\mathcal{X}/M) = 0$ and by the Riemann-Hurwitz formula applied to M we have

$$2g(\mathcal{X}) - 2 = -2m + v(m-1) = (v-2)m - v;$$

hence,

$$2g(\mathcal{X}) - 2 \in \{-2m, (p-1)(m-1) - 2, 2p-4\}.$$

As $2g(\mathcal{X}) - 2 = -2m$ cannot occur, we have that either (Ia) or (Ib) holds.

CASE 2: $g(\mathcal{X}/S) = 1$.

By Proposition 2.12 and its proof, we know that $m > |\Omega|$, G/S admits a (non-trivial) cyclic subgroup of order $m' = m/|\Omega|$ fixing each point of $\mathcal{X}/S$ corresponding to a point in Ω , and one of the cases (e1)-(e7) holds. We will prove that each of these cases cannot actually occur. To do so, first note that by the Riemann-Hurwitz formula we have

$$2g(\mathcal{X}) - 2 = m(2g(\mathcal{X}/M) - 2) + \sum_{\alpha \in M, \alpha \neq id} N(\alpha) \geq -2m + \sum_{\alpha \in M, \alpha \neq id} N(\alpha), \quad (2.2)$$

where $N(\alpha)$ is the number of points of $\mathcal{X}$ fixed by α . We show that provides a contradiction with $N = pm \geq 2g(\mathcal{X}) + 1$ in each of the cases (e1)-(e7).

(e1) $m = 2$, $|\Omega| = 1$, G/S fixes 4 points, and one of such points is in Ω .

Then, Equation (2.2) yields

$$2g(\mathcal{X}) - 2 \geq -2(2) + 1 + 3p,$$

a contradiction.

- (e2) $m = 3$, $|\Omega| = 1$, G/S fixes 3 points, and one of such points is in Ω . Then, Equation (2.2) yields

$$2g(\mathcal{X}) - 2 \geq -2(3) + 2(1 + 2p),$$

a contradiction.

- (e3) $m = 4$, $|\Omega| = 1$, G/S fixes the point in Ω and one point not in Ω , whereas its subgroup of order 2 fixes the point in Ω and two points not in Ω . Then, Equation (2.2) yields

$$2g(\mathcal{X}) - 2 \geq -2(4) + (p + 1 + p + 1 + 3p + 1),$$

a contradiction.

- (e4) $m = 4$, $|\Omega| = 2$, G/S fixes two points not in Ω , whereas its subgroup of order 2 fixes two points in Ω and two points not in Ω . Then, Equation (2.2) yields

$$2g(\mathcal{X}) - 2 \geq -2(4) + (2p + 2p + 2p + 2),$$

a contradiction.

- (e5) $m = 6$, $|\Omega| = 1$, G/S fixes the point in Ω , its subgroup of order 3 fixes two more points not in Ω , and its subgroup of order 2 fixes 3 more points not in Ω . Then, Equation (2.2) yields

$$2g(\mathcal{X}) - 2 \geq -2(6) + (1 + 1 + 1 + 2p + 1 + 2p + 1 + 3p),$$

a contradiction, unless $p = 3$. However, in this case $p = 3$ is not possible as $p = 3$ divides $m = 6$.

- (e6) $m = 6$, $|\Omega| = 3$, G/S fixes one point not in Ω , its subgroup of order 3 fixes three points not in Ω , and its subgroup of order 2 fixes the three points in Ω and one point not in Ω . Then, Equation (2.2) yields

$$2g(\mathcal{X}) - 2 \geq -2(6) + (p + p + 3p + 3p + 3 + p),$$

a contradiction.

- (e7) $m = 6$, $|\Omega| = 2$, G/S fixes one point not in Ω , its subgroup of order 3 fixes two points in Ω and one point not in Ω , and its subgroup of order 2 fixes four points not in Ω . Then, Equation (2.2) yields

$$2g(\mathcal{X}) - 2 \geq -2(6) + (p + p + p + 2 + p + 2 + 4p),$$

a contradiction.

□

Proposition 2.15. *In Case (Ia) of Proposition 2.14, up to birational equivalence $\mathcal{X}$ is the curve of affine equation*

$$y^p - y = a(x^m - b),$$

with $a, b \in \mathbb{K}$.

Proof. By [32, Theorem 12.5], an equation for $\mathcal{X}$ is

$$y^p - y = B(x),$$

where B is a polynomial of degree d . Since the genus of this curve is $(p-1)(d-1)/2$ we have that $m = d$. Also, the fixed field of S is $\mathbb{K}(x)$. Two orbits under the action of S are fixed by G/S , one of size p , say Ω_1 , and the other consisting of the single point in Ω . Clearly the only pole of x in $\mathcal{X}/S$, namely the ideal point of the projective line, corresponds to Ω . Let P_1 be the point lying under Ω_1 and let $a \in \mathbb{K}$ coincide with $x(P_1)$. Without loss of generality we can assume that $a = 0$. Then the divisor of x on $\mathcal{X}$ is preserved by every element in G .

Let σ be a generator of G . Then $\text{div}(\sigma^*(x)) = \text{div}(x)$ and therefore, $\sigma^*(x) = \mu x$ for some $\mu \in \mathbb{K}$. By $\sigma^{pm} = 1$ we deduce that $\mu^m = 1$.

Consider $(\sigma^p)^*(x)$; clearly, $(\sigma^p)^*(x) = \nu x$ holds for some m -th root of unity ν . We claim that ν is primitive. In fact, if $\nu^h = 1$ for a proper divisor of m , then x would be fixed by σ^{ph} , which is not in H and this would contradict that $\mathbb{K}(x)$ is the fixed field of S . As x^m is fixed by G , and the degree of the extension $\mathbb{K}(\mathcal{X})$ over $\mathbb{K}(x^m)$ coincides with $pm = |G|$, we have that $\mathbb{K}(x^m)$ is the fixed field of G . Note that $\mathbb{K}(y)$ and the fixed field of M are both intermediate fields between $\mathbb{K}(\mathcal{X})$ and $\mathbb{K}(x^m)$ such that the degrees $\mathbb{K}(\mathcal{X}) : \mathbb{K}(y)$ and $\mathbb{K}(\mathcal{X}) : \text{Fix}(M)$ are both equal to m . Since G has a unique subgroup of order m , we have that $\mathbb{K}(y)$ is the fixed field of M and hence M fixes y .

Therefore, taking into account that $M = \langle \sigma^p \rangle$, we have that for each $j = 1, \dots, m-1$,

$$(\sigma^{jp})^*(y^p) - (\sigma^{jp})^*(y) = B((\sigma^{jp})^*(x)),$$

which implies

$$y^p - y = B(\nu^j x),$$

and hence

$$B(x) = B(\nu^j x)$$

holds for each $j = 1, \dots, m - 1$.

Since ν is a primitive m -th root of unity, we have $B(x) = a(x^m - z_0)$ for some $z_0 \in \mathbb{K}$. $\square$

Proposition 2.16. *In Case (Ib) of Proposition 2.14, up to birational equivalence $\mathcal{X}$ is the curve of affine equation*

$$by^p + cy = ax + \frac{1}{x}$$

with $a, b, c \in \mathbb{K}$.

Proof. For $m = 2$ and $g(\mathcal{X}) = p - 1$ Proposition 1.117 applies. Then an affine equation for $\mathcal{X}$ is either

$$by^p + cy = ax + \frac{1}{x},$$

or

$$by^p + cy = x^3 + bx.$$

In the former case, clearly $\mathcal{X}$ admits a cyclic automorphism group of size $2p$ consisting of the maps

$$y \mapsto y + \gamma, \quad x \mapsto 1/(ax),$$

and

$$y \mapsto y + \gamma, \quad x \mapsto x,$$

where γ runs over the roots of $bY^p + cY$. In the latter case, the group of order p fixes only one point, contradicting $|\Omega| = 2$. $\square$

The following statement summarizes the results obtained in this subsection.

Theorem 2.17. *If $|G| = p^h m$ with $h \geq 1$ and $(p, m) = 1$ then $|G| = pm$ with $m > 1$, $p \neq 3$ and*

$$g(\mathcal{X}) \in \{(p - 1)(m - 1)/2, p - 1\};$$

also, $\mathcal{X}$ is an Artin-Schreier extension of the projective line. Specifically, up to birational equivalence, if $g(\mathcal{X}) = (p - 1)(m - 1)/2$, then

$$\mathcal{X} : y^p - y = a(x^m - b),$$

with $a, b \in \mathbb{K}$, whereas if $g(\mathcal{X}) = p - 1$ then

$$\mathcal{X} : by^p + cy = ax + \frac{1}{x},$$

with $a, b, c \in \mathbb{K}$.

2.2.2 Proof of Theorem 2.5 when p does not divide N

In [36] a classification of curves admitting a large cyclic automorphism group was given for the case $\mathbb{K} = \mathbb{C}$. Here we prove that an analogue result holds when the characteristic p does not divide the size of the cyclic group. Most of the steps in the proof presented in [36] hold with little modifications; however, some exceptions arise for implications that depend on topological results (see, for example, theorems from references [2] and [3] in [36]).

Throughout the Section, $p > 2$ and $(p, N) = 1$ are assumed. We will show that if $N \geq 2g(\mathcal{X}) + 1$ then (I) in Theorem 2.5 holds.

Let $G = \langle \sigma \rangle$ and $\{\lambda_1, \dots, \lambda_n\}$ be the set of points of $\mathcal{X}/G$ where the covering $\pi : \mathcal{X} \rightarrow \mathcal{X}/G$ ramifies. Using the same terminology and notation as in [36], the automorphism σ is called of kind $(g_0; e_1, e_2, \dots, e_n)$ if the genus of $\mathcal{X}/G$ is g_0 and the ramification index at P_i is e_i , where P_i is any point in $\mathcal{X}$ such that $\pi(P_i) = \lambda_i$.

Proposition 2.18. *Let M be the l.c.m. of $\{e_1, \dots, e_n\}$. Then the following hold:*

- i) $n \geq 2$ and if $g_0 = 0$ then $n \geq 3$;
- ii) M divides N , and, if $g_0 = 0$, $M = N$;
- iii) the l.c.m. of $\{e_1, \dots, \hat{e}_i, \dots, e_n\}$ is M for each i , where $\hat{e}_i$ denotes the omission of e_i .

Proof. i) By Proposition 1.118 and Proposition 1.123 $n \geq 2$ holds. Assuming $g_0 = 0$ and $n = 2$, the Riemann-Hurwitz formula gives

$$2g(\mathcal{X}) - 2 = -2N + \frac{N}{e_1}(e_1 - 1) + \frac{N}{e_2}(e_2 - 1)$$

that is

$$2g(\mathcal{X}) - 2 = -\frac{N}{e_1} - \frac{N}{e_2},$$

which contradicts $g(\mathcal{X}) \geq 2$.

- ii) As each e_i divides N , the same holds for M . Moreover, by Proposition 1.124, the covering $\mathcal{X}/\langle \sigma^{N/M} \rangle \rightarrow \mathcal{X}/G$ is unramified, and hence the Riemann-Hurwitz formula for the covering $\mathcal{X}/\langle \sigma^{N/M} \rangle \rightarrow \mathcal{X}/G$, together with $g_0 = 0$, reads

$$2\bar{g} - 2 = -2\frac{N}{M},$$

where $\bar{g}$ is the genus of $\mathcal{X}/\langle\sigma^{N/M}\rangle$. This implies $\bar{g} = 0$ and $N = M$.

- iii) Let M_i be the *l.c.m.* of $\{e_1, \dots, \hat{e}_i, \dots, e_n\}$. If there exists $j \neq i$ such that $e_j = e_i$ then clearly $M_i = M$. So, assume $e_j \neq e_i$ for each $j \neq i$. Then, by Proposition 1.124 with $d = M_i$, the covering $\mathcal{X}/\langle\sigma^{N/M_i}\rangle \rightarrow X/G$ can be ramified only over λ_i . As this is not possible by Proposition 1.118, $\mathcal{X}/\langle\sigma^{N/M_i}\rangle$ over X/G is unramified and hence e_i divides M_i , which concludes the proof. $\square$

Throughout this section, we denote by A_N the set

$$A_N = \{(r, s) \in \mathbb{Z}^2 : r, s \geq 1 \text{ and } r + s \leq N - 1\},$$

and, according to [36], we refer to an element $(r, s) \in A_N$ as a *primitive pair* if $\text{GCD}(r, s, N) = 1$.

We denote by $F(r, s)$ the non-singular model of equation $y^N = x^r(1 - x)^s$, with function field $\mathbb{K}(x, y)$ and genus $g(r, s)$. Let $\sigma(r, s)$ be the automorphism of $F(r, s)$ defined by

$$\sigma(r, s) : \begin{cases} x' = x, \\ y' = \zeta_N y, \end{cases}$$

where ζ_N is a primitive N -th root of unity. Since $p \nmid N$, $F(r, s)$ is a Kummer extension of the projective line $\mathbb{P}^1(\mathbb{K})$. We denote by

$$\pi(r, s) : F(r, s) \rightarrow \mathbb{P}^1(\mathbb{K})$$

the morphism induced by $\mathbb{K}(x) \subset \mathbb{K}(x, y)$. As (r, s) is a primitive pair, Kummer theory implies that $\pi(r, s)$ ramifies exactly at the three points $(0 : 1)$, $(1 : 1)$, and $(1 : 0)$.

Theorem 2.19. *If $(r, s) \in A_N$ is a primitive pair, then $N \geq 2g(r, s) + 1$.*

Proof. From Kummer theory and the Riemann-Hurwitz formula, we have

$$\begin{aligned} 2g(r, s) - 2 &= -2N + \text{GCD}(N, r) \left(\frac{N}{\text{GCD}(N, r)} - 1 \right) + \\ &\quad \text{GCD}(N, s) \left(\frac{N}{\text{GCD}(N, s)} - 1 \right) + \\ &\quad + \text{GCD}(N, r + s) \left(\frac{N}{\text{GCD}(N, r + s)} - 1 \right), \end{aligned}$$

which simplifies to

$$g(r, s) = \frac{1}{2} (N + 2 - \text{GCD}(N, r) - \text{GCD}(N, s) - \text{GCD}(N, r + s)).$$

This clearly implies that

$$N \geq 2g(r, s) + 1.$$

□

Another family of curves will play an important role in this section. For $\lambda \in \mathbb{K} \setminus \{0, 1\}$, let H_λ be the hyperelliptic curve of genus g defined by the equation $y^2 = (x^{g+1} - 1)(x^{g+1} - \lambda)$ and let τ_λ be an automorphism of H_λ defined by

$$\tau_\lambda^* : (x, y) \longmapsto (\zeta_{g+1}x, -y),$$

where ζ_{g+1} is a primitive $(g + 1)$ -th root of unity.

Theorem 2.20. *Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ admitting an automorphism of $\mathcal{X}$ of order $N \geq 2g(\mathcal{X}) + 1$, with $(p, N) = 1$. Then $\mathcal{X}$ is isomorphic to either $F(r, s)$ for some primitive pair $(r, s) \in A_N$ or to H_λ for some $\lambda \in \mathbb{K} \setminus \{0, 1\}$ with $N = 2g(\mathcal{X}) + 2$ and $g(\mathcal{X})$ even.*

Proof. Let σ be an automorphism of $\mathcal{X}$ of order N . Let $(g_0; e_1, e_2, \dots, e_n)$ be its type. We can assume that $e_1 \leq e_2 \leq \dots \leq e_n$ holds. By the Riemann-Hurwitz formula applied to $G = \langle \sigma \rangle$ we have

$$\frac{2g(\mathcal{X}) - 2}{N} = 2g_0 - 2 + \sum_{i=1}^n \left(1 - \frac{1}{e_i}\right). \quad (2.3)$$

We first prove the following three claims.

1. **$g_0 = 0$.** As $N \geq 2g(\mathcal{X}) + 1$, the left side of (2.3) is smaller than 1. Moreover, by Propositions 1.123 and 1.118, $n \geq 2$. This, together with $g_0 \geq 1$, would imply that the right side of (2.3) is greater than or equal to 1, a contradiction. So, $g_0 = 0$ holds.
2. **If N is odd, then $n = 3$.** Since $g_0 = 0$, we have $n \geq 3$ by Proposition 2.18. Observe that as N is odd, each e_i is odd. This together with (2.3) yields $n < 5$. We will now rule out the case $n = 4$. The possibilities for $n = 4$ are:
 - $n = 4$ and $e_1 \geq 5$. In this case the right-hand side of (2.3) is greater than 1, a contradiction.

- $n = 4$, $e_1 = 3$ and $e_2 \geq 5$. As above, the right-hand side of (2.3) is greater than 1.
 - $n = 4$, $e_1 = 3$, $e_2 = 3$ and $e_3 \geq 7$. Again, the right-hand side of (2.3) is greater than 1.
 - $n = 4$, $e_1 = e_2 = 3$ and $e_3 = 5$. By Proposition 2.18, $15 = \text{lcm}(e_1, e_2, e_3) = \text{lcm}(e_1, e_2, e_3, e_4)$, so either $e_4 = 5$ or $e_4 = 15$. Moreover, as $g_0 = 0$, again by Proposition 2.18 we have $N = \text{lcm}(e_1, e_2, e_3, e_4) = 15$. By (2.3) we obtain that either $g(\mathcal{X}) = 8$ or $g(\mathcal{X}) = 9$, but this contradicts $N \geq 2g(\mathcal{X}) + 1$.
 - $n = 4$, $e_1 = e_2 = e_3 = 3$. By Proposition 2.18 we have $3 = \text{lcm}(e_1, e_2, e_3) = \text{lcm}(e_1, e_2, e_3, e_4)$, from which $e_4 = 3$; again by Proposition 2.18 $N = \text{lcm}(e_1, e_2, e_3, e_4)$ holds. By replacing $e_1 = e_2 = e_3 = e_4 = N = 3$ and $g_0 = 0$ in (2.3) we have $g(\mathcal{X}) = 2$. Whence $N = 2g(\mathcal{X}) - 1$, against $N \geq 2g(\mathcal{X}) + 1$.
3. **If N is even, then either $n = 3$ or $n = 4$ and σ is of type $(0; 2, 2, g(\mathcal{X}) + 1, g(\mathcal{X}) + 1)$ with $g(\mathcal{X})$ even.** Arguing as above we want to prove that either $n = 3$ or $n = 4$, $e_1 = e_2 = 2$, $e_3 = e_4 = g(\mathcal{X}) + 1$ and $g(\mathcal{X})$ is even. With the same arguments of the previous item,
- the unique possibility for $n > 3$ is $n = 4$, $e_1 = e_2 = 2$, and $e_3 \geq 3$. Since from Proposition 2.18 we have $\text{lcm}(e_1, e_2, e_3, e_4) = \text{lcm}(e_1, e_2, e_3)$, then either $e_4 = e_3$ or $e_4 = 2e_3$ holds. In the latter case, by Proposition 2.18 $N = \text{lcm}(2, e_3, 2e_3) = 2e_3$, and from (2.3) we have

$$\frac{2g(\mathcal{X}) - 2}{2e_3} = 2 - \frac{1}{2} - \frac{1}{2} - \frac{1}{e_3} - \frac{1}{2e_3};$$

hence

$$2g(\mathcal{X}) = 2e_3 - 1 = N - 1,$$

a contradiction as N is even.

If, instead, $e_4 = e_3$, then (2.3) reads

$$\frac{2g(\mathcal{X}) - 2}{N} = 2 - \frac{1}{2} - \frac{1}{2} - \frac{1}{e_3} - \frac{1}{e_3}. \quad (2.4)$$

For N there are two possibilities: if e_3 is even, then $N = \text{lcm}(2, e_3) = e_3$, whereas if e_3 is odd, then $N = \text{lcm}(2, e_3) = 2e_3$.

Assume first that e_3 is even; then (2.4) reads

$$\frac{2g(\mathcal{X}) - 2}{e_3} = 2 - \frac{1}{2} - \frac{1}{2} - \frac{1}{e_3} - \frac{1}{e_3},$$

which implies $g(\mathcal{X}) = \frac{e_3}{2} = \frac{N}{2}$ against $N \geq 2g(\mathcal{X}) + 1$.

Finally, if e_3 is odd, then from (2.4) we have

$$\frac{2g(\mathcal{X}) - 2}{2e_3} = 2 - \frac{1}{2} - \frac{1}{2} - \frac{1}{e_3} - \frac{1}{e_3},$$

which yields $e_3 = g(\mathcal{X}) + 1$ and hence $N = 2g(\mathcal{X}) + 2$. In particular, $g(\mathcal{X})$ is even in this case.

We will continue the proof by showing that if $n = 3$ then $\mathcal{X}$ is birationally equivalent to $F(r, s)$ for some primitive pair $(r, s) \in A_N$, whereas if σ is of type $(0; 2, 2, g(\mathcal{X}) + 1, g(\mathcal{X}) + 1)$ and $g(\mathcal{X})$ is even then $\mathcal{X}$ is isomorphic to H_λ for some $\lambda \in \mathbb{K} \setminus \{0, 1\}$ with $N = 2g(\mathcal{X}) + 2$.

Recall that $\mathcal{X} \rightarrow \mathcal{X}/G$ is a cyclic covering of degree N with n ramification points and that $\mathcal{X}/G$ is the projective line $\mathbb{P}^1(\mathbb{K})$. Let x denote a generator of the function field of $\mathcal{X}/G$. For an element β in $\mathbb{K}$ let $S_\beta \in \mathbb{P}^1(\mathbb{K})$ denote the point such that $x(S_\beta) = \beta$; also, let S_∞ denote the only pole of x .

Assume first that $n = 3$ holds. Without loss of generality assume that the three ramification points of $\mathcal{X} \rightarrow \mathcal{X}/G$ are S_0, S_1, S_∞ . Since $\mathcal{X}$ is a Kummer extension of degree N of $\mathbb{K}(x)$, by ([64], Prop. 3.7.3 (b)) an equation for $\mathcal{X}$ is $y^N = \alpha(x)$, with

$\text{GCD}(\text{ord}_{S_0}(\alpha), N) < N$, $\text{GCD}(\text{ord}_{S_1}(\alpha), N) < N$, $\text{GCD}(\text{ord}_{S_\infty}(\alpha), N) < N$ and $\text{GCD}(\text{ord}_P(\alpha), N) = N$ for any other point $P \in \mathbb{P}^1(\mathbb{K})$, $P \notin \{S_0, S_1, S_\infty\}$. Now,

$$\begin{aligned} 0 = \sum_{P \in \mathbb{P}^1(\mathbb{K}), \text{ord}_P(\alpha) \neq 0} \text{ord}_P(\alpha) &= \text{ord}_{S_0}(\alpha) + \text{ord}_{S_1}(\alpha) + \text{ord}_{S_\infty}(\alpha) + \\ &\sum_{P \in \mathbb{P}^1(\mathbb{K}), P \neq S_0, S_1, S_\infty, \text{ord}_P(\alpha) \neq 0} \text{ord}_P(\alpha). \end{aligned} \quad (2.5)$$

Let $R_1, \dots, R_k$ be the points of $\mathbb{P}^1(\mathbb{K})$ where the order of α is different from 0 and it is a multiple of N , and put $\beta_i = x(R_i)$. Therefore,

$$\text{ord}_{R_1}(\alpha) = Nh_1, \dots, \text{ord}_{R_k}(\alpha) = Nh_k$$

for suitable integers $h_1, \dots, h_k$. Then (2.5) becomes

$$0 = \text{ord}_{S_0}(\alpha) + \text{ord}_{S_1}(\alpha) + \text{ord}_{S_\infty}(\alpha) + \sum_{i=1}^k \text{ord}_{R_i}(\alpha).$$

Since $\text{ord}_{R_1}(\alpha) = Nh_1$, α will be of the form $\alpha(x) = (x - \beta_1)^{Nh_1}\alpha_1(x)$ with $\text{ord}_{R_1}(\alpha_1) = 0$.

Consider

$$\begin{cases} y' = \frac{y}{(x - \beta_1)^{h_1}} \\ x' = x \end{cases}, \quad (2.6)$$

then

$$(y')^N = \frac{y^N}{(x - \beta_1)^{Nh_1}} = \alpha_1(x').$$

Therefore, (2.6) defines an isomorphism between the curves $y^N = \alpha(x)$ and $y^N = \alpha_1(x)$.

Moreover, for each $P \in \mathbb{P}^1(\mathbb{K})$ we have

$$\text{ord}_P(\alpha) = Nh_1 \cdot \text{ord}_P(x - \beta_1) + \text{ord}_P(\alpha_1),$$

whence $\text{ord}_P(\alpha) = \text{ord}_P(\alpha_1)$ for any P different from R_1 and S_∞ . So, up to replacing $\alpha(x)$ with $\alpha_1(x)$, we may assume $\text{ord}_{R_1}(\alpha) = 0$. By repeating this process for any $i = 1, \dots, k$, we obtain that, up to birational equivalence, a defining equation for $\mathcal{X}$ is $y^N = \alpha(x)$ with $\text{ord}_P(\alpha) \neq 0$ just in $\{S_0, S_1, S_\infty\}$. Also, either α has two zeros and one pole, or it has two poles and one zero. Actually, if α has two poles and one zero we can replace y with $y' = \frac{1}{y}$ and $\mathcal{X}$

with the curve defined by $(y')^N = \frac{1}{\alpha}$. So, we can assume that α has S_0 and S_1 as zeros, and S_∞ as the unique pole, whence $\alpha(x) = f(x)$ with $f(x) \in \mathbb{K}[x]$. Now, if $r := \text{ord}_{S_0}(f(x))$ and $s := \text{ord}_{S_1}(f(x))$, then $f(x) = x^r(x - 1)^s$ can be assumed. This proves our claim for $n = 3$, as $\text{GCD}(r, s, N) = 1$ follows from the irreducibility of the equation.

Suppose now that $n = 4$, σ is of type $(0; 2, 2, g(\mathcal{X}) + 1, g(\mathcal{X}) + 1)$ and $g(\mathcal{X})$ even. The Riemann-Hurwitz genus formula reads

$$2g(\mathcal{X}) - 2 = -2N + \frac{N}{2} + \frac{N}{2} + \frac{N}{g(\mathcal{X}) + 1}g(\mathcal{X}) + \frac{N}{g(\mathcal{X}) + 1}g(\mathcal{X}),$$

which implies

$$N = 2g(\mathcal{X}) + 2.$$

We can assume that $\pi : \mathcal{X} \rightarrow \mathcal{X}/G$ ramifies at $S_\theta, S_0, S_1, S_\infty$ with $\theta \in \mathbb{K} \setminus \{0, 1\}$ and that

$$\pi^{-1}(S_\theta) = \{P, \sigma(P), \dots, \sigma^{g(\mathcal{X})}(P)\}, \quad \pi^{-1}(S_1) = \{Q, \sigma(Q), \dots, \sigma^{g(\mathcal{X})}(Q)\},$$

$$\pi^{-1}(S_0) = \{P_0, \sigma(P_0)\}, \quad \pi^{-1}(S_\infty) = \{P_\infty, \sigma(P_\infty)\}.$$

Now, if we let $\tau := \sigma^{g(\mathcal{X})+1}$, then τ fixes exactly the set of points

$$\{P, \sigma(P), \dots, \sigma^{g(\mathcal{X})}(P), Q, \sigma(Q), \dots, \sigma^{g(\mathcal{X})}(Q)\}$$

and the Riemann-Hurwitz formula for the covering $\mathcal{X} \longrightarrow \mathcal{X}/\langle \tau \rangle$ reads

$$2g(\mathcal{X}) - 2 = 2(2g' - 2) + (2g(\mathcal{X}) + 2),$$

where g' is the genus of $\mathcal{X}/\langle \tau \rangle$. Hence $g' = 0$ holds and $\mathbb{K}(\mathcal{X}/\langle \tau \rangle) = \mathbb{K}(t)$ for some $t \in \mathbb{K}(\mathcal{X})$ and $\mathcal{X}$ is hyperelliptic. Also,

$$\operatorname{div}(t) = P_0 + \sigma(P_0) - P_\infty - \sigma(P_\infty).$$

By [64, Proposition 6.2.3 (c)], $\mathcal{X}$ has equation $y^2 = f(t)$, for a suitable $f \in \mathbb{K}[t]$ whose zeros are exactly the $2g(\mathcal{X}) + 2$ places of $\mathbb{K}(t)$ that are ramified in the extension $\mathbb{K}(t, y) \mid \mathbb{K}(t)$. So, for $a_i = t(\sigma^i(P))$ and $b_i = t(\sigma^i(Q))$ we have that $\{a_0, \dots, a_{g(\mathcal{X})}, b_0, \dots, b_{g(\mathcal{X})}\}$ are the zeros of f and $\mathcal{X}$ has equation

$$y^2 = \prod_{i=0}^{g(\mathcal{X})} (t - a_i)(t - b_i). \quad (2.7)$$

Note that since

$$\operatorname{div}(\sigma^*(t)) = \operatorname{div}(t) \quad \text{and} \quad (\sigma^{g(\mathcal{X})+1})^*(t) = t$$

we have that $\sigma^*(t) = \zeta t$ where ζ is a primitive $(g(\mathcal{X})+1)$ -th root of unity. Also, $\operatorname{div}(\sigma^*(t - a_i)) = \sigma(\operatorname{div}(t - a_i)) = \operatorname{div}(t - a_{(i+1) \pmod{g(\mathcal{X})}})$ and $\operatorname{div}(\sigma^*(t - b_i)) = \sigma(\operatorname{div}(t - b_i)) = \operatorname{div}(t - b_{(i+1) \pmod{g(\mathcal{X})}})$. Then, $\sigma^*(t - a_i) = \xi(t - a_{(i+1) \pmod{g(\mathcal{X})}})$ and $\sigma^*(t - b_i) = \eta(t - b_{(i+1) \pmod{g(\mathcal{X})}})$ for some $\xi, \eta \in \mathbb{K}$. On the other hand,

$$\sigma^*(t - a_i) = \zeta t - a_i = \zeta \left(t - \frac{a_i}{\zeta} \right)$$

and

$$\sigma^*(t - b_i) = \zeta t - b_i = \zeta \left(t - \frac{b_i}{\zeta} \right).$$

Thus

$$\xi(t - a_{(i+1) \pmod{g(\mathcal{X})}}) = \zeta \left(t - \frac{a_i}{\zeta} \right)$$

and

$$\eta(t - b_{(i+1 \pmod{g(\mathcal{X})})}) = \zeta \left(t - \frac{b_i}{\zeta} \right),$$

whence $\xi = \eta = \zeta$, $a_{(i+1 \pmod{g(\mathcal{X})})} = \frac{a_i}{\zeta}$ and $b_{(i+1 \pmod{g(\mathcal{X})})} = \frac{b_i}{\zeta}$.

So, we obtain $a_i = \frac{a_0}{\zeta^i}$ and $b_i = \frac{b_0}{\zeta^i}$, and hence (2.7) reads

$$y^2 = \prod_{i=0}^{g(\mathcal{X})} \left(t - \frac{a_0}{\zeta^i} \right) \left(t - \frac{b_0}{\zeta^i} \right).$$

Finally, without loss of generality we can assume $a_0 = 1$ and $b_0 = \lambda$, so that (2.7) becomes

$$y^2 = (t^{g(\mathcal{X})+1} - 1)(t^{g(\mathcal{X})+1} - \lambda),$$

which proves the claim. $\square$

2.3 Abelian groups

For the case of abelian automorphism groups known results for Riemann surfaces are proved in [45] and [53]. The paper [45] deals with compact Riemann surfaces of genus $g \geq 2$ admitting an abelian automorphism group G which is large with respect to the genus; in particular, the author relates the order of G with the genus g and, if $|G|$ exceeds a certain threshold, then the structure of the surface X and the form of the quotient X/G are strongly determined.

By considering the Riemann-Hurwitz genus formula for the covering $X \rightarrow X/G$:

$$2g - 2 = |G| \left(2g_0 - 2 + \sum_{i=1}^r \left(1 - \frac{1}{n_i} \right) \right)$$

where g_0 is the genus of X/G and n_i are the orders of the stabilizers of the ramification points, it follows that, when G is large, in general, $g_0 = 0$ and $r \leq 3$.

The fact that G is abelian imposes additional conditions on the n_i , these conditions make the classification more restrictive than in the general case. The author C. Lomuto, under the size hypothesis, lists all the possibilities for the signature and determines which abelian groups can compare as automorphism groups. In many cases it can be proved that the quotient X/G is rational with three ramification points.

In [53] R. Pignatelli and C. Raso studied compact Riemann surfaces of genus $g \geq 2$ admitting an abelian automorphism group not properly "large" in the classical sense, but close to this condition in fact, the group is called quasi-large with respect to $g - 1$. The authors provided a detailed classification of Riemann surfaces admitting a quasi-large abelian group, together with a complete list of the possible signatures and determined the admissible ramified configurations depending on the order of the group; the explicit examples constructed in the paper proved the effective existence of these surfaces.

In this section we will try to extend the known results by Lomuto and Pignatelli-Raso to the case of positive characteristic, but in the case of groups whose order is not divisible by p . By considering Theorem 1.122 we will focus on the case $2g - 1 \leq |G| \leq 4g + 4$.

First of all note that, differently from the complex case, in positive characteristic can exist abelian automorphism groups of algebraic curves acting with a unique short orbit; in fact, in the complex case, this possibility is ruled out in the proof of [53, Proposition 4.1]. While for the case of positive characteristic it is sufficient to consider the Hermitian curve (nonsingular and plane) of equation $X^{p+1} = Y^p + Y$ defined over an algebraically closed field of characteristic p , the translations $X \mapsto X, Y \mapsto Y + i$ for each $i \in \mathbb{Z}_p$ form a cyclic group, and so an abelian group, which fixes a unique point (that is the unique point at infinity) and acts semiregularly on the others. Thanks to the fact that this doesn't happen in the complex case, Pignatelli and Raso were able to prove that if G is an abelian group of order $|G| \geq 2g - 1$, then the quotient is rational, we will see how this claim can be generalized to the case of positive characteristic.

Theorem 2.21. *[30, Section 2.14] Each non-trivial finite abelian group is a direct product of cyclic groups of prime-power order.*

Not every subgroup of a finite abelian group has a complement; an example is any subgroup of order d of a cyclic group of order a power of d , where d is a prime. The claim is true when the subgroup is a maximal cyclic subgroup.

Corollary 2.22. *Let G be a finite abelian group and let C be a cyclic subgroup. If C is not properly contained in any other cyclic subgroup of G , then there exists a subgroup H of G such that $G = C \times H$.*

Proof. Suppose that G is a d -group, where d is a prime. Then by Theorem 2.21

$$G \cong \mathbb{Z}_{d^{h_1}} \times \cdots \times \mathbb{Z}_{d^{h_k}}$$

with $h_1 \leq \dots \leq h_k$. Since C is cyclic, it must be contained in one of the factors, otherwise it would contain two different cyclic subgroups of order d . Then, by maximality, C coincides with one of the factors, hence, we can consider H as the product of the others. Suppose now that G is not a d -group for no prime d , then it is sufficient to consider that any finite abelian group is the direct product of its Sylow subgroups. We proceed by induction on the number of distinct primes which divide the order of G . Let $G = S_d \times K$, where S_d is a Sylow d -subgroup and K is the direct product of the others Sylow. Then $C = C_d \times C'$, with C_d and C' being maximal cyclic of S_d and K , respectively. By induction, the statement follows. $\square$

The next theorem extend to the general case the aforementioned known result of the complex case, the proof is characterized by the absence of topological arguments.

Theorem 2.23. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over an algebraically closed field of characteristic p . If G is an abelian automorphism group of size not divisible by p , then G cannot act with exactly one short orbit.*

Proof. Suppose by contradiction that G acts with a unique short orbit, say Ω . Let P be a point belonging to Ω , and let G_P be the stabilizer of G in P . Since G is tame and P is a ramification point, G_P is cyclic. For any other $Q \in \Omega$ the stabilizers G_P and G_Q are conjugate, but since G is abelian, it follows that $G_Q = G_P$ for all $Q \in \Omega$. Let L be a maximal cyclic subgroup of G containing G_P , then, by Corollary 2.22, there exists a subgroup M of G such that $G = L \times M$. Note that, since $G_P \subseteq L$ and Ω is the only one short orbit under the action of G , then M acts semiregularly on the points of $\mathcal{X}$, we denote by $\mathcal{X}'$ the quotient curve $\mathcal{X}/M$. By the Riemann-Hurwitz formula for M we have that

$$2g - 2 = |M|(2g(\mathcal{X}') - 2)$$

and $g \geq 2$ implies $g(\mathcal{X}') \geq 2$. Furthermore, $\mathcal{X}'$ admits a cyclic automorphism group isomorphic to L , we call it $\bar{L}$. Let $\bar{\Omega}$ the set of the points of $\mathcal{X}'$ which correspond to the orbits of $\mathcal{X}$ under the action of M which are contained in Ω , note that $|\bar{\Omega}| = |L|/|G_P|$. We have that $\bar{L}$ acts transitively on the points of $\bar{\Omega}$ and it acts semiregularly on the points of $\mathcal{X}' \setminus \bar{\Omega}$. Then $\mathcal{X}'$ results to be a curve of genus greater than or equal to 2, with a cyclic automorphism group acting with only one short orbit, against Proposition 1.118. $\square$

Theorem 2.24. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over an algebraically closed field of characteristic p . If G is an abelian automorphism group of order greater than $2g - 2$ and not divisible by p , then $\mathcal{X}/G$ is rational.*

Proof. Let $\Omega_1, \dots, \Omega_k$ be the short orbits under the action of G . If g' denotes the genus of $\mathcal{X}/G$ then, by the Riemann-Hurwitz formula we have

$$|G| > 2g - 2 = |G|(2g' - 2) + \sum_{i=1}^k (|G| - |\Omega_i|) \geq |G|(2g' - 2) + k \frac{|G|}{2}.$$

It follows that $2g' - 2 + \frac{k}{2} < 1$, it is possible just in three cases: $g' = 1$ and $k = 0$, $g' = 1$ and $k = 1$ or $g' = 0$. If $g' = 1$ and $k = 1$ we have a contradiction with the Theorem 2.23; if $g' = 1$ and $k = 0$ then $g = 1$ against $g \geq 2$; hence $g' = 0$. $\square$

We now present a result that can be deduced from [51] and for the sake of completeness, we include the proof.

Theorem 2.25. *Let G be a finite abelian automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|G|$. Suppose that the quotient curve $\mathcal{X}/G$ is rational and denote by $\Omega_1, \dots, \Omega_k$ the short orbits of $\mathcal{X}$ under the action of G . Let G_i be the stabilizer in G of an arbitrary point of Ω_i (note that the definition is well-defined since G is abelian). Finally let g_i be a generator of the cyclic group G_i (G_i is cyclic since p does not divide $|G|$). Then*

- (1) G is generated by $k - 1$ elements arbitrarily chosen in $\{g_i \mid i = 1, \dots, k\}$.
- (2) The size of G divides the product of the orders of $k - 1$ elements arbitrarily chosen in $\{g_i \mid i = 1, \dots, k\}$.
- (3) If G is cyclic, then $|G|$ is equal to the least common multiple of the orders of $k - 1$ elements arbitrarily chosen in $\{g_i \mid i = 1, \dots, k\}$.

Proof. (1) This is a direct consequence of Theorem 2.4.

(2) This follows from the hypothesis that G is abelian.

(3) This was already proved in Proposition 2.18. $\square$

Corollary 2.26. *Let G be a finite abelian automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|G|$. Suppose that the quotient curve $\mathcal{X}/G$ is rational and let $\Omega_1, \dots, \Omega_k$ denote the short orbits under the action of G . Let G_i be the stabilizer in G of*

an arbitrary point of Ω_i and let g_i be a generator of the cyclic group G_i . Then $|G_{i_0}|$ divides the least common multiple of the orders of the $k - 1$ elements $\{g_i \mid i = 1, \dots, k; i \neq i_0\}$.

Proof. From Theorem 2.25 follows that g_{i_0} belongs to the group generated by $\{g_i \mid i = 1, \dots, k; i \neq i_0\}$. Since G is abelian then

$$g_{i_0} = g_1^{\ell_1} \cdots g_{i_0-1}^{\ell_{i_0-1}} \cdots g_{i_0+1}^{\ell_{i_0+1}} \cdots g_k^{\ell_k}$$

for suitable exponents $\ell_1, \dots, \ell_k$. Now, if ℓ is the least common multiple of the orders of $\{g_i \mid i = 1, \dots, k; i \neq i_0\}$, we have $g_{i_0}^\ell = id$, hence the claim. $\square$

Corollary 2.27. *Let G be a finite abelian automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|G|$. Suppose that the quotient curve $\mathcal{X}/G$ is rational and let $\Omega_1, \dots, \Omega_k$ denote the short orbits under the action of G . Let G_i be the stabilizer in G of an arbitrary point of Ω_i and let n_i be the order of G_i . Then for every i_0 such that $1 \leq i_0 \leq k$ the group G is isomorphic to a quotient of the external direct product*

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{i_0-1}} \times \mathbb{Z}_{n_{i_0+1}} \times \cdots \times \mathbb{Z}_{n_k}.$$

Proof. Let g_i denote a generator of G_i and let ϕ be the function

$$\phi : \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{i_0-1}} \times \mathbb{Z}_{n_{i_0+1}} \times \cdots \times \mathbb{Z}_{n_k} \longrightarrow G$$

such that

$$(x_1, \dots, x_{i_0-1}, x_{i_0+1}, \dots, x_k) \longmapsto g_1^{x_1} \cdots g_{i_0-1}^{x_{i_0-1}} \cdot g_{i_0+1}^{x_{i_0+1}} \cdots g_k^{x_k}.$$

Since G is abelian ϕ is a group homomorphism. Furthermore, from Theorem 2.25 follows that ϕ is surjective. $\square$

Theorem 2.28. *Let G be a finite abelian automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|G|$. Suppose that the quotient curve $\mathcal{X}/G$ is elliptic and let $\Omega_1, \dots, \Omega_k$ denote the short orbits under the action of G . Let G_i be the stabilizer in G of an arbitrary point of Ω_i and let g_i be a generator of the cyclic group G_i . Then, if H is a group generated by $k - 1$ elements arbitrarily chosen in $\{g_i \mid i = 1, \dots, k\}$, one of the following claims hold:*

- (1) $G = H$;

(2) the factor group G/H is abelian but not cyclic;

(3) $\mathcal{X}/H$ is elliptic and the extension $\mathcal{X}/H$ over $\mathcal{X}/G$ is unramified.

Proof. Suppose that H is properly contained in G . From the proof of Theorem 2.25 we have that G/H acts on $\mathcal{X}/H$ with at most one short orbit. Since $\mathcal{X}/G$ is elliptic, the Riemann-Horwitz formula for G/H reads

$$2g(\mathcal{X}/H) - 2 = \frac{|G|}{|H|} - m$$

where m is a divisor of $\frac{|G|}{|H|}$. Hence $\mathcal{X}/H$ is elliptic and the covering $\mathcal{X}/H$ over $\mathcal{X}/G$ is unramified, or G/H it is not cyclic since the cyclic extensions cannot have exactly one short orbit. $\square$

In view of Theorem 2.2 and Theorem 2.25 it is possible to extend to the case of arbitrary characteristic the following result, which is proved for the complex case in [45, Theorem 3.1].

Theorem 2.29. *Let G be an abelian finite non-cyclic automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|G|$. Let $|G| > 4g - 4$. Let $\Omega_1, \dots, \Omega_r$ denote the short orbits under the action of G and let $n_1 \leq \dots \leq n_r$ be the sizes of the stabilizers of the points of such orbits. Then either $r = 4$, $(n_1, n_2, n_3, n_4) = (2, 2, 3, 3)$ and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, or $r = 3$ and one of the following possibilities for G and (n_1, n_2, n_3) holds:*

(a) an infinite family

$$(i) \ G \cong \mathbb{Z}_2 \times \mathbb{Z}_{2g+2} \ (2, 2g+2, 2g+2)$$

(b) exceptional cases

$$(ii) \ G \cong \mathbb{Z}_3 \times \mathbb{Z}_9 \ (3, 9, 9)$$

$$(iii) \ G \cong \mathbb{Z}_3 \times \mathbb{Z}_6 \ (3, 6, 6)$$

$$(iv) \ G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \ (5, 5, 5)$$

$$(v) \ G \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \ (4, 4, 4).$$

Proof. By Theorem 2.2 we have $r \in \{3, 4\}$. The only possibilities for $r = 4$ are $(2, 2, 2, n)$ with $n \geq 3$ and $(2, 2, 3, n)$ with $3 \leq n \leq 5$. Corollary 2.26 rules out this cases except for $(2, 2, 3, 3)$. We recall that Theorem 2.3 implies that any two stabilizers generate the whole group. For every $i = 1, 2, 3$ let G_i be the stabilizer of an arbitrary point of Ω_i .

From a deep study of the Riemann-Hurwitz genus formula for G it follows that the only possibilities for (n_1, n_2, n_3) , in addition to those listed, are the following and for each of these the group G must clearly be cyclic:

- $(2, 2g + 1, 4g + 2)$;
- $(2, 4g, 4g)$;
- $(3, 4, 12)$, with genus 3;
- $(3, 5, 15)$, with genus 4;
- $(3, 7, 21)$, with genus 6.

For the structure of the group in the cases listed in the statement, we now examine the different possibilities for G in the non-cyclic case:

- $(2g, 2g + 2, 2g + 2), (3, 9, 9), (3, 6, 6), (5, 5, 5)$: the group generated by G_1 and G_3 cannot coincide with G_3 ; furthermore, since G_1 has prime order, G_1 and G_3 have trivial intersection. Thus $G = G_1 \times G_3 = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_3}$
- $(4, 4, 4)$: the group generated by G_1 and G_3 cannot be G_3 . Furthermore such group cannot have order equal to 8 since, in that case, we will have

$$2g - 2 = -16 + 4 + 4 + 4 < 0$$

that is a contradiction. Thus the group has order 16 and it coincides with $\mathbb{Z}_4 \times \mathbb{Z}_4$.

□

In the case $i)$ there is still a cyclic group of size at least $2g + 2$ and this case is classified in [17]. In the exceptional cases with $r = 3$ we present some equations:

#	G	ramification indices	genus	equations
(ii)	$\mathbb{Z}_3 \times \mathbb{Z}_9$	3, 9, 9	7	$x^3 + y^9 + 1 = 0$
(iii)	$\mathbb{Z}_3 \times \mathbb{Z}_6$	3, 6, 6	4	$x^3 + y^6 + 1 = 0$
(iv)	$\mathbb{Z}_5 \times \mathbb{Z}_5$	5, 5, 5	6	$x^5 + y^5 + 1 = 0$
(v)	$\mathbb{Z}_4 \times \mathbb{Z}_4$	4, 4, 4	3	$x^4 + y^4 + 1 = 0$

Table 2.1: Equations for the considered cases

Note the relevance of diagonal curves like $x^n + y^m + 1 = 0$, we recall that, if m and n are coprime, then the genus is

$$\frac{mn + 1 - m - n}{2}$$

and so, in any case

$$mn = |G| > 2g - 2 = mn - m - n - 1.$$

In this case the group is cyclic. If instead m and n have a common factor, from [40] we know that

$$2g - 2 = mn - m - n - \text{GCD}(m, n)$$

thus the inequality $|G| > 2g - 2$ still holds. Furthermore note that if m divides n (or viceversa) the group is greater and it is described in [40] also if it is not abelian. In particular if m is odd the group is the direct product of a cyclic group of order m by a dihedral group of order $2n$. For instance the curve of equation $x^3 + y^6 + 1 = 0$ has genus equal to 4 and its automorphism group has order 36 that is $12(g - 1)$, Note that the group is solvable. Furthermore this curve gives an example of a curve which admits a dihedral group of size $4(g - 1)$.

Now we proceed to the study of the case of curves of genus $g \geq 2$ admitting an abelian tame automorphism group of order greater than $2g - 2$.

Theorem 2.30. *Let G be a finite abelian automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|G|$. Let $|G| > 2g - 2$. Let $\Omega_1, \dots, \Omega_r$ be the short orbits under the action of G and let $n_1 \leq \dots \leq n_r$ be the sizes of the stabilizers of the points of such orbits. Then $r \leq 5$ and one of the following possibilities for $(n_1, n_2, \dots, n_r)$ holds:*

- $(2, 2, 2, 2, 2);$
- $(2, 2, 2, 3, 3);$
- $(2, 2, t + 1, t + 1), t \text{ even};$
- $(2, 2, 2t + 1, 4t + 2);$
- $(2, 2, 2t, 2t);$
- $(2, 3, 3, 6);$
- $(2, 3, 4, 12);$
- $(2, 3, 5, 30);$
- $(2, 3, 6, 6);$
- $(2, 4, 4, 4);$
- $(3, 3, 3, 3);$
- $(3, 3, 4, 4);$
- $(3, 3, 5, 5,);$
- $(2, m, n), 3 \leq m \leq n; \text{ if } m = 3 \text{ then } n \geq 7; \text{ if } m = 4 \text{ then } n \geq 5;$
- $(3, m, n), 3 \leq m \leq n; \text{ if } m = 3 \text{ then } n \geq 4;$
- $(l, m, n), 4 \leq m \leq n.$

Proof. From Theorem 2.24 we know that the genus of the quotient curve $\mathcal{X}/G$ is zero. Furthermore, from Corollary 2.26 we know that every n_i divides the least common multiple of the others orders of the stabilizers. Form a deep study of the Riemann-Hurwitz genus formula follows that the only possibilities are those listed. The details are similar to those developed in [53]. $\square$

In the different cases of Theorem 2.30 we determine the possible structure of G and the corresponding genus of the curve. We examine separated the different cases. Note how not all the results obtained in [53] have been generalized to the case of arbitrary characteristic, and also when it was possible the proof necessarily differs from that in [53].

We preliminary recall that from (2) of Theorem 2.25 we know that the size of G divides the product of $r - 1$ values arbitrarily chosen between $n_1, \dots, n_r$ and so $|G|$ divides $\text{GCD}(n_1, \dots, n_r)$. We examine the different possibilities.

- $(2, 2, 2, 2, 2)$; the group is the product of $s \leq 4$ copies of $\mathbb{Z}_2$. The case $s = 1$ is ruled out since it implies $2g - 2 = -4 + 5$. If $s = 2$ $g = 2$, if $s = 3$ $g = 3$ and if $s = 4$ $g = 5$.
- $(2, 2, 2, 3, 3)$; from Theorem 2.25 the size of the group divides both 36 and 24, then $|G|$ divides 12. The group generated by G_3 and G_4 is a cyclic group of order 6. If $G = G_3 \times G_4$ we have

$$2g - 2 = -12 + 3(6 - 3) + 2(6 - 2) = 5,$$

that is a contradiction. Thus $|G| = 12$ and

$$2g - 2 = -24 + 3(12 - 6) + 2(12 - 4) = 10,$$

that implies $g = 6$. The group G cannot be cyclic since, otherwise, Lemma 1.124 is not satisfied.

- $(2, 2, t+1, t+1)$, t even; since $t+1$ is odd G is isomorphic to a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_{2(t+1)}$ and G contains a subgroup isomorphic to $\mathbb{Z}_{2(t+1)}$.

Hence the only possibilities are

– G is isomorphic to $\mathbb{Z}_{2(t+1)}$ and

$$2g - 2 = -4(t+1) + 2(2(t+1) - (t+1)) + 2(2(t+1) - 2) = 2(t+1) - 4$$

and so $g = t$; thus an example is the curve of equation

$$y^2 = (x^{t+1} - 1)(x^{t+1} - 1).$$

– G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2(t+1)}$ and

$$2g - 2 = -8(t+1) + 2(4(t+1) - 2(t+1)) + 2(4(t+1) - 4) = 4(t+1) - 8$$

and so $g = 2t - 1$.

- $(2, 2, 2t+1, 4t+2)$; the order of the group can only be $4t+2$ or $8t+4$. If $|G| = 4t+2$ we have

$$2g - 2 = (-8t - 4) + 2(4t + 2 - 2t - 1) + (4t + 2 - 2) + (4t + 2 - 1) = 4t - 1$$

that is a contradiction.

If $|G| = 8t+4$ we have

$$2g - 2 = -16t - 8 + 2(8t + 4 - 4t - 2) + (8t + 4 - 4) + (8t + 4 - 2) = 8t - 2$$

and so $g = 4t$, furthermore G is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2t+1}$ and so it must coincide with such products (that is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{4t+2}$).

- $(2, 2, 2t, 2t)$; the order of the group divides $8t$ and it is a multiple of $2t$. Furthermore it is a quotient of $\mathbb{Z}_{2t} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

If $|G| = 8t$ we have

$$2g - 2 = -16t + 2(8t - 4t) + 2(8t - 4) = 8t - 8$$

and so $g = 4t - 3$. Furthermore, the only possibility is that G coincides with $\mathbb{Z}_{2t} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

If $|G| = 4t$ we have

$$2g - 2 = -8t + 2(4t - 2t) + 2(4t - 2) = 4t - 4$$

and so $g = 2t - 1$. Then the structure of G must necessarily be $\mathbb{Z}_{2t} \times \mathbb{Z}_2$.

If $|G| = 2t$ we have

$$2g - 2 = -4t + 2(2t - t) + 2(2t - 1) = 2t - 2$$

and so $g = t$. Then G is necessarily cyclic.

- $(2, 3, 3, 6)$; the order of G can only be 6 or 18.

If $|G| = 6$ G is isomorphic to $\mathbb{Z}_6$ and the genus is 3.

If $|G| = 18$ we have

$$2g - 2 = -36 + (18 - 9) + 2(18 - 6) + (18 - 3) = 12$$

and so $g = 7$, furthermore G is isomorphic to a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, then it follows that $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

- $(2, 3, 4, 12)$; the order of G divides 24 and it is divisible by 12.

If $|G| = 12$ we have

$$2g - 2 = -24 + (12 - 6) + (12 - 4) + (12 - 3) + (12 - 1) = 10$$

then $g = 6$, furthermore the group is cyclic and then $G = \mathbb{Z}_{12}$.

If $|G| = 24$ we have

$$2g - 2 = -48 + (24 - 12) + (24 - 8) + (24 - 6) + (24 - 2) = 20$$

and so $g = 11$, furthermore G is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$, then it follows that $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$.

- $(2, 3, 5, 30)$; the order of G can only be 30, the genus is 15, furthermore G is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, then it follows that $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.
- $(2, 3, 6, 6)$; the order of G can only be 6, 12, 18 or 36.

If $|G| = 6$ we have

$$2g - 2 = -12 + (6 - 3) + (6 - 2) + 2(6 - 1) = 5$$

that is a contradiction.

If $|G| = 12$ we have

$$2g - 2 = -24 + (12 - 6) + (12 - 4) + 2(12 - 2) = 10$$

and so $g = 6$, furthermore G is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_6$, then it follows that $G = \mathbb{Z}_2 \times \mathbb{Z}_6$.

If $|G| = 18$ we have

$$2g - 2 = -36 + (18 - 9) + (18 - 6) + 2(18 - 3) = 15$$

that is a contradiction.

If $|G| = 36$ we have

$$2g - 2 = -72 + (36 - 18) + (36 - 12) + 2(36 - 6) = 30$$

and so $g = 16$, furthermore G is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_6$, then it follows that $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_6$.

- $(2, 4, 4, 4)$: the order of G can only be 4, 8, 16 or 32.

If $|G| = 4$ we have

$$2g - 2 = -8 + (4 - 2) + 3(4 - 1) = 3$$

that is a contradiction.

If $|G| = 8$ then the genus is 4 and G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. In this case there are exactly two cyclic subgroups of G of order 4 and their intersection has order 2. Since one of these two, say H , must coincide with at least two of the stabilizers of order 4, and since it has a non-trivial intersection with the third, by the Riemann-Hurwitz formula, with respect to the extension $\mathcal{X}$ over $(\mathcal{X}/H)$, we have

$$6 \geq 4(2g(\mathcal{X}/H) - 2) + 8$$

and so $g(\mathcal{X}/H) = 0$. But, on the other hand, it also holds that

$$6 \leq -8 + 9 + 2 + 2$$

that is a contradiction.

If $|G| = 16$ we have

$$2g - 2 = -32 + (16 - 8) + 3(16 - 4) = 12$$

and so $g = 7$, furthermore G is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4$, hence $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ or $G = \mathbb{Z}_4 \times \mathbb{Z}_4$. If $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ G has a unique cyclic subgroup C of order 4, which would therefore coincide with the three stabilizers. But, in this case, G would be generated by C together with an involution, and then $|G| = 8$ that is a contradiction.

If $|G| = 32$ we have

$$2g - 2 = -64 + (32 - 16) + 3(32 - 8) = 24$$

and so $g = 13$, furthermore G is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4$, then it follows that $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

- $(3, 3, 3, 3)$; the order of G can only be 3, 9 or 27, furthermore G is a quotient of $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

If $|G| = 3$ we have

$$2g - 2 = -6 + 4(3 - 1) = 2$$

and so $g = 2$, furthermore the only possibility for G is $|G| = \mathbb{Z}_3$.

If $|G| = 9$ we have

$$2g - 2 = -18 + 4(9 - 3) = 6$$

and so $g = 4$, furthermore the only possibility for G is $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.

If $|G| = 27$ we have

$$2g - 2 = -54 + 4(27 - 9) = 18$$

and so $g = 10$, furthermore the only possibility for G is $G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

- $(3, 3, 4, 4)$; the order of G can only be 12 and the genus is 6. Furthermore G is a quotient of $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4$, then it follows that $G = \mathbb{Z}_3 \times \mathbb{Z}_4$.

- $(3, 3, 5, 5)$; the order of G can only be 15, thus the group is isomorphic to $\mathbb{Z}_{15}$ and the genus is 8.
- $(2, m, n)$, $3 \leq m \leq n$; if $m = 3$ then $n \geq 7$; if $m = 4$ then $n \geq 5$. We recall that $|G|$ divides $2n, 2m$ and mn . Since 2 divides $\text{l.c.m.}(m, n)$ we have that at least one between m and n is even; furthermore m divides $\text{l.c.m.}(2, n)$ and n divides $\text{l.c.m.}(2, m)$.

Hence, if m is even, since n divides $\text{l.c.m.}(2, m) = m$ we have $n = m$; whereas if m is odd n is even and m divides $\text{l.c.m.}(2, n) = n$ and n divides $2m$.

Thus we are in one of the following situations

- $(2, 2\ell, 2\ell)$ with $\ell \geq 3$; then G is cyclic of order 2ℓ or G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2\ell}$.

In the first case

$$2g - 2 = -4\ell + \ell + 2\ell - 1 + 2\ell - 1$$

and $g = \ell/2$. Hence $\mathcal{X}$ admits a cyclic automorphism group of order $4g$. An example is given by

$$y^{4g} = x^{2g}(x + 1).$$

In the second case

$$2g - 2 = -8\ell + 2\ell + 4\ell - 2 + 4\ell - 2$$

and $g = \ell - 1$. Hence $\mathcal{X}$ admits a cyclic automorphism group of order $2g + 2$ and an abelian automorphism group of order $4g + 4$. An example is given by

$$y^{2g+2} = x^2 - 1.$$

- $(2, \ell, 2\ell)$ with ℓ odd; then G is cyclic of order 2ℓ . Furthermore

$$2g - 2 = -4\ell + \ell + 2\ell - 2 + 2\ell - 1$$

and $g = (\ell - 1)/2$. Hence $\mathcal{X}$ admits a cyclic automorphism group of order $4g + 2$. An example is given by

$$y^{4g+2} = x^{2g+1}(x + 1).$$

- $(3, m, n)$, $3 \leq m \leq n$; if $m = 3$ then $n \geq 4$.

If $\text{GCD}(3, m) = 1$, 3 divides n since 3 divides mn . Write $n = 3s$. Since m divides $3n = 9s$ and $\text{GCD}(3, m) = 1$ we have that m divides s . Write $s = tm$, so that $n = 3tm$. Clearly, since n divides $3m$, we have $t = 1$ and $n = 3m$. Then $|G| = 3m$ and G is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_m$. Furthermore,

$$2g - 2 = -6m + (3m - m) + (3m - 3) + (3m - 1)$$

hence $g = m + 1$. An example is the curve

$$y^{g-1} = x^3 + 1.$$

If $\text{GCD}(3, m) > 1$ we have $m = 3t$ with $3 \in \mathbb{N}$, we know that n divides $\text{l.c.m.}(3, 3t) = 3t$, on the other hand $n \geq m$, then it follows that $n = 3t$. Hence we are in the situation $(3, 3t, 3t)$. The only possibility for $|G|$ is $|G| = 3t$, whence G is cyclic. Furthermore

$$2g - 2 = -6t + (3t - t) + (3t - 1) + (3t - 1)$$

and so $g = t$.

A curve that verifies these conditions for $t \not\equiv 2 \pmod{3}$ is

$$y^{3g} = x^g(x + 1),$$

whereas for $t \equiv 2 \pmod{3}$ an example is

$$y^{3g} = x^{2g}(x + 1).$$

- (l, m, n) , $4 \leq l \leq m \leq n$. By the Riemann-Hurwitz formula immediately follows that

$$g = 1 + \frac{|G|}{2} \left(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n} \right).$$

If two of the three parameters are coprime, then the two corresponding stabilizer have trivial intersection and coprime orders and generate a cyclic group which coincides with G . Let G' be the stabilizers of a point of the orbit of length $|G|/n$ and let g' be the genus of the quotient curve $\mathcal{X}/G'$. Since G/G' acts on $\mathcal{X}/G'$ with at most two short orbits, by the Riemann-Hurwitz genus formula we have

$$2g' - 2 = -2|G|/|G'| + (|G|/|G'| - \ell_1) + (|G|/|G'| - \ell_2).$$

Then $g' = 0$ holds and either $G = G'$, so G is cyclic, or $\ell_1 = \ell_2 = 1$. In the latter case, the factor group G/G' acts on the projective line with two fixed point, and thus it is cyclic. Let C be the largest cyclic subgroup which contains G' . Then, by Corollary 2.22, G is the direct product of C by another subgroup E , so that G/G' is cyclic. If C has order $n\alpha$, since

$$G/G' = (C \times E)/G' \cong (C/G') \times E,$$

and so $C/G' \times E$ is cyclic, we can say that:

$$G \cong \mathbb{Z}_{n\alpha} \times \mathbb{Z}_\beta$$

with $\text{GCD}(\alpha, \beta) = 1$. Furthermore, $\alpha\beta$ divides $\text{GCD}(l, m)$, since G is isomorphic both to a quotient of $\mathbb{Z}_n \times \mathbb{Z}_m$ and to a quotient of $\mathbb{Z}_n \times \mathbb{Z}_l$. It also holds that the product $\gamma = \alpha\beta$ coincides with the quotient of m by the order of the stabilizer of two points, one taken from the second orbit and the other from the third, and also with the quotient of l by the order of the stabilizer of two points, one taken from the first orbit and the other from the third.

Then it follows that

$$2g - 2 = n\gamma - \gamma - \frac{n\gamma}{l} - \frac{n\gamma}{m},$$

where

$$l \mid n\gamma, \quad m \mid n\gamma, \quad \gamma \mid \text{GCD}(l, m).$$

Summarizing, we have the following possibilities:

- $\text{GCD}(l, m) = 1$, $G \cong \mathbb{Z}_{lm}$, $n \mid lm$. Since $l \mid mn$ it also holds $l \mid n$ and, similarly, since $m \mid ln$ it also holds $m \mid n$. Hence $n = lm$. Furthermore

$$g = 1 + \frac{1}{2}(n - m - l - 1).$$

A curve which verifies these conditions is

$$x^l + y^m + 1 = 0.$$

- $\text{GCD}(l, n) = 1$, $G \cong \mathbb{Z}_{ln}$, $m \mid ln$. Since $n \mid lm$ it also holds $n \mid m$, that is $n = m$, against Proposition 2.18, since we would have

$$ln = l.c.m..(l, n) = l.c.m..(m, n) = n.$$

- $\text{GCD}(m, n) = 1$, $G \cong \mathbb{Z}_{mn}$, $l \mid mn$. Since $n \mid lm$ it also holds $n \mid l$, that is $n = m = l$, against $\text{GCD}(m, n) = 1$.
- $|G| = n$, $G \cong \mathbb{Z}_n$, $l \mid n$, $m \mid n$. By Proposition 2.18 it follows that $n = lm$. Furthermore, still by Proposition 2.18, we have that $\text{GCD}(l, m) = 1$ and so we are in one of the previous cases.
- $|G| = n\alpha\beta$, $G \cong \mathbb{Z}_{n\alpha} \times \mathbb{Z}_\beta$; let $\gamma = \alpha\beta$,

$$2g - 2 = n\gamma - \gamma - \frac{n\gamma}{l} - \frac{n\gamma}{m},$$

where

$$l \mid n\gamma, \quad m \mid n\gamma, \quad \gamma \mid \text{GCD}(l, m).$$

Note 2.31. *As it can be seen, in the case of even characteristic the possibilities are very limited. Nakajima has already proved that if the genus is greater than 6 the bound is $3g + 6$ and he provided the example $y^3 = x^m - 1$ (classical generalized Fermat curve, signature $(3, m, m)$, group of order $3m$ where m is a multiple of 3, $g = m - 2$).*

2.4 Dihedral groups

Let $H \cong D_N$ be a dihedral automorphism group of $\mathcal{X}$, an algebraic curve of genus greater than or equal to 2 defined over an algebraically closed field of odd characteristic p . Suppose that $|H| = 2N$ and that $(p, N) = 1$. Let G be the cyclic subgroup of index 2 in H . In order to exclude the case where H is abelian, that was studied in the previous section, we suppose that $N > 2$.

Let us recall some general facts on dihedral groups and their subgroups.

First of all we recall that for $N \geq 3$ we have

$$D_N = \{1, r, r^2, \dots, r^{N-1}, s, rs, r^2s, \dots, r^{N-1}s\}$$

where $r^N = s^2 = (rs)^2 = 1$, while $D_1 = \langle r, s \rangle$, where $r = 1$ and s have order 2 and $D_2 = \langle r, s \rangle$, where both r and s has order 2 and they commute.

It follows a complete list of the subgroups of D_N .

Theorem 2.32 ([9]). *Every subgroup of D_N is either cyclic or dihedral. A complete list of the subgroups is the following:*

- (1) $\langle r^d \rangle$, where $d \mid N$, with index $2d$, $\langle r^i s \rangle$, where $0 \leq i \leq N - 1$, with index N ;

(2) $\langle r^d, r^i s \rangle$, where $d \mid N$ and $0 \leq i \leq d - 1$, with index d .

Every subgroup of D_N appears exactly one time in this list.

In this theorem the groups of the first type are cyclic weather those of the second type are dihedral:

$$\langle r^d \rangle \cong \mathbb{Z}_{N/d} \text{ and } \langle r^d, r^i s \rangle \cong D_{N/d}.$$

Now we classify the normal subgroups of D_N .

Theorem 2.33 ([9]). *In D_N , every subgroup of $\langle r \rangle$ is a normal subgroup of D_N (these are the subgroups $\langle r^d \rangle$, for $d \mid N$, and they have index $2d$). These are the only proper normal subgroups of D_N in the case where N is odd. In the case where N is even the only other proper normal subgroups are:*

$$\langle r^2, s \rangle \text{ and } \langle r^2, rs \rangle$$

both of index 2.

In particular, there is at most one normal subgroup in D_N for each index, except for three normal subgroups:

$$\langle r \rangle, \langle r^2, s \rangle \text{ and } \langle r^2, rs \rangle$$

which are all of index 2 when N is even.

Proposition 2.34. *If $N \geq g(\mathcal{X}) - 1$, then the extension $\mathcal{X}$ over $\mathcal{X}/G$ ramifies.*

Proof. Suppose by contradiction that the extension is unramified. Then, by the Riemann-Hurwitz genus formula for G we have:

$$2g(\mathcal{X}) - 2 = N(2g_0 - 2)$$

where g_0 denotes the genus of $\mathcal{X}/G$.

- if $g_0 > 1$, then $2g(\mathcal{X}) - 2 > 2N$, it follows that $N < g(\mathcal{X}) - 1$, that is a contradiction.
- If $g_0 = 1$, then $2g(\mathcal{X}) - 2 = 0$, that is $g(\mathcal{X}) = 1$, against the hypothesis $g(\mathcal{X}) \geq 2$.
- If $g_0 = 0$, then $2g(\mathcal{X}) - 2 = -2N$, that is $2g(\mathcal{X}) - 2 < 0$, against the hypothesis $g(\mathcal{X}) \geq 2$.

□

Proposition 2.35. *If $N \geq g(\mathcal{X}) - 1$ the extension $\mathcal{X}$ over $\mathcal{X}/H$ ramifies.*

Proof. This is a direct corollary of Proposition 2.34. □

The next remark will be useful for many proofs.

Lemma 2.36. *Let Γ be an orbit of $\mathcal{X}$ under the action of the subgroup G of H . Then, for a point P of Γ ,*

- (a) *the orbit of P under the action of H coincides with Γ , or*
- (b) *the orbit of P under the action of H is the (disjoint) union of Γ together with a different orbit under the action of G , say Γ' , of the same length of Γ .*

Furthermore, if Γ is a short orbit under the action of G , then (a) necessarily holds.

Proof. Let $P \in \Gamma$. We recall that H is generated by G and the involution s . If $s(P) \in \Gamma$ then (a) holds, since every element of H send P in a point of Γ . If, instead $s(P) \notin \Gamma$, then the orbit of P under the action of H coincides with the union of Γ with the orbit of $s(P)$ under the action of G .

Suppose now that Γ is a short orbit under the action of G . It follows that the size of the stabilizer G_P in G of a point P of Γ is greater than 1. If the stabilizer H_P of P in H properly contain G_P , then H_P would be a cyclic subgroup of H of size greater than or equal to 4 not contained in G , but such a group doesn't exist. □

Proposition 2.37. *If $N \geq g(\mathcal{X}) - 1$, the number of the short orbits of $\mathcal{X}$ under the action of G is at least 2.*

Proof. By Proposition 2.34 $n > 0$. Since the extension $\mathcal{X}$ over $\mathcal{X}/G$ is a Kummer extension, then $n \neq 1$. □

Proposition 2.38. *If $N > g(\mathcal{X}) - 1$ then $\mathcal{X}/H$ is either rational or elliptic. In the second case either N is odd and H acts with only one short orbit of length 2, or N is even and H acts with only one short orbit of length 4.*

Proof. By the Riemann-Hurwitz genus formula for H it follows that

$$2g(\mathcal{X}) - 2 \geq 2N(2g(\mathcal{X}/H) - 2) > 2(g(\mathcal{X}) - 1)(2g(\mathcal{X}/H) - 2)$$

which implies $2g(\mathcal{X}/H) - 2 < 1$ and so $g(\mathcal{X}/H) \in \{0, 1\}$.

Suppose $g(\mathcal{X}/H) = 1$. Then

$$2g(\mathcal{X}) - 2 = \sum_{i=1}^r (2N - \ell_i)$$

where $\ell_1, \dots, \ell_r$ are the sizes of the short orbits of $\mathcal{X}$ under the action of H . Since $2N - \ell_i \geq N > g(\mathcal{X}) - 1$, and by recalling that the extension $\mathcal{X}$ over $\mathcal{X}/H$ ramifies from Proposition 2.35, necessarily $r = 1$ and

$$2g(\mathcal{X}) - 2 = 2N - \ell$$

where ℓ is the length of the only short orbit under the action of H , say Ω . The stabilizer H_P of a point P of Ω is a cyclic subgroup of H . Since by Proposition 2.37 G has at least two short orbits, then (b) of Lemma 2.36 holds and so $|H/H_P| = 2|G/G_P|$, thus $H_P = G_P$.

Hence H_P is the only one cyclic subgroup of G of size $2N/\ell$. In particular H_P is normal in H and then the covering $\mathcal{X}/H_P$ over $\mathcal{X}/H$ is a Galois covering with respect to the group H/H_P and it is unramified. Thus also $\mathcal{X}/H_P$ is elliptic.

Let $\ell = 2$ and let N be even. In this case H has a normal subgroup M of index 2 not contained in H_P (see [9, Theorem 3.3]). Hence M acts transitively on Ω and the factor group H/M acts on $\mathcal{X}/M$ with only one short orbit, but this is a contradiction since H/M is cyclic of order 2.

Let $\ell > 2$. The factor group H/H_P is a dihedral group of size ℓ and it acts semiregularly as automorphism group of an elliptic curve. Hence H/H_P is a translation group of size ℓ , but this is a contradiction for $\ell \neq 4$ since the translation group of an elliptic curve is abelian, weather the dihedral group of order $\ell > 4$ is not. Note that in this case $N = g(\mathcal{X}) + 1$. $\square$

From the proof of the previous Proposition it easily follows the next result.

Proposition 2.39. *If $N > g(\mathcal{X}) + 1$ then $\mathcal{X}/H$ is rational.*

Proof. By Proposition 2.38 it follows that if $\mathcal{X}/H$ is not rational, then H acts with only one short orbit of length either 2 or 4 and so

$$2g(\mathcal{X}) - 2 = 2N - 2 \quad \text{or} \quad 2g(\mathcal{X}) - 2 = 2N - 4$$

that is a contradiction with $N > g(\mathcal{X}) + 1$. $\square$

We now deal with the case where $\mathcal{X}/H$ is rational.

Theorem 2.40. *Let $H \cong D_N$ be a dihedral automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|H|$. Suppose $N > g(\mathcal{X}) + 1$. Let $\Omega_1, \dots, \Omega_k$ denote the short orbits under the action of H of size smaller than N and let $\Delta_1, \dots, \Delta_t$ denote the short orbits under the action of H of size N . Let $k \geq 1$. Then*

- (a) *for all $i = 1, \dots, k$ and for all $P \in \Omega_i$, the stabilizer of P in H is the only one cyclic subgroup of H $\langle r^{|\Omega_i|} \rangle$ of size $m_i = 2N/|\Omega_i|$;*
- (b) *$t \geq 2$;*
- (c) *if N is odd then t is even;*
- (d) *if $t = 2$ then $N = \text{l.c.m.}(m_1, \dots, m_k)$;*
- (e) *if $t = 3$ then $N = \text{l.c.m.}(m_1, \dots, m_k, 2)$.*

Proof. (a) The stabilizer of P is a cyclic subgroup of H of size greater than 2. The claim follows from Theorem 2.32.

(b) In order to prove that $t \geq 2$ we denote by H_i the stabilizer of an arbitrary point of Ω_i and by L the group generated by $H_1, \dots, H_k$. Clearly L is contained in $G = \langle r \rangle$ and then it is a proper normal (cyclic) subgroup of H . Thus, the factor group H/L acts on the curve $\mathcal{X}/L$ such that

- the quotient curve of $\mathcal{X}/L$ with respect to H/L is rational (since it is isomorphic to $\mathcal{X}/H$);
- the short orbits of $\mathcal{X}/L$ under the action of H/L can only consists of points corresponding to orbits under the action of L contained in $\Delta_1, \dots, \Delta_t$; indeed, for each point P of $\mathcal{X}$ which doesn't belong to the union of the orbits $\Delta_1, \dots, \Delta_t$, the stabilizer of P in H coincides with the stabilizer of P in L ;
- if $|L_Q| = 1$ for a point Q of Δ_i , then the points of $\mathcal{X}/L$ which correspond to orbits under the action of L that are contained in Ω_i , form an orbit under the action of H/L of size $|H|/2|L|$;
- if $|L_Q| = 2$ for a point Q of Δ_i , then the points of $\mathcal{X}/L$ which correspond to orbits under the action of L that are contained in Ω_i , form a long orbit under the action of H/L . This case can occur only if $H_Q = G_Q = \langle r^{N/2} \rangle$; in particular N must be even.

Then, by the Riemann-Hurwitz genus formula, it follows that

$$2g(\mathcal{X}/L) - 2 \leq -2|H|/|L| + t(|H|/|L| - |H|/(2|L|)) = (t/2 - 2)|H|/|L|. \quad (2.8)$$

Since $|H|/|L| \geq 2$, then $t \geq 2$.

- (c) Let L be as in the previous point. Since N is odd, as noted above, we have that for all $i = 1, \dots, t$ the points of $\mathcal{X}/L$ which correspond to orbits under the action of L that are contained in Ω_i , form an orbit under the action of H/L of size $|H|/(2|L|)$; then the inequality in 2.8 is actually an equality and so

$$2g(\mathcal{X}/L) - 2 = (t/2 - 2)|H|/|L| = (t - 4)N/|L|.$$

Since N is odd then it follows that t is even.

- (d) If $t = 2$, 2.8 reads

$$2g(\mathcal{X}/L) - 2 \leq -2N/|L|.$$

The only possibility is that $g(\mathcal{X}/L) = 0$ and $L = G$. Furthermore no element of L fixes a point of some Δ_i . Thus it is possible to apply Proposition 2.18 to the covering defined by G , which has as ramification indices exactly the values m_i , each of them is repeated more than one time since for all Ω_i holds (b) of Lemma 2.36. Then the claim holds.

- (e) If $t = 3$ it follows that N is even and so

$$2g(\mathcal{X}/L) - 2 \leq -N/|L|,$$

it follows that $g(\mathcal{X}/L) = 0$. Furthermore either L is a subgroup of G of index 2 or $L = G$.

In the first case the equality holds and thus no element of L fixes a point of some Δ_i . Then it is possible to apply Lemma 2.36 to the covering defined by L and the claim follows from the fact that the order of L could be odd.

If instead $L = G$, then the element of order 2 in G is the stabilizer of the points of an orbit Δ_i . By Lemma 2.36 follows the claim.

□

The case $k = 0$ is studied in the next theorem.

Theorem 2.41. *Let $H \cong D_N$ be a dihedral automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$ defined over a field of characteristic $p > 0$ where p does not divide $|H|$. Suppose that $N > g(\mathcal{X}) + 1$. Suppose that the only short orbits under the action of H have size N . Then*

- $|H| = 4g(\mathcal{X}) - 4$
- $N \equiv 0 \pmod{4}$
- *Equations for $\mathcal{X}$ are*

$$\begin{cases} Y^2 = X^3 + AX^2 + CX + B \\ f(X, Y)Z^N = g(X, Y) \end{cases}$$

where $A, B, C \in \mathbb{K}$ are such that $Y^2 = X^3 + AX^2 + CX + B$ defines a non-singular curve $\mathcal{E}$ and $\alpha : \frac{g(X, Y)}{f(X, Y)}$ represents a rational function of $\mathcal{E}$, which is not an i -th power for any divisor of N and for which there exist two points P_1 and P_2 of $\mathcal{E}$ where the order of α is an odd multiple of $N/2$ whereas at all the other points of $\mathcal{E}$ the order is an even multiple of $N/2$.

Proof. According with Theorem 2.40 we denote by $\Delta_1, \dots, \Delta_t$ the short orbits under the action of H .

By the Riemann-Hurwitz genus formula it follows that

$$2 \leq 2g(\mathcal{X}) - 2 = -4N + t(2N - N) = (t - 4)N,$$

which implies $t \geq 5$. Actually, from $N > g(\mathcal{X}) + 1$ it follows that t must be exactly 5. Thus $N = 2g(\mathcal{X}) - 2$

Suppose that t' is the number of the short orbits under the action of H that are long orbits with respect to G . Obviously $t' \leq 5$, but from Proposition 2.34 $t' = 5$ cannot actually occur. Hence, by the Riemann-Hurwitz genus formula for G we have

$$N = 2g(\mathcal{X}) - 2 = N(2g(\mathcal{X}/G) - 2) + 2(5 - t')(N - N/2)$$

from which

$$1 = (2g(\mathcal{X}/G) + 3 - t')$$

and

$$g(\mathcal{X}/G) = \frac{t' - 2}{2}$$

for some $t' \in \{2, 4\}$.

If $t' = 2$, then $t - t' = 3$ and each point of these 3 short orbits is fixed by the unique involution of G . This involution, say σ , cannot fix other points. Then, by the Riemann-Hurwitz formula for $\langle \sigma \rangle$ we have

$$N = 2g(\mathcal{X}) - 2 = 2(2g(\mathcal{X}/\langle \sigma \rangle) - 2) + 3N$$

that is

$$(2g(\mathcal{X}/\langle \sigma \rangle) - 2) = -N$$

a contradiction.

Hence $t' = 4$. In this case the unique involution of G fixes exactly N points, then $g(\mathcal{X}/\langle \sigma \rangle) = 1$.

In order to prove that 4 divides N we consider the quotient curve $\mathcal{X}/\langle s \rangle$. Note that s has 4 fixed point on $\mathcal{X}$, this follows by an easy double counting on the set

$$\{(P, v) \mid P \in \mathcal{X}, v \text{ involution of } H \setminus G \text{ such that } v(P) = P\}.$$

The size is $4N$ since each point of the 4 short orbits of H that are long orbits for G has stabilizer of order 2 consisting of the identity and an involution of $H \setminus G$. Since any two arbitrary involutions of $H \setminus G$ are conjugated, the number of fixed points is constant and thus it is equal to 4. Hence we have

$$N = 2(g(\mathcal{X}) - 2) = 2(2g(\mathcal{X}/\langle s \rangle) - 2) + 4$$

from which $g(\mathcal{X}/\langle s \rangle) = N/4$.

Whence $\mathcal{X}$ is a Kummer extension of degree N of an elliptic curve $\mathcal{E} = \mathcal{X}/G$, defined by an equation of type $z^N = \alpha$, where $\alpha \in \mathbb{K}(\mathcal{E})$. Furthermore the group G is defined by $\beta \mapsto \beta$ for all $\beta \in \mathbb{K}(\mathcal{E})$ and $z \mapsto \mu z$ as μ varies among the N -th roots of unity. The involution σ is such that $z \mapsto -z$ and so the quotient curve $\mathcal{E}' = \mathcal{X}/\langle \sigma \rangle$, still elliptic, is a Kummer extension of $\mathcal{E}$ defined by $z^{N/2} = \alpha$.

Furthermore we know that the covering $\mathcal{X} \rightarrow \mathcal{E}$ ramifies exactly in two points and the ramification index is 2. Moreover the covering $\mathcal{E}' \rightarrow \mathcal{E}$ is unramified since both $\mathcal{E}'$ and $\mathcal{E}$ are curves of genus 1.

From Kummer theory we have the following informations on α :

- since the covering $\mathcal{E}' \rightarrow \mathcal{E}$, defined by $z^{N/2} = \alpha$, is unramified, we have that for each $P \in \mathcal{E}$ holds $\text{GCD}(\text{ord}_P(\alpha), N/2) = N/2$ and so $\text{ord}_P(\alpha)$ is always a multiple of $N/2$;

- since the covering $\mathcal{X} \rightarrow \mathcal{E}$, defined by $z^N = \alpha$, ramifies in two points with ramification index equal to 2, we have that there exist P_1 and P_2 in $\mathcal{E}$ such that

$$\text{GCD}(\text{ord}_P(\alpha), N) = N/2$$

and for all the other points $P \in \mathcal{E}$ we have $\text{GCD}(\text{ord}_P(\alpha), N) = N$.

Hence there exist two points P_1 and P_2 of $\mathcal{E}$ where the order of α is an odd multiple of $N/2$ whereas in all the other points the order is an even multiple of $N/2$. Furthermore, in order for the extension to be a Kummer extension, it is necessary that α is not a power with exponent a divisor of N . $\square$

Example 2.42. There exist fields where Theorem 2.41 holds. Suppose that $\mathcal{E}$ is defined by

$$y^2 = x^3 - x.$$

Let $P_1 = (1, 0)$, $P_2 = (-1, 0)$ and $\alpha = \left(\frac{x+1}{x-1}\right)$. Then $\text{div}(\alpha) = 2P_1 - 2P_2$, without α being a square. Hence we define

$$\mathcal{Y} : \begin{cases} y^2 = x^3 - x \\ (x-1)z^4 = (x+1) \end{cases}$$

that is a Kummer extension of $\mathcal{E}$ of degree 4 and genus 3. Then a dihedral group of order $8 = (4 \times 3) - 4$ acts on $\mathcal{Y}$ (this dihedral group is also contained in a larger group). The involution of the dihedral group is the rational map which maps a point P of $\mathcal{X}$ in $P \oplus (0, 0)$, swaps P_1 and P_2 , has four fixed points and maps z in $1/z$.

Explicitly

$$s(x, y, z) = (-1/x, -y/x^2, 1/z) \quad r(x, y, z) = (x, y, \lambda z)$$

where λ is a 4-th primitive root of unity. It is immediate to verify that $s^2 = r^4 = 1$ and that

$$(r \circ s \circ r)(x, y, z) = s(x, y, z),$$

that is $(rs)^2 = 1$. The group is larger since it also contains $(x, y, z) \mapsto (x, -y, z)$. Hence we have a 2-group of order $16 = 8g - 8$ which acts on a curve of genus 3.

We recall [2, Lemma 4.1] (see also Theorem 2.57 and its corollaries): *given an algebraic curve $\mathcal{X}_1$ defined over an algebraically closed field of characteristic different from 2 and of genus $g \geq 2$ admitting an automorphism group*

L of order n , there exists a sequence of algebraic curves $\mathcal{X}_n$ such that the covering $\mathcal{X}_n \rightarrow \mathcal{X}_1/L$ is a Galois covering, the covering $\mathcal{X}_{n+1} \rightarrow \mathcal{X}_n$ is an unramified, elementary abelian, Galois covering, of degree $2^{2g(\mathcal{X}_n)}$. Note that, since $\mathcal{X}_{n+1} \rightarrow \mathcal{X}_n$ is unramified, we have $g(\mathcal{X}_{n+1}) - 1 = 2^{2g(\mathcal{X}_n)}(g(\mathcal{X}_n) - 1)$ and, moreover, since both the coverings $\mathcal{X}_{n+1} \rightarrow \mathcal{X}_1/L$ and $\mathcal{X}_n \rightarrow \mathcal{X}_1/L$ are Galois coverings, $\mathcal{X}_{n+1}$ has an automorphism group of order $2^{2g(\mathcal{X}_n)}$ times the order of the Galois group of the covering $\mathcal{X}_n \rightarrow \mathcal{X}_1/L$.

Thus, if $L = h(g(\mathcal{X}_1) - 1)$, where h is an integer, then $\mathcal{X}_n$ admits an automorphism group L_n of order $h(g(\mathcal{X}_n) - 1)$, furthermore if L is a 2-group, then so is L_n .

Now we apply the previous remarks to the case $\mathcal{X}_1 = \mathcal{Y}$ and $L = H$. Then the curves $\mathcal{X}_n$ constitute an infinite family of curves with genus that goes to infinity admitting an automorphism group of order $4(g(\mathcal{X}_n) - 4)$ and acting with exactly 5 short orbits.

Let then $\mathcal{X}_1 = \mathcal{Y}$ and let L be the group of order $8g - 8$ constructed above. Then the curves $\mathcal{X}_n$ constitute an infinite family of curves attaining the bound of [2, Theorem 3.2], that is disjoint from the family given in [2, Example 4.3].

Note 2.43. *In the complex case there exist examples of curves for which Theorem 2.41 holds for each genus g , and are implicitly described in [56].*

Suppose $N > g(\mathcal{X}) + 1$. Let t denote the number of short orbits under the action of H of length N , let $t' \leq t$ denote the number of such orbits that are long orbits with respect to G and let k denote the number of short orbits under the action of H of length smaller than N .

Lemma 2.44. *Let $k \geq 1$. Then the possible pairs k, t are*

$$(1, 3), (1, 4), (2, 2), (2, 3).$$

Proof. We have $k+t$ short orbits under the action of H . For $k+(t-t')$ of these (b) of Lemma 2.36 holds, while for the remaining t' (a) of Lemma 2.36 holds. We recall that $t \geq 2$. Let $m_1, \dots, m_k$ denote the orders of the stabilizers of the points of the k short orbits of length smaller than N .

The Riemann-Hurwitz genus formula for the three coverings reads

- the covering $\mathcal{X} \rightarrow \mathcal{X}/H$ of degree $2N$

$$2g(\mathcal{X}) - 2 = -4N + \sum_{i=1}^k \left(2N - \frac{2N}{m_i} \right) + tN \quad (2.9)$$

- the covering $\mathcal{X} \longrightarrow \mathcal{X}/G$ of degree N

$$2g(\mathcal{X}) - 2 = N(2g(\mathcal{X}/G) - 2) + 2 \sum_{i=1}^k \left(N - \frac{N}{m_i} \right) + 2(t - t') \left(N - \frac{N}{2} \right) \quad (2.10)$$

- the covering $\mathcal{X}/G \longrightarrow \mathcal{X}/H$ of degree 2

$$2g(\mathcal{X}/G) - 2 = 2(-2) + t'. \quad (2.11)$$

On the other hand, from $t \geq 2$ and 2.11, it follows that for $N \geq g(\mathcal{X}) + 2$

$$2N - 6 \geq 2g(\mathcal{X}) - 2 = -4N + \sum_{i=1}^k \left(2N - \frac{2N}{m_i} \right) + tN \geq -4N + tN + k2N \frac{q-1}{q},$$

where q is the minimum divisor of N greater than 2. Then

$$t + \frac{4}{3}k \leq t + \frac{2q-2}{q}k < 6. \quad (2.12)$$

Furthermore, from $2g(\mathcal{X}) - 2 \geq 2$ we have

$$-4N + k(2N - 2) + tN \geq -4N + \sum_{i=1}^k \left(2N - \frac{2N}{m_i} \right) + tN \geq 2,$$

from which

$$2k + t - 4 > \left(2 - \frac{2}{N} \right) k + t - 4 \geq \frac{2}{N} > 0$$

that is

$$2k + t > 4. \quad (2.13)$$

□

Note that $k = 2$ and $t = 2$ imply $N = l.c.m.(m_1, m_2)$, weather $k = 2$ and $t = 3$ imply $N = l.c.m.(m_1, m_2, 2)$. Moreover $(2, 3)$ also implies $q = 3$, that is $6 \mid N$.

Immediately $k = 1$ and $t = 4$ imply $|H| \leq \frac{2q}{q-1}(g(\mathcal{X}) - 1) \leq 3(g - 1)$.

Furthermore note that from Theorem 2.4 we have $t' \neq 1$. Indeed, $t' = 1$ implies that the stabilizers of the points of $\mathcal{X}$ not contained in the only orbit corresponding to $t' = 1$ are subgroups of G , thus these stabilizers generate a proper subgroup of H , against Theorem 2.4.

Theorem 2.45. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over an algebraically closed field of characteristic $p \neq 2$. Let H be a dihedral automorphism group of size $2N > 2(g+1)$, with $(N, p) = 1$ if $p > 0$. Then either Theorem 2.41 holds or $\mathcal{X}$ is a Kummer extension of degree N of the projective line with Galois group G . In this second case one of the following possibilities holds:*

- $|H| = 4g+4$, $k = 1$, $t = 3$. *The stabilizer of a point in Ω_1 has odd order. The number of the short orbits under the action of G is 4. Furthermore g is even, $\mathcal{X}$ is hyperelliptic and an example is given by the curve of equation*

$$y^2 = (x^{g+1} - \mu^{g+1})(x^{g+1} - 1/\mu^{g+1})$$

with $\mu \in \mathbb{K}$, $\mu \neq 0$.

- $|H| = 4g$, $k = 1$, $t = 3$. *The stabilizer of a point in Ω_1 has even order. The number of short orbits under the action of G is 4. $\mathcal{X}$ is hyperelliptic and an example is given by the curve of equation*

$$y^2 = x(x^g - \mu^g)(x^g - 1/\mu^g)$$

with $\mu \in \mathbb{K}$, $\mu \neq 0$.

- $|H| = 2(g-1)/\left(1 - \frac{1}{e_1} - \frac{1}{e_2}\right)$ *where e_1, e_2 are divisors of $|H|/2$ such that $|H| = 2 \cdot \text{l.c.m.}(e_1, e_2)$. Furthermore $k = 2$, $t = 2$ and the number of short orbits under the action of G is 4.*

Proof. Let, as usual, G be the cyclic subgroup of H of order N . We denote by w (respectively n) the number of short orbits under the action of H (respectively G), and so $w = k + t$, and by m_i (respectively e_i) the ramification indices of the short orbits under the action of H (respectively G). If $k = 0$ then Theorem 2.41 holds. Otherwise, from Lemma 2.44 it follows $w \in \{4, 5\}$.

Note that for the short orbits under the action of G (b) of Lemma 2.36 necessarily holds, and so n is even.

We denote by $\tilde{g}$ the genus of the quotient curve $\mathcal{X}/G$, from Proposition 2.37 we know that $n \geq 2$, hence by the Riemann-Hurwitz genus formula for G we have

$$\frac{2g-2}{N} = 2\tilde{g} - 2 + \sum_{i=1}^n \left(1 - \frac{1}{e_i}\right),$$

since the left-hand side is smaller than 2 and $e_i \geq 2$ for all $i = 1, \dots, n$, it follows that $\tilde{g} \in \{0, 1\}$.

If $\tilde{g} = 1$, from

$$\frac{2g-2}{N} = \sum_{i=1}^n \left(1 - \frac{1}{e_i}\right)$$

it follows that $n = 2$; if instead $\tilde{g} = 0$, from

$$\frac{2g-2}{N} = -2 + \sum_{i=1}^n \left(1 - \frac{1}{e_i}\right)$$

it follows that $n \in \{2, 4, 6\}$.

We also note that $w \geq \frac{n}{2}$ holds.

We proceed by studying the cases separately.

- $w = 4$

- $n = 2$ (and so $k = 1$ and $t = 3$). By the Riemann-Hurwitz genus formula for H we have

$$\frac{2g-2}{2N} = -2 + \left(1 - \frac{1}{e_1}\right) + 3\left(1 - \frac{1}{2}\right),$$

weather by the Riemann-Hurwitz genus formula for G we have

$$\frac{2g-2}{N} = 2\tilde{g} - 2 + 2\left(1 - \frac{1}{e_1}\right)$$

by comparing the two we obtain

$$2\tilde{g} = 3$$

that is a contradiction.

- $n = 4$ (and so either $k = 1$, $t = 3$ and $t' = 2$ or $k = 2$, $t = 2$ and $t' = 2$). In this case $\tilde{g} = 0$. Suppose $t = 3$; by the Riemann-Hurwitz genus formula for G we obtain

$$\frac{2g-2}{N} = -2 + 2\frac{1}{2} + 2\left(1 - \frac{1}{e_3}\right).$$

Moreover, from (e) of Theorem 2.40 we have that $N = l.c.m.(2, e_3)$.

If e_3 is odd we obtain $N = 2g + 2$, $e_3 = g + 1$. From [17, Theorem 27] $\mathcal{X}$ is hyperelliptic. An example is given by

$$y^2 = (x^{g+1} - \mu^{g+1})(x^{g+1} - 1/\mu^{g+1});$$

in this case G is represented by the maps $(x, y) \mapsto (\epsilon x, \pm y)$ as ϵ varies among the $(g+1)$ -th roots of unity, weather an involution in $H \setminus G$ is given by $(x, y) \mapsto (1/x, w/x^{g+1})$. If instead e_3 is even we obtain $N = e_3 = 2g$. Then, in the case where e_3 is even, we have that there are two orbits of length $\frac{N}{2}$ and two fixed pints with respect to G and three orbits of length N and an orbit of length 2 with respect to H . By considering the Riemann-Hurwitz genus formula with respect to the subgroup M of G generated by the unique involution, we have

$$2g - 2 = 2(2g(\mathcal{X}/M) - 2) + 2g + 2$$

from which $\mathcal{X}/M$ is rational and thus $\mathcal{X}$ is hyperelliptic. An example is given by curves of equation

$$y^2 = x(x^g - \mu^g)(x^g - 1/\mu^g)$$

where G is represented by the maps $(x, y) \mapsto (\epsilon^2 x, \epsilon x)$ as ϵ varies among the $2g$ -th root of unity, weather an involution in $H \setminus G$ is given by $(x, y) \mapsto (1/x, y/x^{g+1})$.

Suppose $t = 2$. In this case the sequence of the orders of the stabilizers of the short orbits under the action of H is $(e_1, e_2, 2, 2)$, weather for G we have (e_1, e_1, e_2, e_2) . Moreover, from (d) of Theorem 2.40 we know that $N = l.c.m.(e_1, e_2)$. By the Riemann-Hurwitz genus formula for H (or equivalently for G) we have

$$2g - 2 = -4N + 2N - \frac{2N}{e_1} + 2N - \frac{2N}{e_2} + N + N$$

from which

$$g - 1 = N \left(1 - \frac{1}{e_1} - \frac{1}{e_2} \right)$$

and so

$$N = (g - 1) \frac{e_1 e_2}{e_1 e_2 - e_1 - e_2}. \quad (2.14)$$

Form $N = l.c.m.(e_1, e_2)$, 2.14 reads

$$N = (g - 1) \frac{\text{GCD}(e_1, e_2)}{\text{GCD}(e_1, e_2) - \frac{e_1}{N} - \frac{e_2}{N}}.$$

- $n = 6$. Also in this case $\tilde{g} = 0$. By the Riemann-Hurwitz genus formula for H we have, for $e_1 > 2$, $e_3 > 2$ and $e_5 \geq 2$,

$$\frac{2g-2}{2N} = -2 + \left(1 - \frac{1}{e_1}\right) + \left(1 - \frac{1}{e_3}\right) + \left(1 - \frac{1}{e_5}\right) + \left(1 - \frac{1}{2}\right),$$

weather by the Riemann-Hurwitz genus formula for G we have

$$\frac{2g-2}{N} = -2 + 2\left(1 - \frac{1}{e_1}\right) + 2\left(1 - \frac{1}{e_3}\right) + 2\left(1 - \frac{1}{e_5}\right).$$

By comparing the two we obtain

$$-2 = -3$$

that is a contradiction.

- $w = 5$

- $n = 2$. By the Riemann-Hurwitz genus formula for H we have, for $e_1 > 2$ and $e_3 \geq 2$

$$\frac{2g-2}{2N} = -2 + \left(1 - \frac{1}{e_1}\right) + 4\left(1 - \frac{1}{2}\right),$$

weather by the Riemann-Hurwitz genus formula for G we have

$$\frac{2g-2}{N} = 2\tilde{g} - 2 + 2\left(1 - \frac{1}{e_1}\right)$$

by comparing the two we obtain $\tilde{g} = 2$ that is a contradiction.

- $n = 4$. In this case $\tilde{g} = 0$. Moreover, by the Riemann-Hurwitz genus formula for H we have

$$\frac{2g-2}{2N} = -2 + \left(1 - \frac{1}{e_1}\right) + \left(1 - \frac{1}{e_3}\right) + \left(1 - \frac{1}{2}\right),$$

weather by the Riemann-Hurwitz genus formula for G we have

$$\frac{2g-2}{N} = -2 + 2\left(1 - \frac{1}{e_1}\right) + 2\left(1 - \frac{1}{e_3}\right)$$

by comparing the two we obtain

$$-2 = -1$$

that is a contradiction.

- $n = 6$. Also in this case $\tilde{g} = 0$. As noted above the only possibilities in this case are $k = 1$ and $t = 4$ or $k = 2$ and $t = 3$.

Suppose $t = 4$, this implies $e_1 = e_3 = 2$ and $e_5 > 2$, by replacing in the Riemann-hurwitz genus formula for G we obtain

$$\frac{2g - 2}{N} = 2 - \frac{2}{e_5}.$$

From 3 of Theorem 2.25 if e_5 is even then $N = e_5$, if instead e_5 is odd $N = 2e_5$. If $N = e_5$, by replacing in the Riemann-Hurwitz genus formula for G we obtain

$$\frac{2g - 2}{N} = 2 - \frac{2}{N}$$

from which $N = g$, against the hypothesis $N > g + 1$. If $N = 2e_5$, by replacing in the Riemann-Hurwitz genus formula for G we obtain

$$\frac{2g - 2}{N} = 2 - \frac{4}{N}$$

from which $N = g + 1$ against the hypothesis $N > g + 1$.

Suppose now $t = 3$, this implies $e_1 = 2$ and $e_3, e_5 > 2$, by replacing in the Riemann-Hurwitz formula with respect to H we obtain

$$\frac{2g - 2}{2N} = \frac{3}{2} - \frac{1}{e_3} - \frac{1}{e_5},$$

if $e_3 \geq 4$ the right-hand side would be greater than or equal to 1 weather the left-hand side would be smaller than 1; then $e_3 = 3$, hence the Riemann-Hurwitz genus formula for H reads

$$\frac{2g - 2}{2N} = \frac{7}{6} - \frac{1}{e_5}$$

from which $e_5 < 6$. Whence $e_5 \in \{3, 4, 5\}$ and in each case, from (e) of Theorem 2.40, we have $N = l.c.m.(e_3, e_5, 2)$; so, if $e_5 = 3$ then $N = 6$ and $g = N$, if $e_5 = 4$ then $N = 12$ and $g = N$, finally if $e_5 = 5$ then $N = 30$ and $g = N$. In every case there is a contradiction with the hypothesis $N > g + 1$.

□

Theorem 2.46. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over an algebraically closed field of characteristic $p \neq 2$. Let H be a dihedral automorphism group of $\mathcal{X}$ of size $2N > 2(g+1)$, with $(N, p) = 1$ if $p > 0$. Then either $|H| \in \{4g+4, 4g, 4g-4\}$ or $|H| < 2(g-1)/(1 - \frac{1}{q} - \frac{q}{N})$ where q is the minimum divisor of N greater than 2.*

Proof. If $|H| \notin \{4g+4, 4g, 4g-4\}$, then, from Theorem 2.41, (3) of Theorem 2.45 holds. $\square$

In the case where N is a prime we have the following corollary.

Corollary 2.47. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over an algebraically closed field of characteristic $p \neq 2$. Let H be a dihedral automorphism group of $\mathcal{X}$ of size $2N$, with N a prime different from p if $p > 0$. Then $|H| \leq 2g+2$.*

Proof. Since $N > g+1$, from [34] it necessarily follows that $N = 2g+1$ and thus $|H| = 4g+2$, against Theorem 2.46. $\square$

2.5 Nilpotent groups

Zomorrodian [69] showed that

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

when $\mathbb{K} = \mathbb{C}$ and G is a nilpotent automorphism subgroup of a curve $\mathcal{X}$. The author also proved that, if the equality holds, then $g-1$ is a power of 2. Conversely, if $g-1$ is a power of 2, then there exists a function field of genus g admitting an automorphism group of order $16(g-1)$; hence a nilpotent group of order a power of 2. Note that his approach is also based on the method of Fuchsian groups.

In [2] the case of arbitrary characteristic was studied. More precisely it was obtained a similar bound on the order of an arbitrary nilpotent subgroup of the automorphism group of a curve in positive characteristic, except for one case. More precisely, the main result of [2] is the following.

Theorem 2.48. *Let K be an algebraically closed field of characteristic $p > 0$ and let F/K be a function field of genus $g \geq 2$. Suppose that $G \leq \text{Aut}(F/K)$ is a nilpotent subgroup of order*

$$|G| > 16(g-1).$$

Then the following properties hold:

- (i) G is a p -group.
- (ii) The fixed field F_0 of G is rational.
- (iii) There exists only one place P_0 of F_0 , which ramifies in F/F_0 . Furthermore, P_0 is totally ramified and

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

Here we highlight further examples than those in [2] of curves $\mathcal{X}$ admitting a nilpotent automorphism group of size $16(g(\mathcal{X}) - 1)$ and such that the size is coprime with p .

Example 2.49. For $p \neq 2$, the Fermat curve $x^4 + y^4 + z^4 = 0$ of genus 3 has a nilpotent 2-group with $16(g - 1) = 32$ elements. By proceeding as in [2, Example 4.2] we obtain an infinite family, disjoint from that in [2].

Finally we note that in the Example 2.42, we show that the bound of [2, Theorem 3.2] is attained for a genus tower which start from 3.

2.6 Non-perfect groups

In this chapter we prove some results on algebraic curves which have an automorphism group that is non perfect; this includes the case of solvable groups, thus extending to positive characteristic the known limitation for Riemann surfaces [8].

First of all we recall the definitions of non-perfect groups and solvable groups and some preliminary results.

Definition 2.50. Let G be a group and let $a, b \in G$, the element $a^{-1}b^{-1}ab$ is called *commutator* of a and b and it is denoted by $[a, b]$. The subgroup of G generated by the commutators of each pair of elements of G is called *derived* subgroup of G and it is denoted by G' , that is

$$G' = \langle [a, b] \mid a, b \in G \rangle.$$

Definition 2.51. A group G is called *perfect* (respectively *non-perfect*) if $G' = G$ (respectively if $G' \subsetneq G$).

Theorem 2.52. Let G be a group and let G' be the derived subgroup.

- (i) G' is a characteristic subgroup;
- (ii) The factor group G/G' is abelian;
- (iii) If N is a subgroup of G such that $N \trianglelefteq G$ and G/N is abelian, then $G' \subseteq N$;
- (iv) If $H \leq G$ and $G' \subseteq H$ then H is normal in G .

Theorem 2.53. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over a field of characteristic p . Let G be a non-perfect automorphism group of $\mathcal{X}$, whose order is coprime with p , then*

$$|G| \leq 48(g - 1).$$

Proof. Suppose by contradiction that $|G| > 48(g - 1)$, by the Riemann-Hurwitz genus formula follows that $|G| = 84(g - 1)$ and that G acts on $\mathcal{X}$ with exactly three short orbits, say Ω_1, Ω_2 and Ω_3 of size, respectively, $|G|/2, |G|/3$ and $|G|/7$.

Note that for each point P in the union of such orbits, since the stabilizer G_P of P in G has prime order, either $(G')_P = G_P$ or $(G')_P$ is trivial. For two given points P and P' belonging to the same short orbit Ω_i , we have that the stabilizers of P and P' in G are conjugate and thus, since G' is normal, it follows that $(G')_P = G_P$ if and only if $(G')_{P'} = G_{P'}$.

Finally, we recall that

$$2g - 2 = |G'|(2g(\mathcal{X}/G') - 2) + \epsilon$$

where

$$\epsilon = \sum_{P \in \mathcal{X}} (|G'_P| - 1).$$

We examine eight possibilities separately, with respect to which ϵ is computed, from which a contradiction easily follows.

- $G'_P = \{id\}$ for each P . In this case $\epsilon = 0$. Furthermore G/G' is an abelian group acting on a curve of genus g' such that

$$g' - 1 = (g - 1)/|G'| = |G|/(84)|G'| = |G/G'|/84,$$

but this is a contradiction since $g' > 1$ and G/G' abelian imply $|G/G'| \leq 4g' + 4$.

- $G'_P = G_P \neq \{id\}$ if and only if $P \in \Omega_1$. In this case

$$\epsilon = \frac{|G|}{2}(2-1) = 42(g-1)$$

and so $g' = 0$ and $|G'| = \frac{20}{84}|G|$, against the fact that $|G|/|G'|$ is an integer.

- $G'_P = G_P \neq \{id\}$ if and only if $P \in \Omega_2$. In this case

$$\epsilon = \frac{|G|}{3}(3-1) = 56(g-1)$$

and so $g' = 0$ and $|G'| = \frac{27}{84}|G|$, that is a contradiction.

- $G'_P = G_P \neq \{id\}$ if and only if $P \in \Omega_3$. In this case

$$\epsilon = \frac{|G|}{7}(7-1) = 72(g-1)$$

and so $g' = 0$ and $|G'| = \frac{35}{84}|G|$, that is a contradiction.

- $G'_P = G_P \neq \{id\}$ if and only if $P \in \Omega_1 \cup \Omega_2$. In this case

$$\epsilon = \frac{|G|}{2}(2-1) - \frac{|G|}{3}(3-1) = 98(g-1)$$

and so $g' = 0$ and $|G'| = \frac{48}{84}|G|$, that is a contradiction.

- $G'_P = G_P \neq \{id\}$ if and only if $P \in \Omega_1 \cup \Omega_3$. In this case

$$\epsilon = \frac{|G|}{2}(2-1) - \frac{|G|}{7}(7-1) = 114(g-1)$$

and so $g' = 0$ and $|G'| = \frac{56}{84}|G|$, that is a contradiction.

- $G'_P = G_P \neq \{id\}$ if and only if $P \in \Omega_2 \cup \Omega_3$. In this case

$$\epsilon = \frac{|G|}{3}(3-1) - \frac{|G|}{7}(7-1) = 128(g-1)$$

and so $g' = 0$ and $|G'| = \frac{63}{84}|G|$, that is a contradiction.

- $G'_P = G_P \neq \{id\}$ if and only if $P \in \Omega_1 \cup \Omega_2 \cup \Omega_3$. In this case

$$\epsilon = \frac{|G|}{2}(2-1) - \frac{|G|}{3}(3-1) - \frac{|G|}{7}(7-1) = 170(g-1)$$

and so $g' = 0$ and $|G'| = |G|$, that is a contradiction since G' is a proper subgroup.

□

Note that there exist curves which attain the bound of Theorem 2.53.

Note 2.54. Let $p > 3$ and let $\mathcal{F}_4$ be the plane curve of equation $x^4 + y^4 + 1 = 0$. Then $\mathcal{F}_4$ has genus equal to 3 and admits a solvable automorphism group of size 96.

Proof. The curve is non-singular, thus the genus is $\frac{(4-1)(4-2)}{2} = 3$. It is well known that the Fermat curves $\mathcal{F}_n$ of equation $x^n + y^n + 1 = 0$ admit an automorphism group G of size $6n^2$. Furthermore G has as normal subgroup N a group isomorphic to $\mathbb{Z}_n \times \mathbb{Z}_n$ and the factor group G/N is isomorphic to S_3 . Since both N and G/N are solvable, it follows that also G is solvable. Furthermore in the case $n = 4$ we have $6n^2 = 96 = 48(3-1)$. □

Note 2.55. The curve $\mathcal{Z}$ of equation $y^2 = x(x^4 - 1)$ presented in [2] has genus $g = 2$ and it has a solvable automorphism group of order $48 = 48(g-1)$ isomorphic to $GL(2,3)$. In the complex case this curve is known as Bolza surface and it has the maximum number of automorphisms that a curve of genus 2 can have in the complex case. The subgroup of order 16 is explicitly constructed in [2] as the group generated by σ and τ where

$$\sigma(x) = \xi^2 x, \quad \sigma(y) = \xi y$$

and

$$\tau(x) = 1/x, \quad \tau(y) = y/x^3$$

where ξ is a primitive 8-th root of unity. A further automorphism θ is instead given by

$$\theta(x) = -(x + \xi^2)/(x - \xi^2), \quad \theta(y) = \alpha y/(x - \xi^2)^3$$

where α is such that $\alpha^2 = -8\xi^2$. The group generated by σ, τ and θ turns out to be isomorphic to $GL(2,3)$. The quotient with respect to the hyperelliptic involution $x \mapsto x, y \mapsto -y$ is the symmetric group over 4 elements which acts on the 6 Weierstrass points of the curve.

Note that a Riemann surface of genus 2 with an automorphism group isomorphic to $GL(2,3)$ is presented in [27] without providing explicit equations.

Note 2.56. *If we consider for $p > 5$ the Fermat curve $\mathcal{F}_5 : x^5 + y^5 + 1 = 0$ we can notice that this admits a solvable group with 150 elements weather the genus is 6. In this case we have a solvable group with $15(g - 1)$ elements. Note that from the proof of the Hurwitz bound it follows that $15(g - 1)$ is the maximum order of an automorphism group with odd order coprime with the characteristic p , for curves of genus greater than 1.*

We will see that, by using to the following theorems, some abelian unramified coverings of $\mathcal{F}_4, \mathcal{F}_5$ and $\mathcal{Z}$ give rise to further maximal example.

Theorem 2.57. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over a field of characteristic $p > 0$. Let G be a non-perfect automorphism group of $\mathcal{X}$. Then for each prime $d \neq p$ there exists a curve of genus $g' = d^{2g}(g - 1) + 1$ admitting a non-perfect automorphism group of size $d^{2g}|G|$.*

Proof. Let $M = \mathbb{K}(\mathcal{X})$ be the function field of $\mathcal{X}$ and let F be the subfield of M that is fixed by G . Then the extension $M : F$ is a Galois extension of degree $|G|$.

In a fixed algebraic closure of M there exists only one elementary abelian extension L of $\mathbb{K}(\mathcal{X})$ of degree d^{2g} such that the genus g' of L satisfies

$$g' - 1 = d^{2g}(g - 1)$$

(see for instance [54, Section 4.7]). Let $\mathcal{Y}$ be the algebraic curve whose function field is L and note that the condition on the genus coincides with the fact that the extension $\mathbb{K}(\mathcal{Y}) : \mathbb{K}(\mathcal{X})$ is unramified.

Hence we consider the Galois closure L' of the extension $L : F$ in a fixed algebraic closure of M . Note that, in theory, L' could properly contain L . We will show that actually $L' = L$.

Let $\Gamma = \Gamma(L', F)$, the number of elements of Γ is obviously equal to degree of the extension $L' : F$, that is the product of the degree of $L' : L$ by the degree of $L : F$. Hence $[L' : L] = |\Gamma|/(d^{2g}|G|)$.

Since $M : F$ is a Galois extension, then, from a well known fact from Galois Theory (see for instance [11, Theorem 7.2.5]), each element γ of Γ must map to itself M and so, from the uniqueness of the unramified abelian extension of degree d^{2g} , it must map to itself also L . But this means that $G' = \Gamma(L, F)$ has at least $[L : F]$ elements, that is the extension $L : F$ is a Galois extension. Hence $L' = L$ and $G' = \Gamma$.

Now we recall that, since $M : F$ is a Galois extension, the Galois group $\Gamma(L, M)$ is normal in $\Gamma(L, F)$ and $\Gamma(M, F)$ is isomorphic to $\Gamma(L, F)/\Gamma(L, M)$.

But $\Gamma(L, M)$ is abelian and $\Gamma(M : F) = G$ is non-perfect. Thus $G' = \Gamma(L, F)$ is non-perfect. Since G' is isomorphic to an automorphism group of $\mathcal{Y}$, the claim is proved. $\square$

Note 2.58. *From the previous proof, dismissing the hypothesis that G is non-perfect, the following result holds: if there exists a curve $\mathcal{X}$ of genus $g \geq 2$ with an automorphism group of order $h(g-1)$, then for each prime d different from p there exists a curve of genus $g' = d^{2g}(g-1) + 1$, that is an abelian covering with exponent d of $\mathcal{X}$, with an automorphism group of order $h(g'-1)$. In the complex case this result was obtained By Macbeath in 1961 in [46, Theorem 6] for an arbitrary positive integer d , with different techniques using topological properties of Riemann surfaces.*

Corollary 2.59. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over a field of characteristic $p > 0$. Let G be a non-perfect automorphism group of $\mathcal{X}$ and let $\delta = \frac{|G|}{g-1}$. Then for every positive integer n there exists a curve $\mathcal{Y}$ of genus g' greater than n admitting an automorphism group G' such that $|G'|/(g'-1) = \delta$.*

Corollary 2.60. *For each characteristic $p \geq 3$, there exists an infinite number of curves, with genus that goes to infinity, admitting a non-perfect tame automorphism group of order exactly $48(g-1)$.*

Proof. It sufficient to apply Corollary 2.59 to the Fermat curve $\mathcal{F}_4$ or to the curve $\mathcal{Z}$. $\square$

Corollary 2.61. *For each characteristic $p > 5$, there exists an infinite number of curves, with genus that goes to infinity, admitting a non-perfect tame automorphism group of odd order exactly equal to $15(g-1)$.*

Proof. It sufficient to apply Corollary 2.59 to the Fermat curve $\mathcal{F}_5$. $\square$

2.7 Groups with a cyclic subgroup of index 2

In this section, we investigate curves having an automorphism group H admitting a cyclic subgroup G of index 2, over fields of any characteristic, the results presented in this section are the subject of the paper [16]. Admitting a cyclic subgroup of index 2 might seem a strong condition, but actually there are many possible structures for such groups. Apart from the cyclic, abelian, dihedral, generalized quasi-dihedral cases, there are and several others and a complete list can be found for instance in [12, Proposition 10.2].

Clearly, if an automorphism group H admits a cyclic subgroup of index 2, then $|H| \leq 8g + 4$. If H is abelian, then it is well-known that its size cannot exceed $4g + 4$ (see Theorem 1.122). Over the complex field, it is a classical result that if H is dihedral, then $|H| \leq 4g + 4$. Recently, it has been showed ([31, Theorem 6.1]) that if H is a generalized quasi-dihedral group, then a tighter bound holds; on the other hand, Reyes-Carocca and Speziali [55] studied Riemann-Surfaces of genus g having an automorphism group of size $6g$ admitting a cyclic subgroup of index 2.

The present section is partly motivated by these recent results, trying to ask the following questions:

- does the upper bound $4g(\mathcal{X}) + 4$ holds for dihedral automorphisms groups of curves of genus $g(\mathcal{X}) \geq 2$ defined over any algebraically closed field?
- for a given $g \geq 2$, what are the possible sizes of an automorphism group H of a curve of genus g admitting a cyclic subgroup of index 2?

Since for any $g \geq 2$ there is a curve of genus g admitting a dihedral group of automorphism of order $4g + 4$, with respect to the latter question we focus on the case where $|H|$ is strictly greater than $4g + 4$.

In order to extend the upper bound $4g(\mathcal{X}) + 4$ for dihedral groups from the complex case to that of any algebraically closed field, we first note that by Abhyankar Lemma allow us to deduce that the bound also holds provided that the characteristic does not divide the size of the group.

In subsection 2.7.1 we show that over a field of characteristic $p \neq 2$ there cannot exists a dihedral group of size multiple of p and greater than $4g + 4$.

Theorem 2.62. *Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ defined over a field of positive characteristic $p \neq 2$. Let D be a dihedral group of automorphisms of $\mathcal{X}$. Then $|D| \leq 4g + 4$.*

In subsection 2.7.1 we also show that there exist precisely one case of group H of order multiple of p .

Theorem 2.63. *Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ defined over an algebraically closed field of characteristic $p \geq 3$. Then $\mathcal{X}$ has an automorphism group H of size divisible by p and greater than $4g(\mathcal{X}) + 4$ admitting a cyclic subgroup of index 2 if and only if $\mathcal{X}$ is birationally equivalent to the curve with equation*

$$y^p - y = x^m$$

for some $m > 1$ with $\text{GCD}(m, p) = 1$. In this case $g(\mathcal{X}) = \frac{(p-1)(m-1)}{2}$ and $|H| = 2pm$. Also H is generated by ρ and η where

$$\rho(x) = v^2x, \quad \rho(y) = y + 1$$

and

$$\eta(x) = vx, \quad \eta(y) = -y$$

with $v \in \mathbb{K}$ a primitive $2m$ -th root of unity.

In the subsequent subsections we assume that p does not divide the size of the group. In particular, throughout subsection 2.7.2 we provide a number of necessary conditions, which will then allow us to answer the previous questions. Such conditions are summarized as follows.

Theorem 2.64. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ with an automorphism group H of order $2N > 4g + 4$ admitting a cyclic subgroup of index 2. Let $\text{GCD}(|H|, p) = 1$. Then, the value $M = N - 2 - g$ is an integer divisor of N and H has the following description as an abstract group:*

$$H = \langle \rho, \sigma \mid \rho^N = \sigma^2 = 1, \sigma\rho\sigma = \rho^{lM-1} \rangle,$$

for some $l \in \{1, \dots, \frac{N}{M} - 1\}$, where the possible values of l modulo M are uniquely determined by N and M . An equation of $\mathcal{X}$ is

$$\mathcal{X} : y^N = x(1+x)^s$$

with

- $\text{GCD}(N, s+1) = 1$,
- $d := \text{GCD}(N, s+2) \geq 2$,
- $2g - 2 = N - 2 - \text{GCD}(N, s)$, and
- either N divides ds or $N - 1 - d < ds \pmod{N}$.

For p not dividing N , it turns out that for each $g \geq 2$ there is precisely one hyperelliptic curve of genus g with an automorphism group of size greater than $4g + 4$ admitting a cyclic subgroup of index 2; see Theorem 2.104. The size of the group in this case is $8g$. For non-hyperelliptic curves it turns out that an upper bound is $6g$; Corollary 2.106. Taking into account the possibility $m = 2$ in Theorem 2.63 for the case where p divides N , we have the following result.

Theorem 2.65. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over an algebraically closed field of characteristic $p \neq 2$. Let H be an automorphism group of $\mathcal{X}$ admitting a cyclic subgroup of index 2. Then*

$$|H| \leq \begin{cases} 8g + 4, & \text{if } p \neq 0; \\ 8g, & \text{if } p = 0. \end{cases}.$$

The bound is sharp for $p \neq 2$. For $p > 0$, $p \neq 2$ it is attained by the hyperelliptic curve with equation $y^p - y = x^2$; for $p = 0$ by hyperelliptic curves with equation $y^{4g} = x(1+x)^{2g}$.

It makes sense to define $\alpha(g)$ as the maximum size of an automorphism group of a non-hyperelliptic curve of genus $g \geq 2$ admitting a cyclic subgroup of index 2. Our main result about the value of $\alpha(g)$ is the following; see Section 2.7.3.

Theorem 2.66. *Let $\alpha(g)$ be the maximum size of automorphism group of size not divisible by p of a non-hyperelliptic algebraic curve of genus g which admits a cyclic subgroup of index 2. Then*

1. *if e is the smallest divisor of $2g$ such that $e + 1$ is coprime with $2g$, then*

$$\alpha(g) \geq 4g \frac{e+1}{e}. \quad (2.15)$$

2. *if $g \not\equiv 0 \pmod{210}$, then equality holds in (2.15). In particular,*

- $\alpha(g) = 6g$ when $g \not\equiv 0 \pmod{3}$;
- $\alpha(g) = \frac{16}{3}g$ when $g \equiv 3 \pmod{6}$;
- $\alpha(g) = 5g$ when $g \equiv 0 \pmod{6}$, $g \not\equiv 0 \pmod{30}$;
- $\alpha(g) = \frac{14}{3}g$ when $g \equiv 0 \pmod{30}$, $g \not\equiv 0 \pmod{210}$;

3. $\alpha(g) \leq \frac{32}{7}g$, $g \equiv 0 \pmod{210}$.

Curves of genus g with a group of size $\alpha(g)$ admitting a subgroup of index 2 are completely classified for $g \not\equiv 0 \pmod{210}$

Theorem 2.67. *For $g \geq 2$, $g \not\equiv 0 \pmod{210}$, curves of genus g admitting a tame automorphism group of size $\alpha(g)$ containing a cyclic subgroup of index 2 are precisely the following:*

- $\mathcal{X}(g) : y^{3g} = x(x+1)^g, g \equiv 1 \pmod{3}$
- $\mathcal{Y}(g) : y^{3g} = x(x+1)^{2g}, g \equiv 2 \pmod{3};$
- $\mathcal{A}(g) : y^{8g/3} = x(x+1)^{2g/3}, g \equiv 3 \pmod{6};$
- $\mathcal{B}(g) : y^{8g/3} = x(x+1)^{2g}, g \equiv 3 \pmod{6};$
- $\mathcal{F}(g) : y^{\frac{5}{2}g} = x(x+1)^{4g} g \equiv 6 \pmod{30};$
- $\mathcal{E}(g) : y^{\frac{5}{2}g} = x(x+1)^{3g} g \equiv 12 \pmod{30};$
- $\mathcal{C}(g) : y^{\frac{5}{2}g} = x(x+1)^g g \equiv 18 \pmod{30};$
- $\mathcal{D}(g) : y^{\frac{5}{2}g} = x(x+1)^{2g} g \equiv 24 \pmod{30};$
- $\mathcal{O}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{4g}{3}} g \equiv 30 \pmod{210};$
- $\mathcal{M}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{2g}{3}} g \equiv 60 \pmod{210};$
- $\mathcal{Q}(g) : y^{\frac{7}{3}g} = x(x+1)^{2g} g \equiv 90 \pmod{210};$
- $\mathcal{L}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{g}{3}} g \equiv 120 \pmod{210};$
- $\mathcal{P}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{5g}{3}} g \equiv 150 \pmod{210};$
- $\mathcal{N}(g) : y^{\frac{7}{3}g} = x(x+1)^g g \equiv 180 \pmod{210}.$

In every case, the group H has the following abstract form:

$$H = \langle \rho, \sigma \mid \rho^N = \sigma^2 = 1, \quad \sigma \rho \sigma = \rho^{N-s-1} \rangle.$$

where N (resp. s) is the exponent of y (resp $(x+1)$) in the equation of the curve.

Other examples of curves satysfying the hypothesis of Theorem 2.64 are given in Propositon 2.98.

2.7.1 Groups of size a multiple of p

Throughout the subsection, N is a positive integer and H is a subgroup of the automorphism group of a curve $\mathcal{X}$ of genus $g = g(\mathcal{X})$, admitting a cyclic subgroup G of order N and index 2 in H . In the sequel, ρ is a generator of G and σ is an element in $H \setminus G$. In this subsection, we deal with the case where N is a multiple of the characteristic $p \geq 3$.

The following statement can be deduced from the main result in [17].

Proposition 2.68. *Let $p \geq 3$, and let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ defined over a field of characteristic p with a cyclic automorphism group G of order $N > 2g(\mathcal{X}) + 2$ and divisible by p . Then, up to birational equivalence, $N = pm$ with $m > 1$, $(p, m) = 1$, and $p \neq 3$; also, $g(\mathcal{X}) = \frac{(p-1)(m-1)}{2}$ and*

$$\mathcal{X} : y^p - y = a(x^m - b) \tag{2.16}$$

for some $a, b \in \mathbb{K}$. Also, $G = \langle \rho \rangle$ with

$$\rho(x) = \lambda x, \quad \rho(y) = y + 1.$$

with λ a primitive m -th root of unity.

Proposition 2.69. *Up to birational equivalence, $a = 1$ and $b = 0$ can be assumed in 2.16.*

Proof. Let α and β be elements in $\mathbb{K}$ such that $\alpha^m = a$ and $\beta^p - \beta = -ab$. Also let $x = \frac{1}{\alpha}x'$ and $y = y' + \beta$. Then $(y')^p + \beta^p - y' - \beta = a\frac{1}{\alpha^m}(x')^m - ab$, whence $(y')^p - y' = (x')^m$. $\square$

We first prove the following preliminary result.

Theorem 2.70. *Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ defined over a field of positive characteristic $p \neq 2$, and G be a cyclic subgroup of $\text{Aut}(\mathcal{X})$ of order $N > 2g(\mathcal{X}) + 2$. Assume $p \mid N$ and that there exists an involution σ in $\text{Aut}(\mathcal{X}) \setminus G$ that normalizes G . Then, up to birational equivalence, $\mathcal{X} : y^p - y = x^m$, G is as in Proposition 2.68, m is odd, and*

$$\sigma(x) = -x, \quad \sigma(y) = -y + i,$$

with $i \in \mathbb{F}_p$. In particular, there are at most p involutions in $\text{Aut}(\mathcal{X}) \setminus G$ that normalize G .

Proof. As $p \geq 3$ divides the size of a cyclic group G of automorphisms of size larger than $2g + 2$, by Propositions 2.68 and 2.69 the only possibility is that $\mathcal{X}$ is birationally equivalent to the curve with equation $y^p - y = x^m$ and that G is as in the statement of Proposition 2.68.

The group G fixes the common pole P_∞ of x and y and acts with just another short orbit Δ , consisting of the p zeros of x .

As σ normalizes G , it acts on the short orbits of G . As $|\Delta| = p > 1$, we have that σ preserves both the point P_∞ and the set Δ . Let $H = \langle G, \sigma \rangle$. Then the factor group H/G acts on the quotient curve $\mathcal{X}/G$. Then $\sigma G \in H/G$ fixes the points $\bar{P}_\infty$ and $\bar{P}_0$ in $\mathcal{X}/G$ lying under P_∞ and Δ , respectively. Note that the fixed field of G is $\mathbb{K}(x^m)$; also, $\bar{P}_\infty$ is the only pole of $t = x^m$ in $\mathcal{X}/G$ and $\bar{P}_0$ is the only zero of t in $\mathcal{X}/G$. As there is just one involution of the projective line $\mathcal{X}/G$ fixing $\bar{P}_0$ and $\bar{P}_\infty$, we have $(\sigma G)(t) = -t$. This implies $\sigma(x^m) = -x^m$ and hence $(\sigma(x)/x)^m = -1$. Then $\sigma(x) = vx$ for some v with $v^m = -1$. As σ is an involution, we have $v^2 = 1$. This can only happen when m is odd and $v = -1$. Also, from $\sigma(y)^p - \sigma(y) = \sigma(x)^m$ it follows that

$$0 = \sigma(y)^p + y^p - \sigma(y) - y = (\sigma(y) + y)^p - (\sigma(y) + y),$$

that is $\sigma(y) = -y + i$ for some $i \in \{0, 1, \dots, p-1\}$. □

As a corollary of Theorem 2.70, we obtain that the bound $4g+4$ for dihedral automorphisms groups holds also for orders divided by the characteristic $p \geq 3$.

Theorem 2.71. *Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ defined over a field of positive characteristic $p \neq 2$. Let D be a dihedral group of automorphisms of $\mathcal{X}$. Then*

$$|D| \leq 4g(\mathcal{X}) + 4.$$

Proof. If the characteristic does not divide $|D|$, the result is a consequence of Theorem 2.41 and Theorem 2.45. If $p \geq 3$ divides $|D|$, then Theorem 2.70 implies that there are at most p involutions in $\text{Aut}(\mathcal{X})$ that normalize G . Therefore, there are at most p involutions in D , which is a contradiction for $|D| > 2p$. □

The aim of the final part of the subsection is to prove the following result.

Theorem 2.72. *Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X})$ defined over an algebraically closed field of characteristic $p \geq 3$. Then $\mathcal{X}$ has an automorphism group H of*

size divisible by p and greater than $4g(\mathcal{X}) + 4$ admitting a cyclic subgroup of index 2 if and only if $\mathcal{X}$ is birationally equivalent to the curve with equation

$$y^p - y = x^m$$

for some $m > 1$ with $\text{GCD}(m, p) = 1$. In this case $g(\mathcal{X}) = \frac{(p-1)(m-1)}{2}$ and $|H| = 2pm$. Also, H is generated by ρ and η where

$$\rho(x) = v^2x, \quad \rho(y) = y + 1$$

and

$$\eta(x) = vx, \quad \eta(y) = -y$$

with $v \in \mathbb{K}$ a primitive $2m$ -th root of unity.

Then the *only if* part in Theorem 2.72 is a Corollary to Propositions 2.68 and 2.69. To complete the proof of Theorem 2.72 we need the following statement.

Proposition 2.73. *Let $\mathcal{X}$ the curve defined over an algebraically closed field of characteristic $p \geq 3$ by the following equation:*

$$\mathcal{X} : y^p - y = x^m$$

for some $m > 1$ with $\text{GCD}(m, p) = 1$. Let ρ and η be defined as follows:

$$\rho(x) = v^2x, \quad \rho(y) = y + 1$$

and

$$\eta(x) = vx, \quad \eta(y) = -y$$

with $v \in \mathbb{K}$ a primitive $2m$ -th root of unity. Then

- (a) both ρ and η are automorphisms of $\mathcal{X}$;
- (b) the order of ρ is equal to pm and the order of η is $2m$;
- (c) Let u be the integer between 1 and pm such that $u \equiv 1 \pmod{m}$ and $u \equiv p - 1 \pmod{p}$; then $\eta\rho\eta^{-1} = \rho^u$.
- (d) the group generated by ρ and η has size $2pm$.

Proof. The fact that $\rho(y)^p - \rho(y) = \rho(x)^m$ depends on the fact that $(v^2)^m = 1$; on the other hand, $v^m = -1$ implies that η is an automorphism of $\mathcal{X}$. This proves (a). For a positive integer i we have $\rho^i(x) = v^{2i}x$, $\rho^i(y) = y + i$, $\eta^i(x) = v^i x$, $\eta^i(y) = (-1)^i y$. Since v is a primitive $2m$ -th root of unity and $\text{GCD}(p, m) = 1$, we have that (b) holds.

To prove (c), we compute $\eta\rho\eta^{-1}$. It turns out that $\eta\rho\eta^{-1}(x) = v^2x$ whereas $\eta\rho\eta^{-1}(y) = y - 1$. Now, let u be the integer between 1 and pm such that $u \equiv 1 \pmod{m}$ and $u \equiv p - 1 \pmod{p}$. Then $\rho^u(x) = v^2x$ and $\rho^u(y) = y + p - 1 = y - 1$, which implies $\eta\rho\eta^{-1} = \rho^u$.

Let $G = \langle \rho \rangle$ and $I = \langle \eta \rangle$. Note that $\eta^i \in G$ if and only if i is even, that is, $|G \cap I| = m$. Then $|GI| = 2pm$. To prove (d) we only need to note that by (c) we have $GI = IG$, that is, $\langle G, I \rangle$ coincides with GI . □

2.7.2 Groups of size coprime to p

Throughout this subsection we assume

$$|H| > 4g + 4, \quad (2.17)$$

and, if the characteristic of the ground field is $p > 0$, we assume that p does not divide $2N$.

Note that Condition (2.17) implies that $\mathcal{X}$ admits a cyclic group of automorphisms of size greater than $2g(\mathcal{X}) + 2$. From the classification obtained in [17], then $\mathcal{X}$ must be isomorphic to a curve of equation

$$\mathcal{X}(N, r, s) : y^N = x^r(1 + x)^s$$

where $1 \leq r, s < N$, $\text{GCD}(N, r, s) = 1$. Also, G is the subgroup generated by

$$\rho(x) = x, \rho(y) = \xi y, \quad (2.18)$$

where ξ is a primitive N -th root of unity. We recall some facts on curves of type $\mathcal{X}(N, r, s)$ from [17].

Theorem 2.74. *Let*

$$\mathcal{X}(N, r, s) : y^N = x^r(1 + x)^s$$

where $1 \leq r, s < N$, $\text{GCD}(N, r, s) = 1$, be defined over an algebraically closed field $\mathbb{K}$. If the characteristic p of $\mathbb{K}$ is $p > 0$, assume that p does not divide N . Then the following holds:

(i) The genus g of $\mathcal{X}(N, r, s)$ satisfies

$$2g - 2 = N - \text{GCD}(N, r) - \text{GCD}(N, s) - \text{GCD}(N, r + s).$$

(ii) There are exactly $M_1 := \text{GCD}(N, r)$ places of $\mathcal{X}(N, r, s)$, say $P_1, \dots, P_{M_1}$ centered at the affine point $(0, 0)$.

(iii) There are exactly $M_2 := \text{GCD}(N, s)$ places of $\mathcal{X}(N, r, s)$, say $R_1, \dots, R_{M_2}$ centered at the affine point $(-1, 0)$.

(iv) There are exactly $M_3 := \text{GCD}(N, r+s)$ places of $\mathcal{X}(N, r, s)$, say $Q_1, \dots, Q_{M_3}$ centered at the only infinite point of $\mathcal{X}(N, r, s)$.

(v) the divisors of x , $x + 1$, and y are

$$\text{div}(x) = \frac{N}{M_1}(P_1 + \dots + P_{M_1}) - \frac{N}{M_3}(Q_1 + \dots + Q_{M_3}),$$

$$\text{div}(x + 1) = \frac{N}{M_2}(R_1 + \dots + R_{M_2}) - \frac{N}{M_3}(Q_1 + \dots + Q_{M_3}),$$

and

$$\text{div}(y) = \frac{r}{M_1}(P_1 + \dots + P_{M_1}) + \frac{s}{M_2}(R_1 + \dots + R_{M_2}) - \frac{r+s}{M_3}(Q_1 + \dots + Q_{M_3}),$$

(vi) The genus of the quotient curve $\mathcal{X}(N, r, s)/\langle \rho \rangle$ is 0.

(vii) The only short orbits of the places of $\mathcal{X}(N, r, s)$ under the action of $\langle \rho \rangle$ are $\Omega_1 = \{P_1, \dots, P_{M_1}\}$, $\Omega_2 = \{R_1, \dots, R_{M_2}\}$, $\Omega_3 = \{Q_1, \dots, Q_{M_3}\}$.

Before delving into the investigation of the group H , we prove a series of results about the family of curves $\mathcal{X}(N, r, s)$.

Lemma 2.75. *Curves $\mathcal{X}(N, r, s)$, $\mathcal{X}(N, s, r)$, $\mathcal{X}(N, N - r - s, s)$, $\mathcal{X}(N, r, N - r - s)$ are birationally equivalent.*

Proof. Let $y^N = x^r(x + 1)^s$. Then

- for $x = 1/u$, $y = v/x$ we have $v^N = u^{N-r-s}(1 + u)^s$;
- for $x = -u - 1$ and $y = \zeta v$ with $\zeta^N = (-1)^{r+s}$ we have $v^N = u^s(1 + u)^r$;

- for $x = -\frac{u}{u+1}$, $y = \zeta \frac{v}{u+1}$ with $\zeta^N = (-1)^r$ we have $v^N = u^r(u+1)^{N-r-s}$

□

Let ρ be as in (2.18), and η be an element in $H \setminus G$. As $G = \langle \rho \rangle$ is normal in H , the factor group H/G has order 2 and acts on the projective line. By the Riemann-Hurwitz genus formula, H/G has exactly 2 fixed points on the projective line. This action is isomorphic to that of $\langle \eta \rangle$ on the orbits of $\mathcal{X} = \mathcal{X}(N, r, s)$ under G . As G acts exactly with three short orbits, we deduce that one of them is fixed and the other two are swapped. Moreover, there is also a long orbit Δ under G which is fixed by η . From now on, we denote with σ the non-trivial element in the stabilizer of any point in Δ . Then σ is an involution not belonging to G .

Proposition 2.76. *Let $M_i \geq 1$, $i = 1, 2, 3$, as in Theorem 2.74. Then without loss of generality we may assume that $M_1 = M_3 = 1$ and $M_2 > 2$.*

Proof. Note that (i) together with Condition (2.17) implies that at least one integer among M_1, M_2, M_3 is greater than 1. Without loss of generality, by Lemma 2.75, we may assume that $M_2 > 1$. We next show that $M_1 = M_3 = 1$ and $M_2 > 2$.

From the above discussion, for a $\eta \in H \setminus G$ we can distinguish three cases:

- (A) $\eta(\Omega_3) = \Omega_3$. Here Ω_1 and Ω_2 are swapped. If $\bar{\eta}$ is the non-trivial element in H/G , then we have

$$\bar{\eta}(0) = -1, \bar{\eta}(-1) = 0, \bar{\eta}(\infty) = \infty$$

Therefore the action of η on $\mathbb{K}(x)$ is determined; in particular

$$\eta(x) = -(x+1)$$

- (B) $\eta(\Omega_2) = \Omega_2$ Here Ω_1 and Ω_3 are swapped. Arguing as in case (A) we have

$$\eta(x) = 1/x$$

- (C) $\eta(\Omega_1) = \Omega_1$ Here Ω_2 and Ω_3 are swapped. Arguing as in case (A) we have

$$\eta(x) = -\frac{x}{x+1}$$

In order to investigate the possible values of $\eta(y)$, note that

$$\eta(y)^N = \eta(x)^r(1 + \eta(x))^s.$$

Therefore,

$$\left(\frac{\eta(y)}{y}\right)^N = \frac{\eta(x)^r(1 + \eta(x))^s}{x^r(1 + x)^s}.$$

The computation of the divisor of $\left(\frac{\eta(y)}{y}\right)$ will provide the statement will provide a contradiction in Cases (A) and (C).

- if (A) holds, then

$$\operatorname{div} \left(\left(\frac{\eta(y)}{y} \right)^N \right) = \frac{N(s-r)}{M_1}(P_1 + \dots + P_{M_1}) - \frac{N(s-r)}{M_2}(R_1 + \dots + R_{M_2})$$

Then $\frac{N(s-r)}{M_1}$ must be an integer multiple of N and M_1 is a divisor of $s-r$. As M_1 divides r but $\operatorname{GCD}(M_1, s) = 1$, the only possibility is $M_1 = 1$. Then $|\Omega_1| = 1$ and hence $|\Omega_2| = M_2 = 1$, a contradiction.

- if (B) holds, then

$$\operatorname{div} \left(\left(\frac{\eta(y)}{y} \right)^N \right) = \frac{N(2r+s)}{M_3}(Q_1 + \dots + Q_{M_3}) - \frac{N(2r+s)}{M_1}(P_1 + \dots + P_{M_1})$$

Then $\frac{N(2r+s)}{M_1}$ must be an integer multiple of N and M_1 is a divisor of $2r+s$. As M_1 divides r but $\operatorname{GCD}(M_1, s) = 1$, the only possibility is $M_1 = 1$. Then $|\Omega_1| = 1$ and hence $|\Omega_3| = M_3 = 1$ and

$$\operatorname{div} \left(\frac{\eta(y)}{y} \right) = (2r+s)(Q_1 - P_1).$$

Also, $2g-2 = N-2+M_2$ together with Condition (2.17) gives $M_2 > 2$.

- if (C) holds, then

$$\operatorname{div} \left(\left(\frac{\eta(y)}{y} \right)^N \right) = \frac{N(r+2s)}{M_3}(Q_1 + \dots + Q_{M_3}) - \frac{N(r+2s)}{M_2}(R_1 + \dots + R_{M_2})$$

Arguing as in case (B) we have $M_2 = M_3 = 1$, a contradiction.

□

From now on, we let $M = M_2$ as in Proposition 2.76 and Ω will denote the short orbit of G of size M .

We now show that $r = 1$ can be assumed in $\mathcal{X}(N, r, s)$.

Lemma 2.77. *The curve $\mathcal{X}(N, r, s)$ is birationally equivalent to $\mathcal{X}(N, 1, w)$ for some w . Also, $\text{GCD}(N, s) = 1$ if and only if $\text{GCD}(N, w) = 1$.*

Proof. As $M_1 = 1$ there exists an integer h such that $rh = 1 + N\ell$ for some $\ell \in \mathbb{Z}$. Let $w \in \{0, \dots, N-1\}$ be such that $sh \equiv w \pmod{N}$, that is, $sh = w + Nz$. Consider the following rational functions on $\mathcal{X}(N, r, s)$: $u = x$ and $v = \frac{y^h}{x^\ell(1+x)^z}$. Then

$$v^N = \frac{y^{hN}}{x^{\ell N}(1+x)^{zN}} = \frac{x^{rh}(1+x)^{sh}}{x^{\ell N}(1+x)^{zN}} = x(1+x)^w$$

□

Corollary 2.78. *Up to birational equivalence, $r = 1$ can be assumed.*

Two classes of curves $\mathcal{X}(N, r, s)$ for which Condition (2.17) holds are described as follows.

Example 2.79. Let $m > 3$ be an integer such that $p \nmid m^2 - 1$. Let

$$\mathcal{H}(m) : y^{m^2-1} = x(x+1)^{m-1} \tag{2.19}$$

be defined over an algebraically closed field $\mathbb{K}$. For a primitive $(m^2 - 1)$ -th root of unity $\xi \in \mathbb{K}$, let ρ and σ be the automorphisms of $\mathcal{H}(m)$ defined as follows:

- $\rho(x) = x, \rho(y) = \xi y$
- $\sigma(x) = \frac{1}{x}, \sigma(y) = \frac{x+1}{y^m}$

It is straightforward to check that

$$\rho^{m^2-1} = 1, \sigma^2 = 1, \sigma\rho\sigma = \rho^{m^2-m-1}.$$

Then, for $N = m^2 - 1$, the group H generated by ρ and σ has order $2N$. The genus of $\mathcal{X}$ is $\frac{|H|+2-2m}{4}$, which is clearly less than $\frac{|H|-4}{4}$ as $m > 3$.

Example 2.80. Let $m > 2$ be an integer such that $p \nmid m^2 - 1$. Let

$$\mathcal{L}(m) : y^{m^2-1} = x(x+1)^m \quad (2.20)$$

Let ρ be defined as in Example 2.79. Then $\sigma(x) = -(x+1)$, $\sigma(y) = -y^m/(x+1)$ is an automorphism which normalizes G , since $\sigma\rho\sigma^{-1} = \rho^m$. Also $\sigma^2 \in G$, so the group generated by G and σ has order $2N = 2(m^2 - 1)$. Note that the order of σ is 2 if m is even, 4 if m is odd. The genus of $\mathcal{X}$ is $\frac{|H|+2-2(m+1)}{4}$, which is clearly less than $\frac{|H|-4}{4}$ as $m > 2$.

By Lemma 2.75, Example 2.80 is isomorphic to

$$y^{m^2-1} = x(x+1)^{m^2-m-2}$$

In the following statements we determine some properties of the group H .

Lemma 2.81. *Let L be the (unique cyclic) subgroup of G of order N/M . Then the factor group H/L is the dihedral group of order $2M$.*

Proof. First, observe that L is a characteristic subgroup of G , hence it is normal in H . Moreover, L fixes the two points fixed by G and also each point in the orbit Ω of size M under the action of G . By the Riemann-Hurwitz genus formula, together with (i) of Theorem 2.74,

$$N - M - 2 = 2g(\mathcal{X}) - 2 = |L|(2g(\mathcal{X}/L) - 2) + 2(|L| - 1) + M(|L| - 1),$$

which implies that $\mathcal{X}/L$ is rational. The factor group H/L acts on the projective line as follows:

- has a short orbit of order 2;
- has two short orbits of order M , namely the images of Ω and Δ under the projection $\mathcal{X} \rightarrow \mathcal{X}/L$;
- every point in these two short orbits is fixed by some involution in H/L .

Then the claim follows from [32, Theorem 11.91]. □

Corollary 2.82. *If N/M is coprime to $2M$, then H is a semidirect product of a cyclic group of order N/M and a dihedral group of order $2M$.*

Proof. The claim is a consequence of Lemma 2.81 and the Schur-Zassenhaus Theorem (see e.g. [32, A.5(XI)]). □

Lemma 2.83. *Let L be as in Lemma 2.81 and let ρ be a generator of G . Then for any $\eta \in H \setminus G$ there exists $l \in \{0, \dots, |L| - 1\}$ such that $\eta^2 = \rho^{lM}$.*

Proof. By Lemma 2.81 H/L is dihedral and as ηL does not belong to the cyclic subgroup of H/L of order M , we have $(\eta L)^2 = L$. Therefore η^2 belongs to L and the claim follows. $\square$

As a consequence, we have the following result.

Theorem 2.84. *The group H has the following description as an abstract group:*

$$H = \langle \rho, \sigma \mid \rho^N = \sigma^2 = 1, \sigma \rho \sigma = \rho^{lM-1} \rangle,$$

for some $l \in \{1, \dots, \frac{N}{M} - 1\}$ such that $\text{GCD}(N, lM - 1) = 1$ and $(lM - 1)^2 \equiv 1 \pmod{N}$. Also, $\text{GCD}(N, lM) = M$.

Proof. The description of H follows from Lemma 2.83 applied to $\eta = \sigma\rho$, taking into account that for $l = 0$ the group H would be a dihedral group. As $\sigma\rho\sigma$ must be a generator of $\langle \rho \rangle$, condition $\text{GCD}(N, lM - 1) = 1$ holds. Finally, a straightforward computation shows

$$\rho = \sigma(\sigma\rho\sigma)\sigma = \rho^{(lM-1)^2}$$

which yields that N divides $(lM - 1)^2 - 1$.

To prove that $\text{GCD}(N, lM) = M$, assume by contradiction that $\text{GCD}(N, lM) = vM$ for some $v > 1$. Recall that $M > 2$. Let V be the subgroup of H generated by ρ^{vM} . As V is a characteristic subgroup of G , we have that V is normal in H . The factor group H/V has order $2vM$. We show that H/V is a dihedral group. The element $\bar{\rho} = \rho V$ has order vM and $\bar{\sigma} = \sigma V$ is an involution. Also,

$$\bar{\sigma}\bar{\rho}\bar{\sigma}\bar{\rho} = \sigma\rho\sigma\rho V = \rho^{lM}V = V.$$

We compute the genus $\bar{g}$ of the quotient curve $\mathcal{X}/V$. By the Riemann-Hurwitz genus formula, taking into account that V fixes $M + 2$ points and acts semiregularly on the other points of $\mathcal{X}$, we have

$$N - M - 2 = \frac{N}{vM}(2\bar{g} - 2) + (M + 2)\left(\frac{N}{vM} - 1\right);$$

whence, $vM = 2\bar{g} + M$ and $\bar{g} = (v - 1)M/2$. As $M > 2$, we have $\bar{g} \geq 2$. Also, H/V is a dihedral group of size $2vM > 4\bar{g} + 4 = 2(v - 1)M + 4$ acting on a curve of genus $\bar{g}(v - 1)M/2$, a contradiction to Theorem 2.71. $\square$

Theorem 2.85. *Let $\mathcal{X}$ be a curve $\mathcal{X}(N, 1, s)$ with $M = \text{GCD}(N, s) > 2$ and $\text{GCD}(N, s + 1) = 1$. A necessary condition for $\mathcal{X}$ to have an automorphism group of size greater than $4g(\mathcal{X}) + 4$ admitting a cyclic subgroup of index 2 is that there exists an integer t such that $\text{GCD}(N, t) = M$, $\text{GCD}(N, t + 1) = 1$ and $t^2 + 2t \equiv 0 \pmod{N}$.*

Proof. Let l be as in Theorem 2.84. Let $t = N - lM$. Then $\text{GCD}(N, t + 1) = \text{GCD}(N, N - (lM - 1)) = 1$ and $(t + 1)^2 = (N - lM + 1)^2 \equiv (lM - 1)^2 \equiv 1 \pmod{N}$. $\square$

Remark 2.86. *In the complex case, Theorem 2.85 can be proved by the theory of Fuchsian groups. Consider curves $\mathcal{X}(N, 1, s)$, with $\text{GCD}(N, s + 1) = 1$. For instance it is shown in [5, Example 6]) that in the complex case a necessary and sufficient condition for the existence of an automorphism group H of size $2N$ admitting a cyclic group of index 2 is that there exists an integer a such that $\text{GCD}(a + 1, N) = 1$, $\text{GCD}(a, N) = \text{GCD}(N, s)$, N divides $a^2 + 2a$.*

Remark 2.87. *In Theorem 2.85, condition $t^2 + 2t \equiv 0 \pmod{N}$ is equivalent to N/M dividing $t + 2$. In fact, N divides $t^2 + 2t$ if and only if*

$$M \cdot \frac{N}{M} \text{ divides } t(t + 2). \quad (2.21)$$

As $\text{GCD}(N, t) = M$, we have that M divides t and N/M is coprime with t/M . Then the claim follows.

Corollary 2.88. *The set $H \setminus G$ contains at least $M - 1$ involutions.*

Proof. By Lemma 2.83, we have

$$\{\alpha^2 \mid \alpha \in H \setminus G\} \subset \{1, \rho^M, \dots, \rho^{(\frac{N}{M}-1)M}\}.$$

Then, the N squares distribute on a set of $\frac{N}{M}$ possible outcomes, therefore there are at least $\lceil \frac{N}{M} \rceil - 1 = M - 1$ involutions in $H \setminus G$. $\square$

Corollary 2.89. *Let l be as in Theorem 2.84. Then N and M determine l modulo M . If $\text{GCD}(M, N/M) = 1$ then H is uniquely determined.*

As we will see later, the case $N = 3M$ is of particular interest.

Proposition 2.90. *If $M = N/3$, and 9 does not divide N , then*

- if $M \equiv 2 \pmod{3}$, then

$$H = \langle \rho, \sigma \mid \rho^N = \sigma^2 = 1, \sigma \rho \sigma = \rho^{M-1} \rangle$$

- if $M \equiv 1 \pmod{3}$, then

$$H = \langle \rho, \sigma \mid \rho^N = \sigma^2 = 1, \sigma \rho \sigma = \rho^{2M-1} \rangle$$

Lemma 2.91. *If $M = N/3$, then either $M = 4$ or M is odd.*

Proof. If M is even, then N is even and the only involution in G , say η , is central. Let $\hat{g}$ be the genus of the quotient curve $\mathcal{X}/\langle \eta \rangle$. Since η fixes precisely $M + 2$ points, the Riemann-Hurwitz genus formula gives

$$N - 2 - M = 2(2\hat{g} - 2) + M + 2,$$

that is $N/3 = 4\hat{g}$. If $\mathcal{X}/\langle \eta \rangle$ is elliptic then $N = 12$. Otherwise $\hat{g} \geq 2$ and $G/\langle \eta \rangle$ is a cyclic group of order $\frac{N}{2} > 4\hat{g} + \frac{N}{6}$. But this is impossible for $N > 12$, N a multiple of 4. $\square$

Remark 2.92. *If $M = N/3$ is odd the only possibility is that σ fixes 3 points in Δ and one point in Ω . This gives M involutions. By straightforward computation which takes into account Theorem 2.84, the M involutions are $\sigma \rho^{3j}$, with $j = 0, \dots, M - 1$.*

Lemma 2.93. *Without loss of generality one may assume that $\mathcal{X} = \mathcal{X}(N, 1, s)$, $\text{GCD}(N, s + 1) = 1$,*

$$\text{div} \left(\frac{\sigma(y)}{y} \right) = (s + 2)(Q_1 - P_1).$$

For $d = \text{GCD}(N, s + 2)$, d belongs to the Weierstrass semigroups at both P_1 and Q_1 .

Proof. Let α, β be integers such that

$$d = \alpha N - \beta(s + 2)$$

Recall that $\text{div}(x) = N(P_1 - Q_1)$. Then

$$\text{div} \left((x)^\alpha \left(\frac{\sigma(y)}{y} \right)^\beta \right) = d(P_1 - Q_1).$$

$\square$

Now we investigate the Weierstrass semigroup at points P_1, Q_1 . Let

$$A_N = \{(r, s) \in \mathbb{Z}^2 : r, s \geq 1 \text{ and } r + s \leq N - 1\}$$

and

$$A(r, s) = \{a \in \{1, \dots, N - 1\} \mid (ar \pmod{N}, as \pmod{N}) \in A_N\}.$$

The following result can be deduced from [36].

Proposition 2.94. *Let $(r, s) \in A_N$ such that $\text{GCD}(N, r) = 1$ (resp. $\text{GCD}(N, s) = 1$). The map*

$$\Psi : A(r, s) \longrightarrow \text{Gap}(P_1) \quad (\text{resp. } \text{Gap}(R_1)),$$

defined by $\Psi(a) = ar \pmod{N}$ (resp. $as \pmod{N}$), is bijective.

In [36] it is also implicitly proven the following:

Proposition 2.95. *Let $(r, s) \in A_N$ such that $\text{GCD}(N, s + 1) = 1$. The map*

$$\Psi : A(r, s) \longrightarrow \text{Gap}(Q_1),$$

defined by $\Psi(a) = -a(s + r) \pmod{N}$ is bijective.

For $r = 1$, the elements in $A(1, s)$ are $a \in \{1, \dots, N - 1\}$ such that

$$N - 1 - a \geq as \pmod{N} \geq 1. \quad (2.22)$$

Therefore, gaps at P_1 are $a \in \{1, \dots, N - 1\}$ such that Condition (2.22) holds. Similarly, gaps at Q_1 are $-a(s + 1) \pmod{N}$ for each $a \in \{1, \dots, N - 1\}$ such that Condition (2.22) holds.

Then we have the following Proposition.

Theorem 2.96. *A necessary condition for a curve $\mathcal{X}$ to have a tame automorphism group H admitting a cyclic subgroup of index 2 with $|H| > 4g(\mathcal{X}) + 4$ is that $\mathcal{X} : y^N = x(1 + x)^s$ with $\text{GCD}(N, s + 1) = 1$, $d = \text{GCD}(N, s + 2) \geq 2$ and N divides ds or $N - 1 - d < ds \pmod{N}$.*

Obvious cases where the necessary condition of Proposition 2.96 holds are $N = (s + 1)(s - 1)$ and $N = s(s + 2)$. The former case is $\mathcal{L}(m)$ of Example 2.80, whereas the latter is $\mathcal{H}(m)$ of Example 2.79 for $m = s + 1$. Note that $\mathcal{L}(m)$ and $\mathcal{H}(m)$ are not isomorphic as they have different genera.

Remark 2.97. *Since there is an automorphism of the curve mapping P_1 to Q_1 , then the Weierstrass semigroups at P_1 and Q_1 must coincide. Therefore, the sets $\{a \mid a \in A(1, s)\}$ and $\{-a(s + 1) \pmod{N} \mid a \in A(1, s)\}$ must be equal.*

2.7.3 Classification results

In this subsection we classify curves which for a fixed genus g admit the largest possible automorphism group with a cyclic subgroup of index 2, distinguishing the hyperelliptic and the non-hyperelliptic case.

We first provide an extension of Examples 2.79 and 2.80.

Proposition 2.98. *Assume that N divides $s^2 + 2s$, $\text{GCD}(N, s) > 1$ and $\text{GCD}(N, s + 1) = 1$. Assume also that the characteristic of the ground field $\mathbb{K}$ does not divide $2N$. Then $\mathcal{X}(N, 1, s)$ is a curve of genus $g = \frac{N - \text{GCD}(N, s)}{2}$ with an automorphism group H of order $2N$ which contains a cyclic subgroup of index 2.*

Proof. Let $a = (s^2 + 2s)/N$ and let ξ be a primitive N -th root of unity in $\mathbb{K}$. Let ρ and σ be defined as follows:

- $\rho(x) = x, \rho(y) = \xi y;$
- $\sigma(x) = \frac{1}{x}, \sigma(y) = \frac{(x+1)^a}{y^{s+1}}.$

Clearly ρ is an automorphism of order N . It is straightforward to check that σ is an involution preserving $\mathcal{X}(N, 1, s)$ since $\sigma^2(x) = x$ and

$$\sigma^2(y) = \sigma\left(\frac{(x+1)^a}{y^{s+1}}\right) = \left(\frac{(x+1)^a}{x^a}\right) \frac{y^{(s+1)^2}}{(x+1)^{a(s+1)}} = y \frac{y^{aN}}{x^a(x+1)^{as}} = y$$

Also, σ is an automorphism of $\mathcal{X}(N, 1, s)$ since

$$\sigma(y)^N = \frac{(x+1)^{aN}}{y^{(s+1)N}} = \frac{(x+1)^{s^2+2s}}{x^{s+1}(x+1)^{s^2+2s}}, \quad \sigma(x)(\sigma(x)+1)^s = \frac{1}{x} \left(\frac{1}{x} + 1\right)^s = \frac{1}{x^{s+1}}(1+x)^s$$

Finally, it is straightforward to check that

$$\sigma\rho\sigma = \rho^{N-s-1}.$$

□

Theorem 2.99. *The only curves with an automorphism group of size greater than $4g+4$ admitting a cyclic subgroup of index 2 are precisely those described in Proposition 2.98, plus possibly other curves with the same genus.*

Proof. This is a straightforward consequence of Theorem 2.85. □

Corollary 2.100. *For an integer $N > 6$ the genera $g \geq 2$ of curves with an automorphism group of size $2N > 4g+4$ admitting a cyclic subgroup of index 2 are precisely the integers $\frac{N-M}{2}$ where M is a divisor of N such that there exists $v \in \{1, \dots, \frac{N}{M} - 1\}$ for which $\text{GCD}(N, vM) = M$, $\text{GCD}(N, vM + 1) = 1$ and $vM + 2 \equiv 0 \pmod{N/M}$. An example of a curve with that genus is $y^N = x(1+x)^{vM}$. In this case, the automorphisms in H are explicitly described in Theorem 2.98.*

Theorem 2.101. *Let $\mathcal{S}$ be the spectrum of possible sizes $2N > 4g + 4$ of automorphism group of curves of genus g admitting a cyclic subgroup of index 2. Then*

$$\mathcal{S} = \left\{ 4g \frac{e+1}{e} \mid e \in \mathbb{N}, e \neq 0 \right\}.$$

Proof. We first show that $4g \frac{e+1}{e} \in \mathcal{S}$ for each positive integer e . For $e > 1$ put $s = e - 1$ and take $N = s(s+2)$. Then clearly $\text{GCD}(N, s) = s$ and $2N = 4g + 2s$. But $s = \frac{s(s+2)-s}{s+1} = 2g/(s+1)$, whence

$$2N = 4g(1 + 1/s(s+1)) = 4g \frac{s+2}{s+1}$$

For $e = 1$, take $s = 2g$ and $N = 4g$.

To complete the proof, assume that there exists a curve of genus g with an automorphism group with the required properties. By Proposition 2.76, the curve is isomorphic to some $\mathcal{X}(N, 1, s)$ with $\text{GCD}(N, s) > 1$ and $\text{GCD}(N, s+1) = 1$; also, $2g = N - \text{GCD}(N, s)$. Let $e = \frac{N}{\text{GCD}(N, s)} - 1$. Then $2N = 4g \frac{e+1}{e}$. $\square$

Corollary 2.102. *Let g be an integer greater than 2. Let e be the smallest divisor of $2g$ such that $e+1$ is coprime with $2g$. Then there exists a curve of genus g with an automorphism group of size $4g \frac{e+1}{e}$ admitting a cyclic subgroup of index 2.*

Proof. Clearly $e+1$ has no common factor with $\frac{2g}{e}$. Then there exists an integer $v \in \{1, \dots, e\}$ such that

$$v \frac{2g}{e} + 2 \equiv 0 \pmod{e+1}.$$

Let $N = (e+1) \frac{2g}{e}$ and $s = v \frac{2g}{e}$. By Proposition 2.98, $\mathcal{X}(N, 1, s)$ has an automorphism group of order $2N$ admitting a cyclic group of index 2. Also, the genus of $\mathcal{X}(N, 1, s)$ is clearly g . $\square$

Recall that a pair of rational numbers (a, b) is said to be *admissible* if there exists a family of curves with infinite distinct genera g admitting an automorphism group of size $ag + b$.

Theorem 2.103. *Pairs*

$$\left\{ \left(4 \frac{e+1}{e}, 0 \right) \mid e \geq 1, e \text{ even} \right\}$$

and pairs

$$\left\{ \left(4 \frac{e+1}{e+1-2^k}, 0 \right) \mid e \geq 1, e \text{ odd}, \frac{e+1}{2^k} > 1 \text{ odd} \right\}$$

are admissible.

Proof. Let e be an even integer. The set of even multiples t of e which are coprime with $e+1$ is clearly an infinite set. Then clearly $GCD(\frac{t}{e}, e+1) = 1$ and $GCD(t \frac{e+1}{e}, v \frac{t}{e}) = \frac{t}{e}$ for each $v \in \{1, \dots, e\}$. Let v_0 be such that

$$v_0 \frac{t}{e} + 2 \equiv 0 \pmod{e+1}.$$

Then the curve

$$y^{t \frac{e+1}{e}} = x(1+x)^{v_0 \frac{t}{e}}$$

has genus $t/2$. Also, $t \frac{e+1}{e}$ divides $\frac{t}{e}(v_0 \frac{t}{e} + 2)$. Then the claim for even e follows by Proposition 2.98.

If e is odd, let k be the highest integer such that 2^k divides $e+1$. Assume that $e+1$ is not a power of 2. Again, the set of even multiples t' of e which are coprime with $(e+1)/2^k$ is an infinite set. Also, $GCD(\frac{t'}{e}, \frac{e+1}{2^k}) = 1$ and $GCD(t' \frac{e+1}{2^k e}, v \frac{t'}{e}) = \frac{t'}{e}$ for each $v \in \{1, \dots, ((e+1)/2^k) - 1\}$. Let v_0 be such that

$$v_0 \frac{t'}{e} + 2 \equiv 0 \pmod{\frac{e+1}{2^k}}.$$

Then the curve

$$y^{t' \frac{e+1}{2^k e}} = x(1+x)^{v_0 \frac{t'}{e}}$$

has genus $\frac{t'}{2} \cdot \frac{e+1-2^k}{2^k e}$. Also, $t' \frac{e+1}{2^k e}$ divides $\frac{t'}{e}(v_0 \frac{t'}{e} + 2)$. Then the claim follows by Proposition 2.98. $\square$

Theorem 2.104. *For every genus $g \geq 2$ there exists a unique curve of genus g with an automorphism group of order $8g$ admitting a cyclic subgroup of index 2. Such a curve is*

$$\mathcal{I}(g) : y^{4g} = x(1+x)^{2g}.$$

Proof. In order to have $|H| = 8g$, the only possibility is $N = 4g$, $M = N/2$ and an equation of the curve being that of $\mathcal{I}(g)$. As a matter of fact, $GCD(4g, 2g) = 1$, $GCD(4g, 2g + 1) = 1$, $4g$ divides $2g(2g + 2)$. Hence by Proposition 2.98 $\mathcal{I}(g)$ has an automorphism group of order $8g$ admitting a cyclic subgroup of index 2. $\square$

Note that $\mathcal{I}(g)$ is a hyperelliptic curve, since by the proof of Lemma 2.81 the involution ρ^{2g} is such that the quotient curve $\mathcal{I}(g)/\langle \rho^{2g} \rangle$ is rational.

Throughout the remaining part of the subsection we assume that $\mathcal{X}$ is not hyperelliptic. Therefore, by Lemma 2.81 we have $N/M \geq 3$.

Proposition 2.105. *Let d be as in Proposition 2.7.2. Then $d \geq 3$.*

Proof. As d is a non-gap at some point of $\mathcal{X}$, the claim follows from the assumption that $\mathcal{X}$ is not hyperelliptic. $\square$

Corollary 2.106. *If $\mathcal{X}$ is not hyperelliptic, then $|H| \leq 6g$.*

Proof. As $|L| \geq 3$, we have $M \leq N/3$. Hence $2g = N - M \geq \frac{2}{3}N$. $\square$

We are going to discuss whether, for a fixed genus g , the curve described in Corollary 2.102 is actually the curve with the largest possible automorphism group admitting a cyclic subgroup of index 2. The case $g \not\equiv 0 \pmod{3}$, corresponding to $e = 2$ in Corollary 2.102, is dealt with first.

Theorem 2.107. *Let $\mathcal{X}$ be a curve of genus g admitting an automorphism group H of size $6g$ containing a cyclic group of order $3g$. Then $\mathcal{X}$ is birationally equivalent to one of the two curves*

- $\mathcal{X}(g) : y^{3g} = x(x+1)^g$, for 3 dividing $g-1$;
- $\mathcal{Y}(g) : y^{3g} = x(x+1)^{2g}$, for 3 dividing $g-2$.

Proof. We first note that both $\mathcal{X}(g)$ and $\mathcal{Y}(g)$ have genus g and admit an automorphism group of order $6g$ containing a cyclic subgroup of index 2. In fact, for $g \equiv 1 \pmod{3}$ the integer $3g$ is a divisor of $g(g+2)$, and similarly for $g \equiv 2 \pmod{3}$ we have that $3g$ divides $2g(2g+2)$. Then Proposition 2.98 provides for both $\mathcal{X}(g)$ and $\mathcal{Y}(g)$ an explicit description of the required automorphism group.

Assume now that $\mathcal{X} = \mathcal{X}(N, 1, s)$ with $GCD(N, s) > 1$ and $GCD(N, s+1) = 1$. By $2N = 6g$ and

$$2g - 2 = N - 2 - N/3$$

if follows $N = 3g$ and $GCD(N, s) = g$. Then 3 does not divide g and either $s = g$ or $s = 2g$. In the former case $GCD(3g, g+1) = 1$ yields 3 divides $g-1$; in the latter case, similarly, 3 divides $g-2$. $\square$

Remark 2.108. *In the complex case, Nakagawa [50] classified curves with an automorphism of order $3g$. Very recently, Reyes and Speziali [55] showed that the full automorphism group of $\mathcal{X}(g)$ and $\mathcal{Y}(g)$, viewed as Riemann surfaces, is the direct product of a cyclic group of order 3 by a dihedral group of order $2g$, without describing explicit equations for σ .*

Corollary 2.109. *If $\mathcal{X}$ is not birationally equivalent to either $\mathcal{X}(g)$ or $\mathcal{Y}(g)$ then $|H| \leq \frac{16}{3}g$.*

Proof. If $N/M = 3$ then $|H| = 6g$. Otherwise $N \geq 4M$ and $2g = N - M \geq \frac{3}{4}N$. $\square$

Theorem 2.110. *If $\mathcal{X}$ is a curve of genus $g \equiv 0 \pmod{3}$, then $|H| \leq 16g/3$. The bound is attained if and only if g is odd and $\mathcal{X}$ is birationally equivalent to one the two curves*

- $\mathcal{A}(g) : y^{\frac{8}{3}g} = x(x+1)^{\frac{2}{3}g}$,
- $\mathcal{B}(g) : y^{\frac{8}{3}g} = x(x+1)^{2g}$.

Proof. We first prove the necessary condition. The upper bound is attained if and only if $N = 4M$, so that $2N = 16g/3$. As $N/4$ divides s , the only possibilities for s are $s = N/4 = 2g/3$, $s = N/2 = 4g/3$, or $s = 3N/4 = 2g$. In particular, s is even. Note that the greatest common divisor of N and $s+1$ is equal to 1. As $GCD(N, s+2)$ is at least 3 (see Proposition 2.105), the case $s = N/2$ cannot occur as $GCD(N, (N/2)+2) = 2$. Also, in the other two cases, $GCD(N, s+2) > 2$ implies that g is odd.

To conclude the proof, we need to show that actually $\mathcal{A}(g)$ and $\mathcal{B}(g)$ have an automorphism group of order $\frac{16}{3}g$ admitting a cyclic group of index 2. Note that since g is odd, then $\frac{8}{3}g$ divides both $\frac{2}{3}g(\frac{2}{3}g+2)$ and $2g(2g+2)$. Then the claim follows by Proposition 2.98. $\square$

Theorem 2.111. *If $\mathcal{X}$ is a curve of genus $g \equiv 0 \pmod{6}$, then $|H| \leq 5g$. The bound is attained if and only if $g \not\equiv 0 \pmod{30}$ and $\mathcal{X}$ is birationally equivalent to one the curves below:*

- $\mathcal{C}(g) : y^{\frac{5}{2}g} = x(x+1)^g \ (g \equiv 18 \pmod{30})$

- $\mathcal{D}(g) : y^{\frac{5}{2}g} = x(x+1)^{2g} \ (g \equiv 24 \pmod{30})$
- $\mathcal{E}(g) : y^{\frac{5}{2}g} = x(x+1)^{3g} \ (g \equiv 12 \pmod{30})$
- $\mathcal{F}(g) : y^{\frac{5}{2}g} = x(x+1)^{4g} \ (g \equiv 6 \pmod{30})$

Proof. Assume that $\mathcal{X} = \mathcal{X}(N, 1, s)$ with $GCD(N, s) > 1$ and $GCD(N, s+1) = 1$. By $2N = 5g$ and

$$2g - 2 = N - 2 - N/5$$

it follows $N = \frac{5}{2}g$ and $GCD(N, s) = g$. Then, as $s < N$, we have that $s \in \{g, 2g, 3g, 4g\}$. Recall that $GCD(N, s+1) = GCD(5(g/2), s+1) = 1$ and that $d := GCD(N, s+2) = GCD(5(g/2) + 2, s)$ must be greater than 2.

Assume that $s = g$. As $GCD(5(g/2), 2(g/2) + 2) > 2$ actually $g \equiv 3 \pmod{5}$ and hence $g \equiv 18 \pmod{30}$. If $s = 2g$, $GCD(5(g/2), 2g + 2) > 2$ implies $g \equiv 4 \pmod{5}$ and hence $g \equiv 24 \pmod{30}$. Similarly, if $s = 3g$ then 5 must divide $3g + 2$ and $g \equiv 1 \pmod{5}$; $s = 4g$, then 5 divides $4g + 2$ and $g \equiv 2 \pmod{5}$.

Then $\mathcal{X}$ is birationally equivalent to one of the curve described in the statement.

To conclude the proof, we need to show that actually $\mathcal{C}(g)$, $\mathcal{D}(g)$, $\mathcal{E}(g)$, and $\mathcal{F}(g)$ have an automorphism group of order $5g$ admitting a cyclic group of index 2. Note that in each case 5 divides $s + 2$. Hence $5\frac{g}{2}$ divides $g(s+2)$ and hence $s(s+2)$. Then the claim follows by Proposition 2.98. $\square$

Theorem 2.112. *If $\mathcal{X}$ is a curve of genus $g \equiv 0 \pmod{30}$, then $|H| \leq \frac{14}{3}g$. The bound is attained if and only if $g \not\equiv 0 \pmod{210}$ $\mathcal{X}$ is birationally equivalent to one of the curves below:*

- $\mathcal{L}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{g}{3}}, \text{ with } g \equiv 120 \pmod{210};$
- $\mathcal{M}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{2g}{3}}, \text{ with } g \equiv 60 \pmod{210};$
- $\mathcal{N}(g) : y^{\frac{7}{3}g} = x(x+1)^g, \text{ with } g \equiv 180 \pmod{210};$
- $\mathcal{O}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{4g}{3}}, \text{ with } g \equiv 30 \pmod{210};$
- $\mathcal{P}(g) : y^{\frac{7}{3}g} = x(x+1)^{\frac{5g}{3}}, \text{ with } g \equiv 150 \pmod{210};$
- $\mathcal{Q}(g) : y^{\frac{7}{3}g} = x(x+1)^{2g}, \text{ with } g \equiv 90 \pmod{210}.$

Proof. As $g \equiv 0 \pmod{30}$

$$2g - 2 = N - 2 - \frac{N}{m}$$

for some $m \geq 6$. We first show that actually $m > 6$. Assume by contradiction that $m = 6$. Then $N = 12\frac{g}{5}$, $s = 2v\frac{g}{5}$ for some $v \in \{1, 2, 3, 4, 5\}$. Also,

$$\text{GCD}\left(12\frac{g}{5}, 2v\frac{g}{5} + 1\right) = 1, \quad \text{GCD}\left(12\frac{g}{5}, 2v\frac{g}{5} + 2\right) > 2.$$

Then, $\text{GCD}(6\frac{g}{5}, v\frac{g}{5} + 1) > 1$. As 6 divides $\frac{g}{5}$, this is impossible.

Assume then that $m = 7$. Then $N = 14\frac{g}{6}$, $s = 2v\frac{g}{6}$ for some $v \in \{1, 2, 3, 4, 5, 6\}$. Also,

$$\text{GCD}\left(14\frac{g}{6}, 2v\frac{g}{6} + 1\right) = 1, \quad \text{GCD}\left(14\frac{g}{6}, 2v\frac{g}{6} + 2\right) > 2.$$

Then, $\text{GCD}(7\frac{g}{6}, v\frac{g}{6} + 1) > 1$, that is, 7 divides $v\frac{g}{6} + 1$. For 7 a divisor of g this is clearly impossible. Otherwise this can happen for only one v , namely the inverse of $-\frac{g}{6}$ modulo 7. For this value of v , condition N a divisor of $s(s+2)$ is satisfied since 14 divides $s+2$ and $\frac{g}{6}$ divides s . Then the claim follows by Proposition 2.98. $\square$

Remark 2.113. By Proposition 2.98, for all curves $\mathcal{A}(g)$ - $\mathcal{Q}(g)$, as well as $\mathcal{X}(g)$ and $\mathcal{Y}(g)$, the group H has the following abstract form :

$$H = \{\rho, \sigma \mid \rho^N = \sigma^2 = 1, \quad \sigma\rho\sigma = \rho^{N-s-1}\}.$$

Chapter 3

Galois subcovers of the Hermitian curve

Curves with many points over a finite field have intensively been investigated, particularly for their useful connections to Coding theory, Cryptography, Finite geometry, and shift register sequences. In this context, the most important family consists of the maximal curves introduced in section 1.3. The Hermitian curve is the most known maximal curve and it is also very used for applications, especially in the study of Algebraic-Geometric codes, shortly AG-codes. Actually, many other maximal curves derive from the Hermitian curve since any $\mathbb{F}_{q^2}$ -subcover of a maximal curve is still maximal over the same field. If such a $\mathbb{F}_{q^2}$ -subcover is a Galois subcover with Galois group G then the arising curve is named the quotient curve of the Hermitian curve with respect to G . Up to group isomorphism, the $\mathbb{F}_{q^2}$ -automorphism group of the Hermitian curve is the 3-dimensional projective unitary group $\text{PGU}(3, q)$ which has plenty of subgroups; see [33]. This motivated the systematic study of the quotients curves of the Hermitian curve which was eventually initiated in the seminal paper of Garcà, Stichtenoth and Xing [23]. Ever since important progress has been made in the study of the spectrum of the possible genera of the quotients of the Hermitian curve over a given finite field; see [32, Chapter 10]. Nevertheless, the problem of determining explicit equations for such curves, which is a relevant issue for applications, remains largely open. In fact, this problem has so far been solved by ad hoc methods, apart from the cases where the Galois group has either prime order; see [10], or its order equals the square of the characteristic; see [19].

In this chapter we determine explicit equations for each quotient curve of

the Hermitian curve whose Galois group has order dp where p is the characteristic of $\mathbb{F}_{q^2}$ and d is a prime other than p . We also compute the Weierstrass semigroup at some $\mathbb{F}_{q^2}$ -rational point of those curves, and discuss possible positive impacts on the minimum distance problems of AG-codes. The results presented in this chapter are the subject of the paper [15].

Our main result is the following.

Theorem 3.1. *In the $\mathbb{F}_{q^2}$ -automorphism group $G \cong \text{PGU}(3, q)$ of the Hermitian curve $\mathcal{H}_q$ defined over $\mathbb{F}_{q^2}$ with $q = p^h$ and $p \geq 5$, let H be a subgroup of order dp where $d \geq 5$ is a prime number other than p . Let $\bar{\mathcal{H}}_q = \mathcal{H}_q/H$ be the quotient curve of $\mathcal{H}_q$ with respect to the subgroup H . Then, up to an $\mathbb{F}_{q^2}$ -isomorphism, one of the following cases occurs.*

(I) *If $H = C_p \times C_d$ then $\bar{\mathcal{H}}_q$ has genus*

$$\mathfrak{g} = \frac{1}{2d}(q - d + 1) \left(\frac{q}{p} - 1 \right)$$

and equation

$$\sum_{i=0}^{h-1} Y^{p^i} + \omega X^{(q+1)/d} = 0 \quad \text{with} \quad \omega^{q-1} = -1 \quad \text{and} \quad d \mid (q+1). \quad (3.1)$$

(II) *If $H = C_p \rtimes C_d$ and C_p is in the center of a Sylow p -subgroup of G , then $\bar{\mathcal{H}}_q$ has genus*

$$\mathfrak{g} = \frac{1}{2} \frac{q}{d} \left(\frac{q}{p} - 1 \right)$$

and equation

$$\omega X^{(q-1)/d} - A(X, Y) = 0 \quad \text{with} \quad \omega^{q-1} = -1 \quad \text{and} \quad d \mid (p-1). \quad (3.2)$$

where

$$A(X, Y) = Y + X^{2(p-1)/d} Y^p + \dots + X^{2(p^{h-1}-1)/d} Y^{q/p}.$$

(III) *If $H = C_p \rtimes C_d$ but C_p is not in the center of a Sylow p -subgroup of G , then $\bar{\mathcal{H}}_q$ has genus*

$$\mathfrak{g} = \frac{q}{2dp}(q-1)$$

and equation

$$\left(\frac{Y^2}{X^d} \right)^{(q-1)/d} + 1 - A(X, Y) = 0 \quad \text{and} \quad d \mid (p-1) \quad (3.3)$$

where

$$A(X, Y) = \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} \left(\frac{Y^2}{X^d} \right)^{(p^i-1)/2d} \left(\frac{Y^2}{X^d} \right)^{(p^j-1)/2d} X^{(p^i+p^j)/2}.$$

Throught this chapter, the following results will play a role in the proofs.

Result 3.2. [32, Theorem 11.129] *If $\mathcal{X}$ has zero Hasse-Witt invariant then every non-trivial element of order p has a unique fixed point, and hence no non-trivial element in S_P fixes a point other than P .*

A useful corollary of Result 3.2 is the following.

Result 3.3. *Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_\ell$ whose number of $\mathbb{F}_\ell$ -rational points is $N \geq 2$. If $\mathcal{X}$ has zero Hasse-Witt invariant and S is a p -subgroup of $\text{Aut}_{\mathbb{F}_\ell}(\mathcal{X})$ then S fixes a unique point and $|S|$ divides $N - 1$.*

The following result is due to Stichtenoth [63].

Result 3.4. [32, Theorem 11.78(i)] *Let H be a p -subgroup of $\mathbb{F}(\mathcal{X})$ fixing a point. If $|S|$ is larger than the genus of $\mathbb{F}(\mathcal{X})$ then the Galois subcover of $\mathbb{F}(\mathcal{X})$ with respect to H is rational.*

From now on let $\ell = q^2$ with $q = p^h$ and assume that $\mathcal{X}$ is a $\mathbb{F}_{q^2}$ -maximal curve.

We also use the classification of all groups whose order is the product of two distinct primes.

Result 3.5. *Suppose u and v are distinct prime numbers with $u < v$. Then, there are two possibilities for groups G of order uv :*

- (I) *If $u \nmid (v - 1)$ then G is a cyclic group.*
- (II) *If $u \mid (v - 1)$, then either G is a cyclic group, or G is a semidirect product $C_v \rtimes C_u$.*

3.1 The function field of the Hermitian curve

We refer to Section 1.3 for preliminary results on the automorphisms of the Hermitian curve.

Next, for the sake of completeness, we provide a proof for the classification of subgroups of $\text{PGU}(3, q)$ of order dp . We use the canonical form $y^q - y + \omega x^{q+1} = 0$ with $\omega^{q-1} = -1$. The Galois subcovers of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to a subgroup H of prime order or when its order equals the square of the characteristic were thoroughly classified in [10] and [19] respectively. For the case $|H| = dp$, the classification is reported in the following result.

Theorem 3.6. *Let p and d be two distinct prime numbers both larger than 3. Then, up to conjugacy in $\text{PGU}(3, q)$, there exist at most three subgroups of order dp in $\text{PGU}(3, q)$, one is cyclic and the other two are semidirect products of $C_p \rtimes C_d$ with $p < d$. They are subgroups of the stabilizer of Y_∞ in $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$ with*

- (I) $G = \Sigma_p \times \Sigma_d$ with $\Sigma_p = \langle \varphi_{0,1,1} \rangle$ and $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$ with $\lambda^d = 1$, $d|(q+1)$;
- (II) $G = \Sigma_p \rtimes \Sigma_d$ with $\Sigma_p = \langle \varphi_{0,1,1} \rangle$ and $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$ with $\lambda^d = 1$, $d|(p-1)$;
- (III) $G = \Sigma_p \rtimes \Sigma_d$ with $\Sigma_p = \langle \varphi_{1,\omega/2,1} \rangle$ and $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$ with $\lambda^d = 1$, $d|(p-1)$.

Proof. Let G be a subgroup of order pd in $\text{PGU}(3, q)$. Two cases are treated separately according as $p > d$ or $p < d$.

Case $p > d$

In this case, Result 3.5 shows that G has a unique Sylow p -subgroup Σ_p . Moreover, Σ_p is a normal subgroup of G , and hence $G = \Sigma_p \rtimes \Sigma_d$ where Σ_d is a Sylow d -subgroup of G . Since any non-trivial element of $\text{PGU}(3, q)$ of order p has exactly one fixed point on $\mathcal{H}_q(\mathbb{F}_{q^2})$ whereas $\text{PGU}(3, q)$ acts transitively on $\mathcal{H}_q(\mathbb{F}_{q^2})$, we may assume, up to conjugacy in $\text{PGU}(3, q)$, that Y_∞ is the unique fixed point of Σ_p . As Σ_p is a normal subgroup of G , the point Y_∞ is also fixed by Σ_d . From $|\mathcal{H}_q(\mathbb{F}_{q^2})| - 1 = q^3$, Σ_d must have a fixed point $O \in \mathcal{H}_q(\mathbb{F}_{q^2})$ other than Y_∞ . Since $\text{PGU}(3, q)$ is doubly transitive on $\mathcal{H}_q(\mathbb{F}_{q^2})$ we may assume, up to conjugacy, that $O = (0 : 0 : 1)$. Then Σ_d is generated by $t = \varphi_{0,0,\lambda}$ with $\lambda^d = 1$ where $d|(q^2 - 1)$. Furthermore, as Σ_p is a subgroup of the Sylow subgroup S_p of $\text{PGU}(3, q)$ fixing Y_∞ , two cases arise according as Σ_p is in the center $Z(S_p)$ of S_p or not. Let s be a generator of Σ_p . If $s \in Z(S_p)$ then $s = \varphi_{0,b,1}$ with $b^q - b = 0$. Take $\mu \in \mathbb{F}_{q^2}^*$ such that $\mu^{q+1} = b^{-1}$. Then the conjugate of s by $\varphi_{0,0,\mu}$ is $\varphi_{0,0,1}$ while t and $\varphi_{0,0,\mu}$ commute. Therefore, up to conjugacy, $G = \Sigma_p \rtimes \Sigma_d$ with $\Sigma_p = \langle s \rangle$ and $s = \varphi_{0,0,1}$ whereas Σ_d and t are as before. Since Σ_p is a normal subgroup of G , there exists i with $1 \leq i \leq p-1$

such that $st = ts^i$. A straightforward computation shows that this occurs if and only if $i = 1/\lambda^{q+1}$. For $d|(q+1)$, this implies $i = 1$, thus G is cyclic and Case (I) occurs. For $d|(q-1)$, we have $i \neq 1$ and hence G is not abelian. From Result 3.5, $d|(p-1)$. Thus Case (II) occurs. If $s \notin Z(S_p)$ then $s = \varphi_{a,b,1}$. For $\mu = a^{-1}$, the conjugate of s by $\varphi_{0,0,\mu}$ is $\varphi_{1,b/a^{q+1},1}$ while t and $\varphi_{0,0,\mu}$ commute. Therefore, up to conjugacy, we may assume $G = \Sigma_p \rtimes \Sigma_d$ where $\Sigma_p = \langle s \rangle$ and $s = \varphi_{1,b/a^{q+1},1}$ while Σ_d and t are not changed. Then $st = \phi_{1,b/a^{q+1},\lambda}$ and, from (1.5),

$$ts^i = \phi_{\lambda i, \lambda^{q+1}(\omega(i^2-i)/2+ib/a^{q+1}), \lambda}.$$

Therefore, $st = ts^i$ if and only if $\lambda i = 1$ and $\lambda^{q+1}(\frac{1}{2}\omega(i^2-i)+ib/a^{q+1}) = b/a^{q+1}$. The latter condition can also be written as

$$\frac{1}{2}\omega(i^2-i) = (i^2-i)b/a^{q+1},$$

that is, $b = \frac{1}{2}\omega a^{q+1}$ as $\lambda \neq 1$. Therefore, $st = ts^i$ if and only if $s = \varphi_{1,\omega/2,1}$ and $i\lambda = 1$. In particular, G is not abelian, and $d|(p-1)$. This gives Case (III).

Case $p < d$

In this case, a Sylow d -subgroup Σ_d of G is a normal subgroup of G , and hence Σ_d is the unique d -subgroup of G . As d divides the order of $\text{PGU}(3, q)$, either $d|(q-1)$, or $d|(q+1)$, or $d|(q^2-q+1)$. Assume that Σ_d fixes a point on $\mathcal{H}_q(\mathbb{F}_{q^2})$. Then Σ_d has at least two fixed points, as $|\mathcal{H}_q(\mathbb{F}_{q^2})| - 1$ equals q^3 . Up to conjugacy, we may assume that Σ_d fixes Y_∞ and O . Then $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$ with $\lambda^d = 1$. If $\lambda^{q+1} \neq 1$ then Σ_d has no any further fixed point, and hence G preserves the pair $\{Y_\infty, O\}$. Since $p > 2$ this yields that elements of G of order p fix two points on $\mathcal{H}_q(\mathbb{F}_{q^2})$ which is not possible. Therefore, $\lambda^{q+1} = 1$ and $d|(q+1)$. This implies that Σ_d fixes all points $P = (0, \eta)$ with $\eta^q - \eta = 0$, i.e. with $\eta \in \mathbb{F}_q$. Since Σ_d is a normal subgroup of G , this yields that a generator s of Σ_p takes O to a point $P = (0, \eta)$ with $\eta \in \mathbb{F}_q$. But then $s = \varphi_{0,b,1}$ with $b \in \mathbb{F}_q^*$. For $\mu = b^{-1}$, the conjugate of s by $\varphi_{0,0,\mu}$ with $\mu^{q+1} = 1$ is $\varphi_{0,1,1}$ while a generator t of Σ_d and $\varphi_{0,0,\mu}$ commute. Therefore, up to conjugacy, we may assume $s = \varphi_{0,1,1}$. Also, $st = ts$ and Case (I) occurs. We are left with the case where Σ_d fixes no point on $\mathcal{H}_q(\mathbb{F}_{q^2})$. Then either $d|(q+1)$, or $d|(q^2-q+1)$. We look at the action of $\text{PGU}(3, q)$ as a projective group of the plane $\text{PG}(2, \mathbb{K})$ where $\mathbb{K}$ is an algebraic closure of $\mathbb{F}_{q^2}$. Then the Hermitian curve $\mathcal{H}_q$ is left invariant by $\text{PGU}(3, q)$. In particular, $\text{PGU}(3, q)$ preserves both $\mathcal{H}_q(\mathbb{F}_{q^2})$ and its complementary set in $\text{PG}(2, \mathbb{F}_{q^2})$ whose size equals

$$q^4 + q^2 + 1 - (q^3 + 1) = q^2(q^2 - q + 1).$$

Furthermore, $\mathcal{H}_q(\mathbb{F}_{q^2})$ can also be viewed as the set of all isotropic points of a unitary polarity π of $\text{PG}(2, \mathbb{F}_{q^2})$. If $d|(q+1)$ then Σ_d fixes a point $R \in \text{PG}(2, \mathbb{F}_{q^2})$ outside $\mathcal{H}_q(\mathbb{F}_{q^2})$.

Let r be the polar line of R w.r.t. π . Then r is a chord of $\mathcal{H}_q(\mathbb{F}_{q^2})$. Since r has as many as $q(q-1)$ points other than those on $\mathcal{H}_q(\mathbb{F}_{q^2})$, there are at least two fixed points on r outside $\mathcal{H}_q(\mathbb{F}_{q^2})$ under the action of Σ_d . Since Σ_d does not fix r pointwise, these two points, say R_1, R_2 are the only fixed points of Σ_d on r . In particular, Σ_d fixes the vertices of the triangle RR_1R_2 .

We show that no more point in $\text{PG}(2, \mathbb{F}_{q^2})$ is fixed by Σ_d . In fact, such a further fixed point T of Σ_d should lie on a side of the triangle, and that side would be fixed pointwise by Σ_d . But this is impossible in our case, since the sides of RR_1R_2 are chords of $\mathcal{H}_q(\mathbb{F}_{q^2})$ whereas Σ_d is supposed not to fix points on $\mathcal{H}_q(\mathbb{F}_{q^2})$. Since Σ_d is a normal subgroup of G , the triangle RR_1R_2 is left invariant by G . But then G is contained in a maximal subgroup of $\text{PGU}(3, q)$ whose order equals $6(q+1)^2$. By the Lagrange theorem $pd = |G|$ divides $6(q+1)^2$. Since $p > 3$ and $p \nmid (q+1)$, this is impossible.

A similar geometric approach is used to rule out the other possibility, i.e. $d|(q^2 - q + 1)$. Look at the action of $\text{PGU}(3, q)$ on $\text{PG}(2, \mathbb{F}_{q^6})$. From

$$|\mathcal{H}_q(\mathbb{F}_{q^6})| = q^6 + 1 + q^4(q-1) \quad \text{and} \quad |\mathcal{H}_q(\mathbb{F}_{q^3})| = q^3 + 1,$$

the Hermitian curve $\mathcal{H}_q$ has as many as $q^3(q+1)^2(q-1)$ points in $\text{PG}(2, \mathbb{F}_{q^6})$ but not in $\text{PG}(2, \mathbb{F}_{q^2})$. From $d|(q^2 - q + 1)$ and $d > 3$, Σ_d fixes a point $R \in \mathcal{H}_q(\mathbb{F}_{q^6})$ not lying in $\text{PG}(2, \mathbb{F}_{q^2})$. The Frobenius collineation $\mathfrak{f}$ which sends the point $P = (a_1 : a_2 : a_3)$ to the point

$$P_{q^2} = (a_1^{q^2} : a_2^{q^2} : a_3^{q^2})$$

leaves $\mathcal{H}_q(\mathbb{F}_{q^6})$ invariant. Since $\mathfrak{f}$ and Σ_d commute, Σ_d also fixes the points R_{q^2} and R_{q^3} . Actually, Σ_d does not fix another point, otherwise one of the sides, say ℓ , of the triangle $RR_{q^2}R_{q^4}$ would be fixed by Σ_d pointwise. Since $\mathfrak{f}$ takes ℓ to another side r of $RR_{q^2}R_{q^4}$ and $\mathfrak{f}$ and Σ_d commute, this would yield that r is also fixed pointwise by Σ_d , which is impossible. As before, this implies that G leaves the triangle $RR_{q^2}R_{q^4}$ invariant. Therefore G is contained in a maximal subgroup of $\text{PGU}(3, q)$ whose order equals $3(q^2 - q + 1)$. Arguing as before, the Lagrange theorem yields that this is impossible. $\square$

Result 3.7. [32, Theorem 5.74] *Let H be a subgroup of $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$ of order p . The Galois subcover $\mathbb{F}_{q^2}(\mathcal{F}')$ of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to H is $\mathbb{F}_{q^2}$ -isomorphic to the function field $\mathbb{F}_{q^2}(\xi, \eta)$ where either (I) or (II) hold:*

- (I) $\sum_{i=1}^h \eta^{q/p^i} + \omega \xi^{q+1} = 0$ with $\omega^{q-1} = -1$, $\mathfrak{g}(\mathbb{F}_{q^2}(\mathcal{F}')) = \frac{1}{2}q \left(\frac{q}{p} - 1\right)$, and H is in the center of a Sylow p -subgroup of $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$;
- (II) $\eta^q + \eta - (\sum_{i=1}^h \xi^{q/p^i})^2 = 0$ for $p > 2$, $\mathfrak{g}(\mathbb{F}_{q^2}(\mathcal{F}')) = \frac{1}{2}\frac{q}{p}(q-1)$, and H is not in the center of a Sylow p -subgroup of $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$.

The following result is a corollary of [23, Section 4].

Result 3.8. *Let $\mathfrak{g}$ be the genus of the Galois cover of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to a subgroup G of $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}_q))$ of order dp . Let S_p be a Sylow p -subgroup of $\text{Aut}(\mathbb{F}_{q^2}(\mathcal{H}))$ containing a subgroup H of G of order p . Then either*

$$\mathfrak{g} = \frac{1}{2} \frac{q}{d} \left(\frac{q}{p} - 1 \right) \quad \text{for} \quad (d, q+1) = 1,$$

or

$$\mathfrak{g} = \frac{1}{2d}(q-d+1) \left(\frac{q}{p} - 1 \right) \quad \text{for} \quad (d, q+1) = d.$$

3.2 Galois subcovers of $\mathbb{F}_{q^2}(\mathcal{H})$ of type (I) of Theorem (3.6)

As in Remark 1.129, take $\mathbb{F}_{q^2}(\mathcal{H}_q)$ in its canonical form $\mathbb{F}_{q^2}(x, y)$ with $y^q - y + \omega x^{q+1} = 0$ and $\omega^{q-1} = -1$. The group $\Phi = \langle \varphi_{0,1,1} \rangle$ has order p , and it is contained in $Z(S_p)$. Let $\eta = y^p - y$ and $\xi = x$. Then $\varphi_{0,1,1}(\eta) = \varphi_{0,1,1}(y^p - y) = \varphi_{0,1,1}(y)^p - \varphi_{0,1,1}(y) = (y+1)^p - (y+1) = y^p - y = \eta$. Moreover, $y^q - y = \text{Tr}(\eta)$. Since $\varphi_{0,1,1}$ fixes ξ , this shows that the Galois subcover $\mathbb{F}_{q^2}(\mathcal{F}')$ of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to Φ is as in (i) of Result 3.7. That equation can also be written as

$$\sum_{i=0}^{h-1} \eta^{p^i} + \omega \xi^{q+1} = 0. \quad (3.4)$$

Take an element $r \in \mathbb{F}_{q^2}$ with $r^d = 1$. Then $\varphi_{0,0,r}$ commutes with $\varphi_{0,1,1}$. Therefore, if $d|(q+1)$ then $\varphi_{0,0,r}$ induces an automorphism φ of $\mathbb{F}_{q^2}(\mathcal{F}')$. More precisely, a straightforward computation shows that φ is the map $\varphi : (\xi, \eta) \mapsto (r\xi, \eta)$. Let Φ_r be the $\mathbb{F}_q$ -automorphism group of $\mathbb{F}_{q^2}(\mathcal{F}')$ generated by φ . Then the Galois subcover of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to G of Result (3.6) of type (I) is the same as the Galois subcover G_r of $\mathbb{F}_{q^2}(\mathcal{F}')$ with respect to Φ_r .

Theorem 3.9. *The Galois subcover $G_r = \mathbb{F}_{q^2}(\zeta, \tau)$ of $\mathbb{F}_{q^2}(\mathcal{F}')$ with respect to Φ_r has genus*

$$\mathfrak{g} = \frac{1}{2d}(q - d + 1)\left(\frac{q}{p} - 1\right)$$

and is given by

$$\sum_{i=0}^{h-1} \tau^{p^i} + \omega \zeta^{q+1/d} = 0, \quad d \mid (q+1). \quad (3.5)$$

Proof. We show first that the fixed field F of Φ_r is generated by $\tau = \eta$ together with

$$\zeta = \xi^d. \quad (3.6)$$

Since $\varphi(\tau) = \tau$ and

$$\varphi(\zeta) = \varphi(\xi^d) = \varphi(\xi)^d = r^d \xi^d = \xi^d = \zeta,$$

we have $\mathbb{F}_{q^2}(\zeta, \tau) \subseteq F$. Furthermore, $[\mathbb{F}_{q^2}(\mathcal{F}') : \mathbb{F}_{q^2}(\zeta, \tau)] = d$. Since d is prime, this yields either $\mathbb{F}_{q^2}(\zeta, \tau) = F$ or $F = \mathbb{F}_{q^2}(\mathcal{F}')$. The latter case cannot actually occur, and hence $F = \mathbb{F}_{q^2}(\zeta, \tau)$. Therefore $F = G_r$. Now, eliminate ξ from Equations (3.4) and (3.6). Since d divides $q+1$, replacing ξ^{q+1} with $(\xi^{q+1/d})^d$ and $\tau = \eta$ in (3.4) gives equation in (3.5). The formula for the genus follows from [32, Lemma 12.1(iii)(b)]. $\square$

3.3 Galois subcovers of $\mathbb{F}_{q^2}(\mathcal{H})$ of type (II) of Theorem (3.6)

We keep our notation up from Section 3.2. Assume that d divides $p-1$, and take $r \in \mathbb{F}_p^*$ with $r^d = 1$. Then $\varphi_{0,0,r}^{-1} \circ \varphi_{0,1,1} \circ \varphi_{0,0,r} = \varphi_{0,r^2,1} \in \langle \varphi_{0,1,1} \rangle$, and hence $\varphi_{0,0,r}$ induces an automorphism φ of $\mathbb{F}_{q^2}(\mathcal{F}')$. Here, φ is the map $\varphi : (\xi, \eta) \mapsto (r\xi, r^2\eta)$. Let Φ_r be the $\mathbb{F}_q$ -automorphism group of $\mathbb{F}_{q^2}(\mathcal{F}')$ generated by φ . Then the Galois subcover of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to G of Result (3.6) of type (II) is the Galois subcover G_r of $\mathbb{F}_{q^2}(\mathcal{F}')$ with respect to Φ_r .

Theorem 3.10. *The Galois subcover $G_r = \mathbb{F}_{q^2}(\epsilon, \rho)$ of $\mathbb{F}_{q^2}(\mathcal{F}')$ with respect to Φ_r has equation*

$$\omega \epsilon^{(q-1)/d} - A(\epsilon, \rho) = 0, \quad d \mid (p-1) \quad (3.7)$$

where

$$A(\epsilon, \rho) = \rho + \epsilon^{2(p-1)/d} \rho^p + \cdots + \epsilon^{2(p^{h-1}-1)/d} \rho^{q/p}.$$

Proof. We show first that the fixed field F of Φ_r is generated by

$$\epsilon = \xi^d \quad (3.8)$$

together with

$$\rho = \frac{\eta}{\xi^2}. \quad (3.9)$$

Since

$$\varphi(\epsilon) = \varphi(\xi^d) = \varphi(\xi)^d = r^d \xi^d = \xi^d = \epsilon$$

and

$$\varphi(\rho) = \frac{\varphi(\eta)}{\varphi(\xi^2)} = \frac{\varphi(\eta)}{\varphi(\xi)^2} = \frac{r^2 \eta}{r^2 \xi^2} = \frac{\eta}{\xi^2} = \rho,$$

we have $\mathbb{F}_{q^2}(\epsilon, \rho) \subseteq F$. Furthermore, $[\mathbb{F}_{q^2}(\mathcal{F}') : \mathbb{F}_{q^2}(\epsilon, \rho)] = d$. Since d is prime, this yields either $\mathbb{F}_{q^2}(\epsilon, \rho) = F$ or $F = \mathbb{F}_{q^2}(\mathcal{F}')$. The latter case cannot actually occur, and hence $F = \mathbb{F}_{q^2}(\epsilon, \rho)$. Therefore $F = G_r$. We have to eliminate ξ and η from equations (3.4), (3.8) and (3.9). From (3.9) we have $\eta = \rho \xi^2$ then $Tr(\eta) = Tr(\rho \xi^2)$. This yields that

$$Tr(\eta) = \xi^2 \rho + \xi^{2p} \rho^p + \cdots + \xi^{2q/p} \rho^{q/p}, \quad (3.10)$$

whence

$$Tr(\eta) = \xi^2 \left(\rho + \xi^{2(p-1)} \rho^p + \cdots + \xi^{2(q/p-1)} \rho^{q/p} \right). \quad (3.11)$$

Since d divides $p-1$, $Tr(\eta)$ in (3.10) can also be written as

$$Tr(\eta) = \xi^2 \left(\rho + (\xi^d)^{2(p-1)/d} \rho^p + \cdots + (\xi^d)^{2(p^{h-1}-1)/d} \rho^{q/p} \right). \quad (3.12)$$

Therefore

$$Tr(\eta) = \xi^2 \left(\rho + \epsilon^{2(p-1)/d} \rho^p + \cdots + \epsilon^{2(p^{h-1}-1)/d} \rho^{q/p} \right) = \xi^2 A(\epsilon, \rho). \quad (3.13)$$

This, together with (3.4), give

$$\omega \xi^{q+1} = \xi^2 A(\epsilon, \eta). \quad (3.14)$$

Since $d \mid (p-1)$ the number $\frac{q-1}{d}$ is an integer. Thus Equation (3.7) follows from (3.14). $\square$

3.4 Galois subcovers of $\mathbb{F}_{q^2}(\mathcal{H})$ of type (III) of Theorem (3.6)

This time, take $\mathbb{F}_{q^2}(\mathcal{H}_q)$ in its canonical form $\mathbb{F}_{q^2}(x, y)$ with $y^q + y - x^{q+1} = 0$. The group $\Psi = \langle \psi_{1,1/2,1} \rangle$ has order p , and it is not contained in $Z(S_p)$. Let $\xi = x^p - x$ and $\eta = y - \frac{1}{2}x^2$. A straightforward computation shows that $\psi_{1,1/2,1}(\xi) = \xi$ and $\psi_{1,1/2,1}(\eta) = \eta$. Moreover,

$$y^q + y - x^{q+1} = \eta^q + \frac{1}{2}x^{2q} + \eta + \frac{1}{2}x^2 - x^{q+1} = \eta^q + \eta + \frac{1}{2}x^{2q} + \frac{1}{2}x^2 - x^{q+1} = \eta^q + \eta + \frac{1}{2}(x^q - x)^2.$$

Since $Tr(\xi) = x^q - x$, this gives

$$\eta^q + \eta + \frac{1}{2}(x^q - x)^2 = \eta^q + \eta + \frac{1}{2}Tr(\xi)^2.$$

Therefore, the Galois subcover $\mathbb{F}_{q^2}(\mathcal{F}')$ of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to Ψ is $\mathbb{F}_{q^2}(\xi, \eta)$ with

$$\eta^q + \eta + \frac{1}{2} \left(\sum_{i=1}^h \xi^{p^{i-1}} \right)^2 = 0.$$

Replacing η by $-\frac{1}{2}\eta$ this equation becomes

$$\eta^q + \eta - \left(\sum_{i=1}^h \xi^{p^{i-1}} \right)^2 = 0. \quad (3.15)$$

In particular, $\mathbb{F}_{q^2}(\mathcal{F}')$ is the same as (II) of Result 3.7. Assume that d divides $p - 1$, and take $r \in \mathbb{F}_p^*$ with $r^d = 1$. Then $\psi_{0,0,r}^{-1} \circ \psi_{1,1/2,1} \circ \psi_{0,0,r} = \varphi_{r,1/2r^2,1} \in \langle \varphi_{1,1/2,1} \rangle$, and hence $\varphi_{0,0,r}$ induces an automorphism φ of $\mathbb{F}_{q^2}(\mathcal{F}')$. Moreover, ψ is the map $\psi : (\xi, \eta) \mapsto (r\xi, r^2\eta)$. Let Ψ_r be the $\mathbb{F}_q$ -automorphism group of $\mathbb{F}_{q^2}(\mathcal{F}')$ generated by ψ . Then the Galois subcover of $\mathbb{F}_{q^2}(\mathcal{H}_q)$ with respect to G of Result (3.6) of type (III) is the Galois subcover G_r of $\mathbb{F}_{q^2}(\mathcal{F}')$ with respect to Ψ_r .

Theorem 3.11. *The Galois subcover $G_r = \mathbb{F}_{q^2}(\iota, \nu)$ of $\mathbb{F}_{q^2}(\mathcal{F}')$ with respect to Ψ_r has genus*

$$\mathfrak{g} = \frac{q}{2dp}(q - 1)$$

and is given by

$$\left(\frac{\tau^2}{\iota^d} \right)^{(q-1)/d} + 1 - A(\iota, \tau) = 0 \quad (3.16)$$

where

$$A(\iota, \tau) = \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} \left(\frac{\tau^2}{\iota^d} \right)^{(p^i-1)/2d} \left(\frac{\tau^2}{\iota^d} \right)^{(p^j-1)/2d} \iota^{(p^i+p^j)/2}.$$

Proof. We show first that the fixed field F of Ψ_r is generated by

$$\nu = \eta^d, \quad (3.17)$$

together with

$$\iota = \frac{\xi^2}{\eta}, \quad (3.18)$$

and

$$\tau = \xi^d. \quad (3.19)$$

Since

$$\varphi(\nu) = \varphi(\eta)^d = r^{2d}\eta^d = \eta^d = \nu, \quad \varphi(\tau) = \varphi(\xi)^d = r^d\xi^d = \xi^d = \tau$$

and

$$\varphi(\iota) = \varphi\left(\frac{\xi^2}{\eta}\right) = \frac{\varphi(\xi^2)}{\varphi(\eta)} = \frac{\varphi(\xi)^2}{\varphi(\eta)} = \frac{(r\xi)^2}{r^2\eta} = \frac{r^2\xi^2}{r^2\eta} = \frac{\xi^2}{\eta},$$

we have $\mathbb{F}_{q^2}(\iota, \nu, \tau) \subseteq F$. Furthermore, $[\mathbb{F}_{q^2}(\iota, \nu, \tau)(\xi) : \mathbb{F}_{q^2}(\iota, \nu, \tau)] = d$ and $\eta \in \mathbb{F}_{q^2}(\iota, \nu, \tau)(\xi)$. Therefore, $[\mathbb{F}_{q^2}(\mathcal{F}') : \mathbb{F}_{q^2}(\iota, \nu, \tau)] \leq d$. Since d is prime, this yields either $\mathbb{F}_{q^2}(\iota, \mu, \nu) = F$ or $F = \mathbb{F}_{q^2}(\mathcal{F}')$. The latter case cannot actually occur, and hence $F = \mathbb{F}_{q^2}(\iota, \mu, \nu)$. Therefore $F = G_r$. We go on by eliminating ξ and η from Equations (3.15), (3.17), (3.18) and (3.19). From the definition of the trace of ξ , $Tr(\xi)^2 = (\xi + \dots + \xi^{q/p})^2$. By a straightforward computation,

$$Tr(\xi)^2 = \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} \xi^{p^i+p^j}.$$

This can also be written as

$$Tr(\xi)^2 = \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} (\xi^2)^{(p^i+p^j)/2}. \quad (3.20)$$

From (3.18), $\xi^2 = \eta\iota$. Therefore, in (3.20) the square trace of ξ is equal to

$$\sum_{i=0}^{h-1} \sum_{j=0}^{h-1} (\eta\iota)^{(p^i+p^j)/2}. \quad (3.21)$$

Since $\frac{1}{2}(p^i + p^j) - 1 = \frac{1}{2}(p^i - 1) + \frac{1}{2}(p^j - 1)$, the sum in (3.21) turns out to be equal to

$$\eta \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} \eta^{(p^i-1)/2} \eta^{(p^j-1)/2} \iota^{(p^i+p^j)/2}. \quad (3.22)$$

As d and 2 divide both $p^i - 1$ and $p^j - 1$, the sum in (3.21) equals

$$\eta \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} (\eta^d)^{(p^i-1)/2d} (\eta^d)^{(p^j-1)/2d} \iota^{(p^i+p^j)/2} \quad (3.23)$$

and by replacing η^d with ν we obtain

$$\eta \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} \nu^{(p^i-1)/2d} \nu^{(p^j-1)/2d} \iota^{(p^i+p^j)/2} \quad (3.24)$$

Let

$$A(\iota, \nu) = \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} \nu^{(p^i+p^j-2)/2d} \iota^{(p^i+p^j)/2}. \quad (3.25)$$

Therefore, $\eta^q + \eta = \eta A(\iota, \nu)$, and dividing both sides by η gives $\eta^{q-1} + 1 = A(\iota, \nu)$. Since d divides $q - 1$, replacing η^d by ν shows

$$\nu^{(q-1)/d} + 1 - A(\iota, \nu) = 0. \quad (3.26)$$

From (3.17), (3.18), and (3.19), $\nu = \frac{\tau^2}{\iota^d}$. Now the claim follows from (3.26). $\square$

3.5 Weierstrass semigroups and application to AG-codes

We compute the Weierstrass semigroup at the unique place centred at the point at infinity of some of the maximal curves considered in the present chapter.

Proposition 3.12. *Let P_∞ be the unique point at infinity of the following two curves*

$$\begin{aligned} \sum_{i=1}^h Y^{q/p^i} + \omega X^{q+1} &= 0, & \omega^{q-1} &= -1, h \geq 2; \\ \sum_{i=1}^h Y^{q/p^i} + \omega X^{(q+1)/d} &= 0, & \omega^{q-1} &= -1, d \mid (q+1). \end{aligned} \quad (3.27)$$

Then the Weierstrass semigroup at P_∞ is generated by $\frac{q}{p}$, and $q+1$, respectively by $\frac{q}{p}$, and $\frac{q+1}{d}$.

Proof. For the first equation the claim follows from the remark after the proof of Lemma 12.2 in [32] applied for $n = h - 1$ and $m = q + 1$. For the second equation the claim follows from the remark after the proof of Lemma 12.2 in [32] applied for $n = h - 1$ and $m = \frac{q+1}{d}$. $\square$

Let S be a numerical semigroup. The gaps of S are the elements in $\mathbb{N} \setminus S$. The number $g(S)$ of gaps of S is the *genus* of S . If S is the Weierstrass semigroup of a curve at a point then $g(S)$ coincides with the genus of the curve. Let $(a_1, \dots, a_k)$ be a sequence of positive integers such that their greatest common divisor is 1. Let $d_0 = 0$, $d_i = \text{g.c.d.}(a_1, \dots, a_i)$ and $A_i = \left\{ \frac{a_1}{d_i}, \dots, \frac{a_i}{d_i} \right\}$ for $i = 1, \dots, k$. Let S_i be the semigroup generated by A_i . The sequence $(a_1, \dots, a_k)$ is called *telescopic* whenever $\frac{a_i}{d_i} \in S_{i-1}$ for $i = 2, \dots, k$. A *telescopic semigroup* is a numerical semigroup generated by a telescopic sequence.

Result 3.13. [38, Lemma 6.5] *For the semigroup generated by a telescopic sequence $(a_1, \dots, a_k)$, let*

$$l_g(S_k) := \sum_{i=1}^k \left(\frac{d_{i-1}}{d_i} - 1 \right) a_i \quad \text{then} \quad g(S_k) = \frac{l_g(S_k) + 1}{2}.$$

Theorem 3.14. *Let P_∞ be the unique point of infinity of the curves $\bar{\mathcal{H}}_q$ in Theorem 3.1. Then the Weierstrass semigroup $H(P_\infty)$ has the following properties:*

- (I) $H(P_\infty) = \langle \frac{q}{p}, q + 1 \rangle$, for the curve of Equation (I);
- (II) $\frac{q}{p}, \frac{q-1}{d} \in H(P_\infty)$, for the curve of Equation (II);
- (III) $\frac{2(q-1)}{d}, q - 1 \in H(P_\infty)$, for the curve of Equation (III).

Proof. Case (i). The pole numbers of x and y at P_∞ are q and $2q/p$, respectively. Since the curve is $\mathbb{F}_{q^2}$ -maximal and P_∞ is an $\mathbb{F}_{q^2}$ -rational point, $q + 1 \in H(P_\infty)$; see [32, Theorem 10.6]. Let $d_0 = 0$, $d_1 = 2\frac{q}{p}$, $d_2 = \frac{2}{q}$ and $d_3 = 1$, and $A_1 = \{1\}$, $A_2 = \{2, p\}$, $A_3 = \{2\frac{q}{p}, q, q + 1\}$. Then $p \in S_1$ and $q + 1 \in S_2$. Thus the sequence $\{2\frac{q}{p}, q, q + 1\}$ is telescopic. Furthermore,

$$l_g(S_3) = -\frac{2q}{p} + q + \left(\frac{q}{p} - 1 \right) (q + 1) = \frac{q^2}{p} - \frac{q}{p} - 1,$$

whence the claim follows by Result (3.13).

Case (ii). From Equation (II), $[\mathbb{F}_{q^2}(\bar{\mathcal{H}}_q) : \mathbb{F}_{q^2}(x)] = \frac{q}{p}$ and $[\mathbb{F}_{q^2}(\bar{\mathcal{H}}_q) : \mathbb{F}_{q^2}(y)] = \frac{q-1}{d}$. Therefore, $\frac{q}{p}$ and $\frac{q-1}{d}$ are non-gaps at P_∞ .

Case (iii). The above argument applied to the curve $\bar{\mathcal{H}}_q$ of Equation (III), shows that $\frac{q-1}{d}$ and $\frac{q}{p}$ are non-gaps of G_r at P_∞ . $\square$

Let C denotes any $\mathbb{F}_{q^2}$ -maximal curve equipped with an $\mathbb{F}_{q^2}$ -rational point P . Let D be a set of $\mathbb{F}_{q^2}$ -rational points of C other than P . From previous work by Janwa [37] and García-Kim-Lax [20], if the divisor G is taken as multiple of P then knowledge of the gaps at P_∞ may allow one to show that the minimum distance of the resulting evaluation code $C_L(G, D)$ or differential code $C_\Omega(G, D)$ may be better than the designed minimum distance of that code. In particular, it is shown in [21] that t consecutive gaps at P (under some conditions on the order sequence at P) gives a minimum distance d of the code at least t greater than the designed minimum distance. This motivates to investigate large intervals of gaps at the point P_∞ of the $\mathbb{F}_{q^2}$ -maximal curves considered in the present chapter. Here we limit ourselves to show a couple of experimental results. We use Janwa's result as stated in [21, Theorem 2] together with [21, Theorem 3] for the zero divisor $B = 0$.

Example 3.15. Take the curve of equation (3.1) for $\mathcal{C}$, and let $p = 7, d = 5, h = 2$. Then $d \mid (q + 1) = 7^2 + 1$. From Proposition 3.12, the non-gaps at P_∞ are $q/p = 7$ and $(q + 1)/d = 10$. The gap sequence at P_∞ is 1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 13, 15, 16, 18, 19, 22, 23, 25, 26, 29, 32, 33, 36, 39, 43, 46, 53. Each of the integers $11 = \gamma - 2 = \gamma - t$, $12 = \gamma - 1$ and $13 = \gamma$ is a gap at P_∞ . From [21, Theorem 3], the minimum distance of the code $C_L(\gamma P_\infty, D)$ is at least $d^* = |D| - \gamma + t + 1 = 5037$ whereas the designed minimum distance is $d' = |D| - \gamma = 5034$, so we have an $[n, k, d^*] = [5047, 3, 5037]$ - code.

Example 3.16. Take the curve of equation (3.1) for $\mathcal{C}$, and let $p = 5, d = 3, h = 3$. Then $d \mid (q + 1) = 5^3 + 1$. From Proposition 3.12, the non-gaps at P_∞ are $q/p = 25$ and $(q + 1)/d = 42$. The gap sequence at P_∞ is 1, ..., 24, 26, ..., 41, 43, ..., 66, 68, ..., 920, 922, ..., 962, 964, ..., 981, 983. Each of the integers $1022 = \alpha, \dots, 1030 = \alpha + 8 = \alpha + t$ and $1072 = \beta, \dots, 1063 = \beta - t = \beta - (t - 1)$ is a gap at P_∞ . From [21, Theorem 4], the minimum distance of the differential code $C_\Omega(\gamma P_\infty, D)$ with $\gamma = \alpha + \beta - 1$ is at least $d^* = \alpha + \beta - 1 - (2g - 2) + (t + 1) = 1120$ whereas the designed minimum distance is $d' = \alpha + \beta - 1 - (2g - 2) = 1112$, so we have an $[n, k, d^*] = [138625, 1593, 1120]$ - code.

It may be noticed that the curve of equation (3.1) is a C_{ab} -curve with $a = q/p$ and $b = (q + 1)/d$. Evaluation codes defined over a C_{ab} -curve have been the subject of recent papers where both encoding and decoding problems are also treated; see [4].

Bibliography

- [1] N. Anbar, D. Bartoli, S. Fanali and M. Giulietti, *On the size of the automorphism group of a plane algebraic curve*, Journal of Pure and Applied Algebra 217 (2013), 1224-1236.
- [2] N. Anbar and B. Gunes, *On nilpotent automorphism groups of function fields*, Advances in Geometry 22 (2022), 1, 69-78.
- [3] N. Arakelian and P. Speziali, *Algebraic curves with automorphism groups of large prime order*, Mathematische Zeitschrift 299 (2021), 2005-2028.
- [4] P. Beelen, J. Rosenkilde and G. Solomatov, *Fast decoding of AG codes*, IEEE Trans. Inform. Theory 68 (2022), 7215-7232.
- [5] A. Broughton, T. Shaska and A. Wootton, *On automorphisms of algebraic curves*, Contemporary Mathematics 724 (2019), 175-212.
- [6] M. Bonini, A. Dionigi, F. Ghiandoni, *On QC and GQC Algebraic-Geometric codes* (In preparation).
- [7] E. Bujalance, F.J. Cirre, J. M. Gamboa and G. Gromadzki, *On compact Riemann surfaces with dihedral groups of automorphisms*, Mathematical Proceedings of the Cambridge Philosophical Society, 2003; 134(3), 465-477.
- [8] B. P. Chetiya, *On genuses of compact Riemann surfaces admitting solvable automorphism groups*, Indian J. Pure Appl. Math 12(11) (1981), 1312-1318.
- [9] K. Conrad, *Dihedral Groups II*, <https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral2.pdf> (accessed 12 april 2025).

- [10] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra 28 (2000), 4707–4728.
- [11] D.A. Cox, *Galois Theory*, John Wiley and Sons, 2012.
- [12] K. Csiszter and M. Domokos, *The Noether number for the groups with a cyclic subgroup of index two*, Journal of Algebra 399 (2014) 546–560.
- [13] L.E. Dickson, *Linear Groups, with an Exposition of the Galois Field Theory*, Teubner, Leipzig, (1901).
- [14] Y. Ding and H. Tong, *Quasi-cyclic NMDS codes*, Finite Fields and Their Applications 24 45-54, 2013.
- [15] A. Dionigi, B. Gatti, *Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order dp with $d \neq p$ prime*, Designs, Codes and Cryptography 93, pp 2647-2670, 2025
- [16] A. Dionigi, M. Giulietti and M. Timpanella *Curves with a large automorphism group admitting a cyclic subgroup of index 2* (In preparation).
- [17] A. Dionigi, M. Giulietti and M. Timpanella, *Algebraic curves with a large cyclic automorphism group*, arXiv:2410.13590 (Accepted by Journal of Algebra).
- [18] W. Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, (1989).
- [19] B. Gatti and G. Korchmáros, *Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order p^2* , arXiv:2307.15192, (2023).
- [20] A. Garcia and R.F. Lax, *Goppa codes and Weierstrass gaps*, Coding Theory and Algebraic Geometry, Proceedings, Luminy, (1991), Lecture Notes in Mathematics, 1518 (Springer, Berlin), (1992), 33-42.
- [21] A. Garcia, S. J. Kim and R. F. Lax, *Consecutive Weierstrass gaps and minimum distance of Goppa codes*, J. Pure Appl. Algebra 84 (1993), 199-207.

BIBLIOGRAPHY

- [22] A. Garcia and H. Stichtenoth *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bull.Braz. Math. Soc. (N.S.) 37, 1, pp. 139-152, 2006.
- [23] A. García, H. Stichtenoth and C.P. Xing, *On Subfields of the Hermitian Function Field*, Comp. Math 120 (2000), 137-170.
- [24] A. Garcia and S. Tafazolian, *Certain maximal curves and Cartier operators*, Acta Arith:235(3)199–218, 2008.
- [25] M. Giulietti and G. Korchmáros, *Large 3-groups of automorphisms of algebraic curves in characteristic 3*, arXiv:1312.5108, (2013).
- [26] M. Giulietti and G. Korchmáros, *Algebraic curves with many automorphisms*, Advances in Mathematics 349 (2019), 162–211.
- [27] G. Gromadzki, *Maximal groups of automorphisms of compact Riemann surfaces in various classes of finite groups*, Rev. R. Acad. Sc. Madrid 82, 1988, pp 267–276.
- [28] D. Harbater, A. Obus, R. Pries and K. Stevenson, *Abhyankar’s conjectures in Galois theory: current status and future directions*, Bull. Amer. Math. Soc. 55, 2018, 239-287.
- [29] H. W. Henn, *Funktionenkorper mit grosser Automorphismengruppe*, J. Reine Angew. Math. 302 (1978), 96-115.
- [30] I. N. Herstein, *Algebra*, Editori Riuniti, 1989.
- [31] R. A. Hidalgo, Y. L. Marín Montilla and S. Quispe, *Generalized quasi-dihedral group as automorphism group of Riemann Surfaces*, preprint arxiv.org/pdf/2210.01577.
- [32] J.W.P Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves Over a Finite Field*, Princeton Univ. Press, Princeton and Oxford, (2008).
- [33] A.R. Hoffer, *On unitary collineation groups*, J. Algebra 22 (1972), 211–218.
- [34] M. Homma, *Automorphisms of prime order of curves*, Manuscripta Math. 33 (1980/81), 1, 99-109.

- [35] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften 134, Springer, Berlin, 1967, xii+793 pp.
- [36] S. Irokawa and R. Sasaki, *On a family of quotients of Fermat curves*, Tsukuba Journal of Mathematics 19 (1995), 121-139.
- [37] H. Janwa, *On the parameters of algebraic geometric codes*, in Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991), 19–28, Lecture Notes in Comput. Sci., 539, Springer, Berlin, 1991.
- [38] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Information Theory, 41 (1995), 1720-1732.
- [39] S. Kondo, T. Katagiri and T. Ogihara, *Automorphism groups of one-point codes from the curves $y^q + y = x^{q^r+1}$* , IEEE Trans. Inform. Theory 47 (2001), 2573–2579.
- [40] A. I. Kontogeorgis, *The group of automorphisms of the function fields of the curve $x^n + y^m + 1 = 0$* , J. Number Theory 72(1), 1998, pp 110–136.
- [41] G. Korchmáros and M. Montanucci, *Large odd prime power order automorphism groups of algebraic curves in any characteristic*, Journal of Algebra 547 (2020) 312–344.
- [42] G. Korchmáros and M. Montanucci, *Ordinary algebraic curves with many automorphisms in positive characteristic*, Algebra Number Theory 13 (1) (2019) 1–18.
- [43] R. Kulkarni, *Riemann Surfaces admitting Large Automorphism Groups*, in Extremal Riemann Surfaces (San Francisco, CA, 1995), 63–79, Contemp. Math. 201, American Mathematical Society, Providence, RI, 1997.
- [44] S. Lia and M. Timpanella, *Bound on the order of the decomposition groups of an algebraic curve in positive characteristic*, Finite Fields and Their Applications 69 (2021), 101771.
- [45] C. Lomuto, *Riemann surfaces with a large abelian group of automorphisms*, Collect. Math. 57 (2006), 3: 309-318.
- [46] A. M. Macbeath, *On a Theorem of Hurwitz*, Glasgow Mathematical Journal 5(2) 1961, pp. 90–96.

BIBLIOGRAPHY

- [47] M. Matignon and M. Rocher, *Smooth curves having a large automorphism p -group in characteristic $p > 0$* . Algebra & Number Theory 2(8) (2008), 887–926.
- [48] M. Montanucci and P. Speziali, *Large automorphism groups of ordinary curves in characteristic 2*, Journal of Algebra 526 (2019) 30–50.
- [49] M. Montanucci and G. Zini, *Generalized Artin-Mumford curves over finite fields*, Journal of Algebra 485 (2017), 310–331.
- [50] K. Nakagawa, *On the orders of automorphisms of a closed Riemann surface* Pac. J. Math. 115(2) (1984), 435–443.
- [51] S. Nakajima, *On abelian automorphism groups of algebraic curves*, London Math. Soc. 36 (1987), pp. 23–32.
- [52] S. Nakajima, *p -ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. 303 (1987), 595–607.
- [53] R. Pignatelli and C. Raso, *Riemann surfaces with a quasi large abelian group of automorphisms*, Le Matematiche 66(2) (2011), pp. 77–90.
- [54] R. Pries and K. Stevenson, *A survey of Galois theory of curves in characteristic p* . In WIN—women in numbers, volume 60 of Fields Inst. Commun., pages 169–191. Amer. Math. Soc., Providence, RI, 2011.
- [55] S. Reyes-Carocca and P. Speziali, *Classifying compact Riemann surfaces by number of symmetries*, Manuscripta Mathematica 176 (2025), article number 18, DOI: 10.1007/s00229-025-01618-x.
- [56] S. Reyes-Carocca, *On Riemann Surfaces of genus g with $4g - 4$ automorphisms*, Israel Journal of Mathematics 237(1), 415–436, 2020.
- [57] H.G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. 457, (1994), 185–188.
- [58] R. Sanjeewa, *Automorphism groups of cyclic curves defined over fields of any characteristic*, Albanian Journal of Mathematics 3(4) (2009), 131–160.
- [59] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics, 67, Springer, New York, (1979), viii+241 pp.

- [60] J. P. Serre, *Topics in Galois Theory - Course at Harvard University - Fall 1988 - Notes written by Henry Darmon*, 1991.
- [61] J.H. Silverman, *The arithmetic of elliptic curves*, Second edition, Graduate Texts in Mathematics, 106 Springer, Dordrecht, (2009). xx+513 pp.
- [62] B. Singh, *On the group of automorphisms of a function field of genus at least two*, J. Pure Appl. Algebra 4 (1974) 203–229.
- [63] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. 24 (1973), 527–544.
- [64] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, (1993), x+260 pp.
- [65] H. Stichtenoth, *On automorphisms of geometric Goppa codes*, J. Algebra 130 (1990), 113–121.
- [66] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer, Amsterdam, 1991.
- [67] C. Xing, *On automorphism groups of the Hermitian codes*, IEEE Trans. Inform. Theory 41 (1995), 1629–1635.
- [68] S. Wesemeyer, *On the automorphism group of various Goppa codes*, IEEE Trans. Inform. Theory 44 (1998), 630–643.
- [69] R. Zomorrodian, *Nilpotent automorphism groups of Riemann surfaces*, Trans. Amer. Math. Soc., 288(1), 241–255, 1985.