Acknowledgements

First of all, I would like to thank my supervisor Eyal Goren for all the help gave me. Despite his very busy schedule and his family obligations, he spent very many hours coaching me, explaining new theory, guiding my writing, pushing me to greater heights and helping my English.

I would also like to thank all the professors who taught me during my graduated studies. I have gained a lot from the courses they gave me, they greatly stimulated my interest for mathematics. I also want to thank the Department of Mathematics and Statistics of McGill University, FCAR, and ISM for their financial support.

I hereby express my infinite gratitude to my family, that is, all my friends and relatives, for their constant love and support. Finally, I would like to give a special thanks to Neil for all his patience and for all the encouragement he gave me during the last year.

Abstract

Oort gave a complete description of symplectic commutative group schemes killed by p and of rank p^{2g}. Each such group appears as the p-torsion group scheme of some principally polarized abelian variety and this classification can be given in terms of final sequences. In this thesis, we focus on the particular situation where the abelian variety is the Jacobian of a hyperelliptic curve. We concentrate on describing the subspace of the moduli space of hyperelliptic curves, or rather the cycle, corresponding to a given final sequence. Especially, we concentrate on describing the subspace corresponding to the non-ordinary locus, which is a union of final sequences.

Résumé

Une description complète des schémas commutatifs symplectiques de rang p^{2g} annihilés par p a été donnée par Oort. Cette classification peut être donnée en termes de suites finales et chacun de ces schémas peut être réalisé comme le schéma en groupes de p-torsion d'une variété abelienne principalement polarisé. Dans ce mémoire nous nous restreignons au cas particulier où la variété abélienne est la Jacobienne d'une courbe hyperelliptique. Nous nous appliquons à la description du sous-espace de l'espace des modules des courbes hyperelliptiques, qui est en fait un cycle, correspondant à une suite finale donnée. Nous nous attardons particulièrement à la description du lieu non-ordinaire, sous-espace correspondant à une union de suites finales.

Contents

Introduction

A complete description of symplectic commutative group schemes killed by p and of rank p^{2g} is known and can be given in terms of final sequences. Each such group appears as the p-torsion group scheme of some principally polarized abelian variety. This classification gives a stratification of $\mathcal{A}$, the moduli space of principally polarised abelian varieties, called the Ekedahl-Oort stratification. In this thesis, we focus on the particular situation where the abelian variety is the Jacobian of a hyperelliptic curve. We concentrate on describing the subset of the moduli space of hyperelliptic curves corresponding to a given final sequence, that is a stratum in $\mathcal{A}$. This thesis is subdivided in two major sections.

In the first chapter, we discuss all the theory involved in our explorations. Starting with the basic definition of a curve, we introduce the general background for the topic, such as divisors and Jacobians. In the second, the genus of a curve is introduced. We also discuss two main theorems: the Riemann-Roch theorem and the Hurwitz formula. Section 3 is devoted to the particular curves we are interested in: the hyperelliptic curves. It is a self contained section and leads to a very precise description of these curves in terms of Weierstrass points.

The fourth section introduces the theory of moduli spaces. For this section only, we assume that the reader is familiar with the theory of schemes. After some basic definitions, we construct H_g, the moduli space of genus g hyperelliptic curves. Also we construct the moduli space of these special curves together with a level structure. The definition of an affine group scheme is developed in section 5. These group schemes are central in our study. Indeed, it turns out that for a genus g curve C defined over a field of characteristic p, the p-torsion of its Jacobian, $\mathrm{Jac}(C)[p]$, is a self-dual p-torsion commutative group scheme of order p^{2g}. The Frobenius morphism is also introduced in this section and is used in a later classification of the hyperelliptic curves.

There is an equivalence of categories between these particular p-torsion groups and certain Dieudonné modules. These modules are finite dimensional vector spaces over k together with two maps: F and V, and an alternating pairing such that certain identities hold. The last section of the first chapter deals with these new objects. A partial classification of our curves in terms of ordinary and non-ordinary curves can be given using the Hasse-Witt matrix. This matrix describes the Frobenius morphism on $H^1(\mathrm{Jac}(C), \mathcal{O}_{\mathrm{Jac}(C)})$. Since we have an equivalence of categories, with some work we deduce that the matrix can be given through the action of V on $H^0(C, \Omega^1_C)$ which gives an explicit matrix. To end this theorical section, a complete classification of self-dual p-torsion commutative group schemes of order p^s is introduced. This classification is given in terms of final sequences and can also be used to describe Dieudonné modules. With all these tools in our hands, the main goal of the second part of this thesis is to relate these final sequences with the moduli space of hyperelliptic curves.

A brief description of the general problem is given first in the exploration chapter. We start with a very general and difficult question and finally narrow down to a very particular case. One can try to describe the subset of the moduli space H_g that corresponds to a given final sequence ψ , *i.e.*, the subset of points x, such that the corrseponding hyperelliptic curve C_x has that fixed elementary sequence ψ. Also, one can seek to describe the points that correspond to the non-ordinary locus, which corresponds to a union of sequences.

We then consider the same problem for coverings of curves, especially degree 2 unramified double coverings of genus g hyperelliptic curves. These particular coverings of hyperelliptic curves can be described by a moduli space H_g^2. We then give special attention to describing the subspace of H_g^2 corresponding to non-ordinary coverings, that is coverings $\gamma : D \longrightarrow C$ for which D is non-ordinary. A special curve is then introduced: the maxno-2 curve, which is a hyperelliptic curve such that all its double unramified coverings are non-ordinary. We have specially considered the situation for genus 2 curves. One example of maxno-2 curve is provided and we prove that for each prime p there is only a finite number of maxno-2 curves defined over a field of characteristic p.

CHAPTER 1

General Theory

Throughout this thesis, we assume the basic background of algebraic geometry. For the very beginning we work over an algebraically closed field k and we use the convention that a variety is irreducible.

1. Curves

DEFINITION 1.0.1. *A curve C over k is a smooth projective variety over k of dimension* 1.

For a curve C defined over k, its function field $k(C)$ is of transcendence degree one over k. It follows that $k(C)$ is an algebraic function field, *i.e.*, $k(C)$ is algebraic over any subfield $k(x)$ generated by a non constant function $x \in k(C)$. Thus, $k(C)$ can be written as $k(x, y)$, where x and y are two non-constant functions on C satisfying $F(x, y) = 0$, an algebraic relation. If we let C_0 be the affine curve defined by F, and C_1 the projective curve obtained by taking the closure of C_0 in $\mathbb{P}^2(k)$, we get that C_0 and C_1 are birational to C. Such curves are called models of C, and every curve has a plane projective model and a plane affine model. Note that usually these models are not smooth.

An example that is central in this thesis is $F(x, y) = y^2 - f(x)$ with $f(x) \in k(x)$ and $\mathrm{char}(k) \neq 2$. Note that by changing y, we may assume that $f(x)$ is in $k[x]$ and is squarefree, hence separable. The affine curve defined by $F(x, y) = 0$ is then non-singular, but its projective closure defined by homogenizing $F(x, y)$ is usually singular.

Conversely, given K, a finitely generated field extension of transcendence degree one of k, that we define as a *function field*, we would like to consider the curve C whose function field is K. To do so, we consider C_K, the set of all discrete valuation rings of K/k. For every smooth curve C and every point P on it, the local ring $\mathcal{O}_{C,P}$ of P on C is a discrete valuation ring contained in $k(C)$. Hence, the following definition of the curve C_K seems to be natural.

DEFINITION 1.0.2. *An abstract non-singular curve C is an open subset $U \subseteq C_K$, where K is a function field of dimension 1 over k, with the induced topology, and the notion of regular functions on its open subsets. (See* [**8**, page 42]*.)*

To link these abstract curves with our first definition, one can find the following theorem in [**8**, I, § 6, Thm 9].

THEOREM 1.0.1. *Let K be a function field of dimension 1 over k. Then the abstract nonsingular curve C_K is isomorphic to a nonsingular projective curve over k whose function field is K.*

If we consider Y, a variety of dimension 1 which is not necessarily smooth and projective, having function field K, then Y is birationally equivalent to the abstract curve C_K which is non-singular and projective. Also, we can always write a function field as $k(x)[y]/(F(x,y))$ to get a planar curve. Then by taking the projective closure and then taking the normalisation we get a non-singular projective curve. Therefore, we can restate the above theorem:

COROLLARY 1.0.1. *Every curve, in the general sense, is birationally equivalent to a non-singular projective curve.*

Theorem 1.0.1 and Corollary 1.0.1 are fundamentals for the following equivalence of categories that allows us to study curves in different contexts.

THEOREM 1.0.2. *The following categories are equivalent:*

(1) *non-singular projective curves, and non-constant morphisms;*

(2) *quasi-projective curves, and non-constant rational maps;*

(3) *function fields of dimension 1 over k, and k-homomorphisms.*

Remark: The equivalence between (2) and (3) reverses arrows.

1.1. Divisors on curves over an algebraically closed ground field.

Let k, be an algebraically closed field and let C be a non-singular projective curve over k. A *divisor* D on C over k is, by definition, a formal

$$D = \sum_{P \in C} n_P[P],$$

where the P are points on the curve, $n_P \in \mathbb{Z}$ and only finitely many n_p are non-zero .

The set $\mathrm{Div}(C)$ of all divisors D on a curve C is a free abelian group on the basis $\{ [P] : P \in C \}$. We let $\deg(D) := \sum n_p$ denote the degree of a divisor D. We denote by $\mathrm{Div}^0(C)$ the group of *divisors of degree zero*, and we say that a non-zero divisor $D = \sum n_P[P]$ is *effective* if $n_P \geq 0$ for all P. Furthermore, $D = \sum n_P[P]$ is said to be greater or equal to $D' = \sum n'_P[P]$ if $n_P \geq n'_P$ for all P. We use the usual the notation $D \geq D'$.

To any function f in $k(C)^*$ we can associate a divisor

$$(f) = \sum_{P \in C} \mathrm{val}_P(f)[P],$$

where $\mathrm{val}_P(f)$ is given by the valuation of f at the point P in the local ring $\mathcal{O}_{C,P}$. Such divisors are called principal divisors. If N denotes the set of zeros of f, and Z denotes the set of poles of f, we define

$$(f)_0 := \sum_{P \in N} \mathrm{val}_P(f)[P], \qquad \text{the } \textit{zero divisor} \text{ of } f,$$

$$(f)_\infty := \sum_{P \in Z} -\mathrm{val}_P(f)[P], \qquad \text{the } \textit{polar divisor} \text{ of } f.$$

Clearly, $(f)_0 \geq 0$, $(f)_\infty \geq 0$ and $(f) = (f)_0 - (f)_\infty$. Also, one can find in [**8**, II,§6] that $\deg(f)_0 = \deg(f)_\infty$. The relation $(f \cdot g) = (f) + (g)$ shows that the principal divisors form a group denoted

$$\mathrm{Pr}(C) : = \{(f) \mid f \in k(C)^*\},$$

where the zero element is the empty divisor (1), and the inverse of (f) is (f^{-1}).

The following factor group

$$\mathrm{Pic}(C) := \mathrm{Div}(C)/\mathrm{Pr}(C),$$

is called the *divisor class group*. Two divisors D and D' are said to be *linearly equivalent* if $D - D'$ is a principal divisor, *i.e.*, if they are equal in $\mathrm{Pic}(C)$. Since the degree of a principal divisor (f) is, counting multiplicity, equal to the difference between the number of the poles of f and the number of zeros of f, we have that $\deg(f) = 0$. Therefore, $\mathrm{Pr}(C)$ is a subgroup of $\mathrm{Div}^0(C)$ and we can define the Jacobian of a curve C to be:

$$\mathrm{Jac}(C) = \mathrm{Div}^0(C)/\mathrm{Pr}(C).$$

It is well known that $\mathrm{Jac}(C)$ is the k-points of an abelian variety over k see [**20**, §10] and the result has been given first by Weil.

To a divisor D, we can associate the k-vector space $\mathcal{L}(D)$ defined by

$$\mathcal{L}(D) = \{f \in k(C)^* \mid (f) \geq -D\} \cup \{0\}.$$

The dimension of $\mathcal{L}(D)$ is denoted $l(D)$. For $D = \sum n_P[P] - \sum m_Q[Q]$ with $n_P > 0$ and $m_Q > 0$, the k-vector space $\mathcal{L}(D)$ consists of elements f in $k(C)$ such that

(1) f has a zero of order at least m_Q at every point Q, and

(2) f may have poles only at the points P, with the pole order at P being at most n_P.

Clearly, if $\deg(D) < 0$, then $\mathcal{L}(D) = \{0\}$ and $l(D) = 0$. One can also prove that $\mathcal{L}(D)$ is finite dimensional, and that $\mathcal{L}(D') \cong \mathcal{L}(D)$ if the two divisors are linearly equivalent, see [**9**, A,§ 2.2].

1.2. Divisors on curves over arbitrary ground fields.

Let k be any perfect field and $\overline{k}$ its algebraic closure. We say that a curve C is *defined over* k if there exist homogeneous polynomials $f_1, ...f_s \in k[x]$ such that $C/\overline{k}$ is a curve defined as the zero set of $I = (f_1, ...f_s)$, an ideal in $\overline{k}[x]$. For the situation $k = \overline{k}$ we will often omit the ground field and denote the curve just by C. For any Galois extension,

$$\begin{array}{c} \overline{k} \\ | \\ L \end{array}$$

we easily check that $C(L)$, the L-rational points on the curve C, are also given as $C(\overline{k})^\Gamma$ where $\Gamma = \mathrm{Gal}(\overline{k}/L)$.

On the other hand, if we consider, instead of the category of curves, the category of function fields of dimension 1 we have that $F = k(C)/k$, the function field over field k, has field extension $\overline{k}(C)/\overline{k}$. The set $\tilde{k} := \{z \in k(C) \mid z \text{ is algebraic over } k\}$ is a subfield of $k(C)$ and is called the *field of constants* of $k(C)/k$. We say that k is the *full constant field* of $k(C)$ if $\tilde{k} = k$. Since the transcendence degree of F is 1, the field of constants of an algebraic function field F is a finite extension field of k, thus F can be regarded as function field over $\tilde{k}$. Therefore from here on, $k(C)$ will always denote an algebraic function field of one variable such that k is the full constant field of $k(C)/k$. In this scope it is also possible to introduce the notion of divisor.

DEFINITION 1.2.1. *A place P of the function field $k(C)$ is the maximal ideal of some valuation ring $\mathcal{O}_P \in C_{k(C)}$. We denote the set of all such places by $\mathcal{P}_{k(C)}$, and the residue class field by $k(C)_P := \mathcal{O}_P/P$.*

For $f \in k(C)$, we say that a place P is a *zero* of f if $v_P(f) > 0$, that is if f belongs to P. We denote $\deg P = [k(C)_P : k]$ the degree of the place P and one can find in [**30**, page 6] that $\deg P \leq [k(C) : k(x)] < \infty$. In this situation, the free abelian group which is generated by the places of $k(C)$ is named the *divisor group defined over k* and denoted $\mathrm{Div}_k(C)$. The divisors can now be expressed this way

$$D = \sum_{P \in \mathcal{P}_{k(C)}} n_P[P] \text{ with } n_P \in \mathbb{Z} \text{ and almost all } n_P = 0,$$

and the degree of such divisor is defined by

$$\deg(D) := \sum_{P \in \mathcal{P}_{k(C)}} \mathrm{val}_P(D) \deg P.$$

Indeed this definition is analogous to the definition of divisors over algebraically closed fields. To see that assume that C is affine with ring of regular functions $R = k[x_1, ..., x_n]/(f_1, ...f_s)$. Every prime ideal is maximal (since R is of dimension 1) and hence, by Hilbert's Nullstellensatz, of the form $(x_1 - \alpha_1, ..., x_n - \alpha_n)$ for suitable $\alpha_1, ..., \alpha_n$. We therefore see that places correspond to points.

As for the previous situation, for $f \in k(C)$ and for any place P, $\mathrm{val}_P(f)$ still makes sense, therefore we can define (f) to be the principal divisor associated to the function f. One can verify easily that except for the Jacobian of such curve, the definitions made previously hold in this situation. Moreover for $x \in k(C)$, we can find in [**30**, page 18] that $\deg(x)_0 = \deg(x)_\infty = [k(C) : k(x)]$.

Let C/k be a curve over k and let $\Gamma = \mathrm{Gal}(\overline{k}/k)$ act on $\mathrm{Div}_{\overline{k}}(C)$ and $\mathrm{Div}^0_{\overline{k}}(C)$ by the rule

$$D \overset{\sigma}{\mapsto} D^\sigma = \sum_{P \in \mathcal{P}_{\overline{k}(C)}} n_P[P^\sigma], \quad \sigma \in \Gamma,$$

and where the corresponding valuation is given by

$$\mathrm{val}_{\sigma(P_i)}(y) = \mathrm{val}_{P_i}(\sigma^{-1}(y)) \text{ for } y \in \overline{k}(C).$$

The main point here is that a place of $k(C)$ corresponds to a Galois orbit of places of $\overline{k}(C)$. In fact, the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set of places $P_i \in L$ lying over a given place $Q \in K$.

Theorem 1.2.1. *Let L be a Galois extension of K and $P_1,\ P_2 \in \mathcal{P}_L$ be extensions of $Q \in \mathcal{P}_K$. Then $P_2 = \sigma(P_1)$ for some $\sigma \in \Gamma = \mathrm{Gal}(L/K)$.*

Proof: Assume the opposite, *i.e.* that $\sigma(P_1) \neq P_2$ for all $\sigma \in \Gamma$. By the approximation theorem, see [**30**, I.§3.1], there is an element $z \in L$ such that $\mathrm{val}_{P_2}(z) > 0$ and $\mathrm{val}_P(z) = 0$ for all $P \in \mathcal{P}_L$ lying above Q and different of P_2. Let $N_{L/K} : L \longrightarrow K$ be the norm map. We obtain

$$\begin{aligned} \mathrm{val}_{P_1}(N_{L/K}(z)) &= \mathrm{val}_{P_1}(\prod_{\sigma\in\Gamma} \sigma(z)) \\ &= \sum_{\sigma \in G} \mathrm{val}_{P_1}(\sigma(z)) \\ &= \sum_{\sigma\in\Gamma} \mathrm{val}_{\sigma^{-1}(P_1)}(z) \\ &= \sum_{\sigma\in\Gamma} \mathrm{val}_{\sigma(P_1)}(z) = 0, \end{aligned}$$

since P_2 does not occur among the places $\sigma(P_1)$, for $\sigma \in G$.

On the other hand,

$$\mathrm{val}_{P_2}(N_{L/K}(z)) = \sum_{\sigma\in\Gamma} \mathrm{val}_{\sigma(P_2)}(z) > 0.$$

But $N_{L/K}(z) \in K$, therefore

$$\mathrm{val}_{P_1}(N_{L/K}(z)) = 0 \Leftrightarrow \mathrm{val}_Q(N_{L/K}(z)) = 0 \Leftrightarrow \mathrm{val}_{P_2}(N_{L/K}(z)) = 0,$$

a contradiction. $\square$

Thus, we can consider $\mathrm{Div}_k(C)$ as a subset of $\mathrm{Div}_{\overline{k}}(C)$ the following way:

$$\begin{aligned}\mathrm{Div}_k(C) &= \left\{\sum_i^n n_i[P_i] \mid n_i \in \mathbb{Z}\right\} \\ &= \left\{\sum_i^n n_i(\sum_{Q\in\theta_i}[Q]) \mid n_i \in \mathbb{Z},\ \theta_i \text{ is the orbit of } \Gamma \text{ in } \mathcal{P}_{\overline{k}(C)} \text{ corresponding to } P_i\right\} \\ &\subset \mathrm{Div}_{\overline{k}}(C).\end{aligned}$$

Since every orbit corresponds to a place in $\mathrm{Div}_k(C)$, the only divisors in $\mathrm{Div}_{\overline{k}}(C)$ fixed by Γ will be of this form and we have the following equality:

$$\mathrm{Div}_k(C) = \left\{\sum_i^n n_i(\sum_{p\in\theta_i}[P]) \mid n_i \in \mathbb{Z},\ \theta_i \text{ is an orbit of } \Gamma \text{ in } \mathcal{P}_{\overline{k}(C)}\right\} = (\mathrm{Div}_{\overline{k}}(C))^\Gamma.$$

It follows similarly that the *group of divisors of degree* 0 *defined over* k will be

$$\mathrm{Div}^0_k(C) = (\mathrm{Div}^0_{\overline{k}}(C))^\Gamma.$$

For instance, take $k = \mathbb{Q}$ and the curve $C : y^2 - 2x = 0$. Let $m = (y^2 - 2, x - 1)$; it is a maximal ideal of some valuation ring of $\mathbb{Q}(C)$. Therefore the place P associated to this ideal can be viewed as $[1, \sqrt{2}] + [1, -\sqrt{2}]$ and this place corresponds to one orbit of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Note that one place in $\overline{\mathbb{Q}}(C)$ is sent to the other via

$$\sigma : \sqrt{2} \mapsto -\sqrt{2}.$$

For $f \in k(C)^*$, we can, as done previously, associate to it the divisor

$$(f) = \sum_{P\in\mathcal{P}_{k(C)}} \mathrm{val}_P(f)[P] = \sum_{P\in\mathcal{P}_{k(C)}} \mathrm{val}_P(f)(\sum_{Q\in\theta_P}[Q])$$

where θ_P is an orbit of Γ in $\mathcal{P}_{\overline{k}(C)}$ corresponding to P. And for any $\sigma \in \Gamma$ we easily check that

$$(f)^\sigma = \sum_{P \in \mathcal{P}_{k(C)}} \mathrm{val}_P(f)(\sum_{Q \in \theta_P} [Q]^\sigma) = (f),$$

since σ permutes the elements in the orbits. Therefore

$$\mathrm{Pr}_k(C) = \{\ D \in \mathrm{Div}_k(C) \mid D = (f) \text{ for some } f \in k(C)^*\} \subset (\mathrm{Pr}_{\overline{k}}(C))^\Gamma,$$

and we would like to have equality. Since k is perfect, $\overline{k}/k$ is a separable extension, so $\overline{k}^\Gamma = k$, and $(\overline{k}(C)^*)^\Gamma = k(C)^*$. We consider the exact sequence

$$1 \longrightarrow \overline{k}^* \longrightarrow \overline{k}(C)^* \xrightarrow{div} \mathrm{Pr}_{\overline{k}}(C) \longrightarrow 0.$$

By applying Galois cohomology we get

$$1 \longrightarrow (\overline{k}^*)^\Gamma \longrightarrow (\overline{k}(C)^*)^\Gamma \xrightarrow{div} (\mathrm{Pr}_{\overline{k}}(C))^\Gamma \longrightarrow H^1(\Gamma, \overline{k}^*) \longrightarrow \cdots, \tag{1.1}$$

which leads to the short exact sequence

$$1 \longrightarrow k^* \longrightarrow k(C)^* \xrightarrow{div} \mathrm{Pr}_{\overline{k}}(C)^\Gamma \longrightarrow 0,$$

since by Hilbert's 90, $H^1(\Gamma, \overline{k}^*) = 0$. Therefore, we have the equality

$$\mathrm{Pr}_k(C) = \mathrm{Pr}_{\overline{k}}(C)^\Gamma.$$

We can also define $\mathrm{Jac}_k(C)$ to be the subgroup of $\mathrm{Jac}_{\overline{k}}(C)$ fixed by Γ. In general, $\mathrm{Jac}_k(C)$ is not the quotient of $\mathrm{Div}_k^0(C)$ by its subgroup of principal divisors. But in the particular case that will interest us, the case where k is a finite field, we have what we would expect.

For $k = \mathbb{F}_q$ and $\Gamma = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ we have another exact sequence

$$0 \longrightarrow \mathrm{Pr}_{\overline{\mathbb{F}}_q}(C) \longrightarrow \mathrm{Div}^0_{\overline{\mathbb{F}}_q}(C) \longrightarrow \mathrm{Jac}_{\overline{\mathbb{F}}_q}(C) \longrightarrow 0,$$

and, by taking the Galois cohomology, we get

$$0 \longrightarrow \mathrm{Pr}_{\mathbb{F}_q}(C) \longrightarrow \mathrm{Div}^0_{\mathbb{F}_q}(C) \longrightarrow \mathrm{Jac}_{\overline{\mathbb{F}}_q}(C)^{\Gamma} \longrightarrow H^1(\Gamma, \mathrm{Pr}_{\overline{\mathbb{F}}_q}(C)) \longrightarrow \cdots.$$

As stated before, this is generally not a short exact sequence. But in the case of finite fields, the cohomology group $H^1(\Gamma, \mathrm{Pr}_{\overline{\mathbb{F}}_q}(C))$ is zero. For if we consider the continuation of the sequence (1.1) we have

$$\cdots \longrightarrow H^1(\Gamma, \overline{\mathbb{F}}_q^*) \longrightarrow H^1(\Gamma, \overline{\mathbb{F}}_q(C)^*) \longrightarrow H^1(\Gamma, \mathrm{Pr}_{\overline{\mathbb{F}}_q}(C)) \longrightarrow H^2(\Gamma, \overline{\mathbb{F}}_q^*) \longrightarrow \cdots.$$

Again by Hilbert's 90, we get that $H^1(\Gamma, \overline{\mathbb{F}}_q^*) = 0 = H^1(\Gamma, \overline{\mathbb{F}}_q(C)^*)$ and one can find in [**18**] that the Brauer group $H^2(\Gamma, \overline{\mathbb{F}}_q^*)$ is zero for finite fields. Therefore,

$$\begin{aligned} \mathrm{Jac}_{\mathbb{F}_q}(C) : &= \mathrm{Jac}(C)^{\Gamma}_{\overline{\mathbb{F}}_q} \\ &= (\mathrm{Div}^0_{\overline{\mathbb{F}}_q}(C))^{\Gamma} / (\mathrm{Pr}_{\overline{\mathbb{F}}_q}(C))^{\Gamma} \\ &= \mathrm{Div}^0_{\mathbb{F}_q}(C) / \mathrm{Pr}_{\mathbb{F}_q}(C). \end{aligned}$$

1.3. Covering of curves.

We will be interested in this thesis in particular morphisms between curves, thus the following terminology will be needed.

DEFINITION 1.3.1. *A covering of a curve C is a finite separable morphism of curves $f : D \longrightarrow C$.*

In terms of function fields it corresponds to a finite separable extension $k(D)/k(C)$. As stated before, we assume that the field k is *perfect*, *i.e.*, that all algebraic extensions L/k are separable. For example, k is perfect if it is algebraically closed or if it is a finite field.

DEFINITION 1.3.2. *Let $k(D)$ be an algebraic extension of $k(C)$, and let $P \in \mathcal{P}_{k(D)}$ be a place of $k(D)$ lying over $Q \in \mathcal{P}_{k(C)}$. The integer e_P satisfying*

$$\mathrm{val}_P(x) = e_P \cdot \mathrm{val}_Q(x)$$

for any $x \in k(C)$ is called the ramification index of P over Q.

If k is algebraically closed, the equivalence of categories between curves and function field allows the following equivalent formulation:

Definition 1.3.3. *Let $f : D \to C$ be a finite morphism of smooth projective curves. For $P \in D$, $Q = f(P)$, and $t \in \mathcal{O}_Q(C)$ an uniformizing parameter, the integer $e_P = \mathrm{val}_P(f^*t)$ is called the ramification index of f at P.*

We say that a covering of curves (or an extension of function fields) is *unramified* at a point (or a place) P if $e_P = 1$, otherwise the covering is said to be *ramified* at this point (or place). Such a covering (or extension) will be called unramified if it is unramified at every point (or place) of D. For instance, for k a field of odd characteristic, consider the curve D with affine model $y^2 = xg(x)$ and such that $g(0) \neq 0$ (note that this condition is needed to have a smooth curve). We then have a canonical mapping from D to the projective line. The degree two map

$$\begin{array}{ccc} D & \longrightarrow & \mathbb{P}^1 \\ (x,y) & \mapsto & x \end{array}$$

is ramified since there is at least one ramification point on the curve. Indeed the map has a ramification index $e_P = 2$ at the point $P = (0,0)$. But note that some points on D are unramified, for instance the points on D of the form $R = (\alpha, \beta)$, where $\beta \neq 0$, have ramification index $e_R = 1$.

Let $k(D)/k(C)$ be a Galois extension and let Q be any place of $k(C)$. The Galois group $\Gamma = \mathrm{Gal}(k(D)/k(C))$ acts on the set of places P_i lying over Q via $\sigma(P_i) = \{\sigma(x) |\ x \in P_i\}$, where $\sigma \in \Gamma$ and the corresponding valuation is given by

$$\mathrm{val}_{\sigma(P_i)}(y) = \mathrm{val}_{P_i}(\sigma^{-1}(y)) \text{ for } y \in k(D).$$

In fact, Theorem 1.2.1 shows that the Galois group $\mathrm{Gal}(k(D)/k(C))$ acts transitively on the set of places $P_i \in k(D)$ lying over a given place $Q \in k(C)$.

2. The genus of a curve

One of the most important invariants in the study of curves is the genus which is a birational invariant. One way to define it is the following:

DEFINITION 2.0.4. *The genus of a non-singular projective curve C is the dimension of the k-vector space of holomorphic differentials on C, denoted*

$$g_C := \dim\ H^0(C, \Omega_C^1).$$

The genus of a curve can be expressed in different ways, in particular, one can show that the dimension of $\mathrm{Jac}(C)$ is precisely g_C, that $g_C = \dim\ H^1(C, \mathcal{O}_C)$ and that over the complex numbers $\mathrm{rk}_{\mathbb{Z}} H_1(C(\mathbb{C}), \mathbb{Z}) = 2g_C$.

2.1. The Riemann-Roch theorem and the Hurwitz formula.

Some of the most important tools in the study of curves are the Riemann-Roch theorem and the Hurwitz formula. For example, the Riemann-Roch theorem allows us to link elements of $k(C)$ with the genus of the curve. Given a covering of curves, the Hurwitz formula links the genus of the two curves with the number of ramification points. It is known that the sheaf of differential forms Ω_C^1 is locally free of rank one:

$$\Omega_C^1 \cong \mathcal{O}_C(K_C),$$

where K_C is a divisor on C. This is well define up to a principal divisor. Let $\omega \in H^0(C, \Omega_C^1)$, *i.e.*, ω is a holomorphic differential, then the *canonical* divisor is given by $K_C = (\omega)$.

Example:

(1) For $C = \mathbb{P}^1$, we have $\omega = dz = \frac{-1}{u^2} du$ for $u = \frac{1}{z}$, thus $K_C = -2\infty$;
(2) for C an elliptic curve, $K_C = 0$ is the empty divisor;

(3) for C a smooth projective model of $y^2 - f(x)$, with $f(x)$ a separable polynomial of degree $2g+2$, we have $\omega = dx = \frac{2y}{f'(x)}dy$. Therefore

$$K_C = \sum_{\lambda, f(\lambda)=0} [(\lambda, 0)] - 2\infty_1 - 2\infty_2,$$

where ∞_1, ∞_2 are the two points lying over ∞ under the natural map $C \longrightarrow \mathbb{P}^1$.

THEOREM 2.1.1. (Riemann-Roch) *Let C be a curve and K_C a canonical divisor, then for all divisors D,*

$$l(D) - l(K_C - D) = \deg(D) - g_C + 1,$$

where g_C is the genus of the curve C.

One can find a proof of this theorem in [**30**, I.5], and this corolarry will be usefull in our later study.

COROLLARY 2.1.1.

(1) *For K_C a canonical divisor, we have*

$$l(K_C) = g_C, \qquad deg(K_C) = 2g_C - 2.$$

(2) *If* $\deg(D) > 2g_C - 2$, *then*

$$l(D) = \deg(D) - g_C + 1.$$

Proof: (1) By taking $D = 0$, we get

$$l(0) - l(K_C) = \deg(0) - g_C + 1,$$

since $\mathcal{L}(0) = k$ and $\deg(0) = 0$, we get that $l(K_C) = g_C$. Setting now $D = Kc$, from this previous result, we obtain the following:

$$g_C - 1 = \deg(K_C) - g_C + 1,$$

which easily leads to the equality $\deg(K_C) = 2g_C - 2$.

(2) From Riemman-Roch theorem, we only need to show that $l(K_C - D) = 0$. Since $\deg(D) > 2g_C - 2$ and $\deg(K_C) = 2g_C - 2$, we have that $\deg(K_C - W) < 0$, therefore, it follows that $l(K_C - D) = 0$. $\square$

THEOREM 2.1.2. (Hurwitz's formula) *Let C be a curve of genus g_C, let D be a curve of genus g_D, and let $f : D \to C$ be a finite separable morphism of degree n. For each point $P \in D$, write e_P for the ramification index of f at P, and assume that either* $\mathrm{char}(k) = 0$ *or else that* $\mathrm{char}(k)$ *does not divide the e_P's, i.e., the covering is tamely ramified. Then*

$$2g_D - 2 = (2g_C - 2)n + \sum_{P \in D} (e_P - 1).$$

A proof can be found in [**30**, III.4] and, in order to introduce the analogue of the Hurwitz formula in the situation of function fields, we need some preliminary definitions. We will consider an algebraic function field $k(C)$ and a finite separable extension $k(D)/k(C)$.

DEFINITION 2.1.1. *For $P \in \mathcal{P}_{k(C)}$, let $\mathcal{O}'_P$ denote the integral closure of $\mathcal{O}_P$ in $k(D)$. Then the set*

$$\mathcal{C}_P := \{z \in k(D) \mid Tr_{k(D)/k(C)}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

is called the complementary module over $\mathcal{O}_P$.

One can verify that $\mathcal{C}_P$ is an $\mathcal{O}'_P$-module. In fact $\mathcal{O}'_P$ is contained in $\mathcal{C}_P$ and there is an element $t \in k(D)$ (depending of P) such that $C_P = t \cdot \mathcal{O}'_P$. One can also show that $\mathrm{val}_{P'}(t) \leq 0$ for all P' lying above P and $\mathcal{C}_P = \mathcal{O}'_P$ for almost all $P \in \mathbb{P}_k(C)$. Then we define the *different exponent* of P' over P by

$$d(P'|P) := -\mathrm{val}_{P'}(t).$$

Since $C_P = 1 \cdot \mathcal{O}'_P$ for almost all P, then $d(P'|P) = 0$ almost everywhere so we can define the divisor

$$\mathrm{Diff}(k(D)/k(C)) := \sum_{P \in \mathcal{P}_{k(C)}} \sum_{P'|P} d(P'|P) \cdot P',$$

called the *different* of $k(D)/k(C)$.

THEOREM 2.1.3. (Hurwitz formula II) *Let $k(C)$ be an algebraic function field of genus g_C, and $k(D)$ a finite separable extension of genus g_D, then*

$$2g_D - 2 = (2g_C - 2)[k(D) : k(C)] + \deg\ \mathrm{Diff}(k(D)/k(C)).$$

Remark: In fact, $\Omega^1_{D/C} = \mathcal{O}_C(\mathrm{Diff}(k(D)/k(C))$, where $\Omega^1_{D/C}$ is the sheaf of relative differentials.

2.2. Classification of curves by their genus.

The genus of a curve allows us to make a distinction between some of them, and, in the scope of the above theorems, this invariant can give a good description of some particular curves.

2.2.1. *Genus* 0.

If we consider a curve defined over an algebraically closed field, the only curve of genus 0 is the projective line. Indeed, if the genus of the curve is 0, by the Riemann-Roch Theorem, $l([P]) = 2$ for all points in C. Therefore we have a non constant function $x \in \mathcal{L}(P)$ having at most a pole of multiplicity one at P. So $\deg(x)_\infty = 1 = [k(C) : k(x)]$, *i.e.*, the curve C is birationaly equivalent to $\mathbb{P}^1$. We therefore restrict our attention to $\mathbb{P}^1$. If $D = \sum n_p[P]$ is a divisor of degree 0, where $P = [\alpha_P, \beta_P] \in \mathbb{P}^1$, then D is clearly the divisor associated to the function

$$f = \prod_P (\beta_P X - \alpha_P Y)^{n_P} \in k(\mathbb{P}^1).$$

Hence, $\mathrm{Pic}(\mathbb{P}^1) \cong \mathbb{Z}$ and $\mathrm{Jac}(\mathbb{P}^1)$ is trivial, therefore it has dimension $g_{\mathbb{P}^1} = 0$.

If the curve is not defined over an algebraically closed field, problems may arise when there is no k-rational point on the curve. One can find in [**9**, A,§ 4.3], that one of these two situations will occur.

- The curve C is isomorphic over k to a conic in $\mathbb{P}^2$ *i.e.*, a variety defined by an irreducible quadratic polynomial.
- The curve C is isomorphic over k to $\mathbb{P}^1$ if and only if it possesses a k-rational point.

2.2.2. *Genus* 1.

The curves of genus 1 principally consist of the well known elliptic curves. An elliptic curve is a non-singular curve of genus 1 with a specified rational point. Over certain fields there are curves of genus 1 that are not elliptic curves, for instance one can find in [**9**, X,§4] that the curve of genus 1

$$2w^2 = 1 - 17z^4,$$

has no $\mathbb{Q}$-rational point. But for C a genus 1 curve, $\mathrm{Jac}_k(C)$ will always be an elliptic curve over k since the empty divisor is rational. The elliptic curves deserve a particular interest because we have that $C/k \cong \mathrm{Jac}_k(C)$. Indeed, we can show that there is a group law on the elliptic curve E that corresponds to the addition of the elements of $\mathrm{Jac}(E)$.

PROPOSITION 2.2.1. *Let P_0 a fixed basepoint on E, then the following map*

$$\begin{aligned} \phi: \ E &\rightarrow \mathrm{Jac}(E) \\ P &\mapsto [P] - [P_0]. \end{aligned}$$

is an isomorphism.

Proof:

- ϕ is injective.

  Suppose $\phi(P) = [P] - [P_0] = [Q] - [P_0] = \phi(Q)$, then there exist $f \in k(E)$ such that $(f) = [P]-[Q]$. Then $f \in \mathcal{L}([Q])$, and since $\deg([Q]) = 1 > 2g_E - 2$, by Corollary 2.1.1, we have that

  $$l([Q]) = deg([Q] - g_E + 1 = 1.$$

  But $\mathcal{L}([Q])$ already contains the constant functions, hence $f \in k$ and $P = Q$.

- ϕ is surjective.

  Consider $D \in \mathrm{Div}^0$, and let $D' = D + [P_0]$. Since $\deg(D') = 1 > 2g_E - 2$, again by Corollary 2.1.1 we deduce that $l(D') = 1$. Therefore, there exist $f \in \mathcal{L}(D')$ such that $(f) \geq -D - [P_0]$. Since $\deg(f) = 0$, and since the function f can not have other poles, we have

  $$(f) = -D - [P_0] + [P]$$

  for some $P \in E$. Hence $D \sim [P] - [P_0]$, so every divisor in $\mathrm{Jac}(E)$ is reached by ϕ.

- ϕ is a homomorphism of groups.

  Consider the points P and Q on the curve. By applying the same argument we have used for the surjectivity, with $D' = [P] + [Q] - [P_0]$, we can find a function f and a point P^* such that

  $$(f) = [P^*] - [P] - [Q] + [P_0].$$

  Hence, $\phi(P^*) = [P^*] - [P_0] = [Q] - [P_0] + [P] - [P_0] = \phi(P) + \phi(Q)$ in $\mathrm{Jac}(E)$. It suffices now to show that there is a group law on E and that the point P^* is in fact the sum of P and Q. To do so we will consider the group law induced by ϕ. We can assume first that E lies in $\mathbb{P}^2$. We can take P_0 to be the point O at infinity and choose l_1 the line through P and Q, we will denote R the third intersection point. We can also consider the line l_2 through P_0 and R where $P^{*\prime}$ is the other intersection point. Therefore $g = \frac{l_1}{l_2} \in k(E)$ and $(g) = [P] + [Q] + [R] - [P_0] - [P] - [P^{*\prime}]$. If we consider $g \cdot f \in k(E)$ we obtain the principal divisor $[P^*] - [P^{*\prime}]$. But there is no rational function on E with only one pole and one divisor, therefore $[P^{*\prime}] = [P^*]$. This defines a composition law $\oplus$ given by the following rule: Let $P, Q \in E$, L the line connecting P and Q (the tangent line if P=Q), and R the third point of intersection of L with E. Let L' be the line connecting R and P_0, then $P \oplus Q$ is the point such that L' intersect the curve E at P_0, R, and $P \oplus Q$. □

2.2.3. *Genus* ≥ 2.

The curves of higher genus are, with no surprise, more complicated. We will focus only on those that interest us, which are the hyperelliptic curves, in the next section.

3. Hyperelliptic curves

For this section we will consider k to be a perfect field not necessarily algebraically closed.

DEFINITION 3.0.1. *A hyperelliptic function field over k is an algebraic function field $k(C)/k$ of genus $g \geq 2$ which contains a rational subfield $k(x) \subseteq k(C)$ with $[k(C) : k(x)] = 2$. A hyperelliptic curve is a smooth projective curve associated to such a hyperelliptic function field $k(C)$.*

In other words, a curve of genus $g \geq 2$ is said to be a hyperelliptic curve if it is a double covering of the projective line $\pi : C \longrightarrow \mathbb{P}^1$. The points in C that are sent to ramification points are called *Weierstrass points* and the rational subfield $\pi^*(k(x))$ will often be denoted $k(x)$ to ease our notation. We shall see below that the terminology is appropriate, it does not depend on π.

PROPOSITION 3.0.2.

(1) *A curve C of genus $g \geq 2$ is hyperelliptic if and only if there exists a divisor D with* $\deg(D) = 2$ *and* $l(D) \geq 2$.
(2) *Any curve C of genus 2 is hyperelliptic.*

Proof: (1) Suppose that $k(C)$ is hyperelliptic. We can take $x \in k(C)$ such that $[k(C) : k(x)] = 2$, and consider the divisor $D := (x)_\infty$. Then the divisor D has degree equal to $[k(C) : k(x)] = 2$, and since the elements $1, x \in \mathcal{L}(D)$ are linearly independent over k, we have that $l(D) \geq 2$.

Conversely, suppose that $k(C)$ has genus $g_C \geq 2$ and D is a divisor of degree 2 with $l(D) \geq 2$. We know [**30**, I.4] that there exist an effective divisor $D_1 \sim D$ such that $\deg(D_1) = 2$ and $l(D_1) \geq 2$. Therefore we can find an element $x \in \mathcal{L}(D_1) \setminus k$ with $(x)_\infty \leq D_1$. Hence $[k(C) : k(x)] = \deg(x)_\infty \leq 2$. Since $k(C)$ is not rational, we conclude that $[k(C) : k(x)] = 2$.

(2) Consider now a function field of genus $g_C = 2$. For any canonical divisor $K_C \in Div(C)$, from corollary 2.1.1 of the Riemann-Roch theorem, we get that $\deg(K_C) = 2g_C - 2 = 2$ and $l(K_C) = g_C = 2$. By (1), this implies that $k(C)$ is hyperelliptic. □

If $k(C)$ is hyperelliptic and $k(x)$ is a rational subfield of $k(C)$ with $[k(C) : k(x)] = 2$, the extension $k(C)/k(x)$ is separable, see [**30**, VI.2] for more details. Hence $k(C)/k(x)$ is a cyclic Galois extension of degree 2, Indeed it is a cyclic Artin-Schreier extension if the characteristic of k is 2, and a cyclic Kummer extension otherwise. These extensions are well known and provide an explicit description of hyperelliptic curves.

3.1. Hyperelliptic curves over field of characteristic different from 2.

Let k be a perfect field of characteristic different from 2, the case where $k(C)$ is a Kummer extension of degree 2. Recall that a Kummer extension with Galois group $\mathbb{Z}/n\mathbb{Z}$ can be written as,

$$k(C) = k(x, y) \text{ with } y^n = u$$

for $k(x)$ containing a n-th root of unity, $(n, \text{char } k) = 1$ and $u \in k(x)$ satisfying the following conditions: $u \neq w^d$ for all $w \in k(x)$ and $d > 1$ dividing n. Moreover, it is well known, see [**30**, III.7.3], that for $P \in \mathcal{P}_{k(x)}$ and $P' \in \mathcal{P}_{k(C)}$ lying over P, we have

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

where $r_P := \gcd(n, \text{val}_P(u))$.

PROPOSITION 3.1.1. *Let k be a field of characteristic different from 2.*

(1) *Let $k(C)$ be a hyperelliptic function field of genus g_C. Then there exists $x, y \in k(C)$ such that $k(C) = k(x, y)$ and*

$$y^2 = f(x) \in K[x] \tag{1.2}$$

with a square-free polynomial $f(x)$ of degree $2g_C + 1$ or $2g_C + 2$.

(2) *Conversely, if $k(C) = k(x, y)$, $y^2 = f(x) \in K[x]$ with a square-free polynomial $f(x)$ of degree $m > 4$, then $k(C)$ is hyperelliptic of genus*

$$g_C = \begin{cases} (m-1)/2 & \text{if} \quad m \equiv 1 \mod 2, \\ (m-2)/2 & \text{if} \quad m \equiv 0 \mod 2. \end{cases}$$

(3) *Let $k(C) = k(x, y)$ with $y^2 = f(x)$ as in (1.2). Then the places in $\mathcal{P}_{k(x)}$ which ramify in $k(C)$ are the following:*
- *all zeros of f(x) if* $\deg(f) \equiv 0 \mod 2$;
- *all zeros of f(x) and the pole of x if* $\deg(f) \equiv 1 \mod 2$.

Hence, if $f(x)$ decomposes into linear factors, exactly $2g_C + 2$ places of $k(x)$ are ramified.

Proof: Since $k(C)$ is cyclic of degree two, there exists an element $\omega \in k(C)$ such that $k(C) = k(x, \omega)$ and $\omega^2 = u(x) \in k(x)$. To get a squarefree polynomial, write

$$u(x) = c \cdot \prod p_i(x)^{r_i} \quad , \; 0 \neq c \in K,$$

with pairwise distinct irreducible monic polynomials $p_i(x) \in K[x]$ and $r_i \in \mathbb{Z}$. Let $r_i = 2s_i + l_i$, $s_i \in \mathbb{Z}$, and $l_i \in \{0, \; 1\}$. Set

$$y := \omega \cdot \prod p_i(x)^{-s_i}.$$

Then $k(C) = k(y, x)$ and $y^2 = f(x) = p_1(x)p_2(x) \cdots p_s(x)$ a squarefree polynomial in $k[x]$, which proves the first part of (1).

Let $P_i \in \mathcal{P}_{k(x)}$ denote the zeros of $p_i(x)$, P_∞ the pole of x in $k(x)$ and m the degree of $f(x)$. Then $\mathrm{val}_{P_i}(f(x)) = 1$ and $\mathrm{val}_{P\infty}(f(x)) = -m$. The numbers r_P are easily seen to be

$$\begin{aligned}
r_{P_i} &= \quad 1 \quad \text{for } i = 1, ..., s, \\
r_{P_\infty} &= \begin{cases} 1 & \text{if } m \equiv 1 \mod 2, \\ 2 & \text{if } m \equiv 0 \mod 2, \end{cases} \\
r_P &= \quad 2 \quad \text{for all the other places.}
\end{aligned}$$

Since $e(P_i|p_i) = \frac{n}{r_{P_i}}$, this gives us exactly the ramification points needed in (3). By the Hurwitz formula and some manipulations we get

$$\begin{aligned}
2g_{k(C)} - 2 &= (2g_{k(x)} - 2)[k(C) : k(x)] + \deg\ \mathrm{Diff}(k(D)/k(C)) \\
&= (2 \cdot 0 - 2) \cdot 2 + \sum_{P \in \mathbb{P}_{k(x)}} (n - r_p) \deg P, \\
&= \begin{cases} -4 + \sum_{i=1}^{s} \deg P_i + 1 & \text{if} \quad m \equiv 1 \mod 2, \\ -4 + \sum_{i=1}^{s} \deg P_i & \text{if} \quad m \equiv 0 \mod 2. \end{cases} \\
&= \begin{cases} m - 3 & \text{if} \quad m \equiv 1 \mod 2, \\ m - 4 & \text{if} \quad m \equiv 0 \mod 2. \end{cases}
\end{aligned}$$

Thus the degree of the polynomial $f(x)$ is either $2g + 1$ or $2g + 2$ and this allows us to conclude the proposition. $\square$

Over an algebraically closed field, the relations above give the following affine model for C

$$C: \ y^2 = f(x) = \prod_{i=1}^{2g+2} (x - \lambda_i).$$

This model is called the *Rosenhain normal form* and is given by the $2g + 2$ distinct Weierstrass points. A complete smooth model for C is obtained by gluing this affine curve to the affine curve given by the equation

$$v^2 = f^*(u) := u^d f(u^{-1}),$$

where $d = \deg(f)$ if $\deg(f)$ is even, and $d = \deg(f) + 1$ otherwise. The two affine subsets of C are glued together using the map

$$(u, v) \to (x^{-1}, yx^{-d/2}).$$

3.2. Hyperelliptic curves over a field of characteristic 2.

We now consider the situation where char $k = 2$, the case of an Artin-Schreir extension. Recall that in such an extension

$$k(C) = k(y, x) \text{ with } y^p - y = u,$$

for $u \in k(x)$ satisfying $u \neq w^p - w$ for all $w \in k(x)$ and p the characteristic of the field. In this situation, all ramified places of $k(x)$ in the quadratic extension are wildly ramified and one can show that the number of such places, say s, lies in the range $1 \leq s \leq g + 1$, where we can find an example for each integer [**30**, VI.2]. Such hyperelliptic curves have an affine model given by

$$y^2 - y = f(x)$$

and their behavior is less known and more difficult to understand then that of hyperelliptic curves defined over fields of odd characteristic. In our study of hyperelliptic curves, we will restrict ourselves to the simpler situation, when the field k has odd characteristic.

3.3. The hyperelliptic involution.

PROPOSITION 3.3.1. *Consider a hyperelliptic function field $k(C)$ of genus g_C and a rational subfield $k(x) \subset k(C)$ with $[k(C) : k(x)] = 2$. Then all rational subfield $k(z) \subset k(C)$ with $[k(C) : k(z)] \leq g_C$ are contained in $k(x)$. In particular, $k(x)$ is the only rational subfield of $k(C)$ with $[k(C) : k(x)] = 2$.*

To prove the above proposition we will need to use Riemann's inequality that gives the following estimate for the genus of a function field. A proof can be found in [**30**, III.10.4].

Riemann's inequality: Let $F = k(x, y)$ then

$$g \leq ([F : k(x)] - 1) \cdot ([F : k(y)] - 1).$$

Proof of the proposition: Suppose that $[k(C) : k(z)] \leq g_C$ but $z \notin k(x)$. Then $k(C) = k(x, z)$, and by the Riemann's inequality,

$$g_C \leq ([k(C) : k(x)] - 1) \cdot ([k(C) : k(z)] - 1).$$

On the other hand,

$$([k(C) : k(x)] - 1) \cdot ([k(C) : k(z)] - 1) \leq (2 - 1) \cdot (g_C - 1) = g_C - 1.$$

a contradiction. □

PROPOSITION 3.3.2. *Let C be an hyperelliptic curve over k, a field of odd characteristic.*

1. *There exists a unique canonical involution $\iota : C \longrightarrow C$, characterized by inducing a non-trivial automorphism of $k(C)$ over its unique rational subfield of index two.*
2. *The fixed points of ι are the Weierstrass points of C.*
3. $\iota \in Z(Aut(C))$.
4. *Let $f, g : C \longrightarrow \mathbb{P}^1$ be double coverings, then $f = \frac{ag+b}{cg+d}$ for some invertible matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in PGL_2(k)$.*

Proof:

$(1), (2)$ We see easily that the map

$$\begin{aligned} \iota : C &\longrightarrow C \\ (x, y) &\mapsto (x, -y) \end{aligned}$$

is the one we are looking for. Note that if C has two points at infinity, that is when C is given by an even degree polynomial, ι permutes the two points; and if C has a single point at infinity, ι fixes it. Clearly ι induces a non-trivial automorphism ι^* of $k(C)$ that fixes $k(x)$ and the uniqueness follows from $[k(C) : k(x)] = 2$. Thus, the fixed points of ι are the ones of the form $(x, 0)$ and, depending of the situation, the point at infinity. These points are exactly the ramification points of the double covering of the projective line.

(3) Let $\pi : C \longrightarrow \mathbb{P}^1$ be a double cover, to avoid confusion we will denote the rational field $k(\pi^*(x))$, and we have $[k(C) : k(\pi^*(x))] = 2$. Consider j, any automorphism of C, similarly, from the double cover $\pi \circ j : C \longrightarrow \mathbb{P}^1$ we have $[k(C) : k(j^*\pi^*(x))] = 2$, thus, by Proposition 3.3.1, $k(\pi^*(x)) = k(j^*\pi^*(x))$. But $k(j^*\pi^*(x)) = j^*(k(\pi^*(x))$ therefore j^* preserves $k(\pi^*(x))$. It follows that the automorphism $j^*\iota^*(j^*)^{-1}$ is trivial on $k(\pi^*(x))$, thus by (1), $j\iota j^{-1} = \iota$, which means that the involution commutes with any element of $\mathrm{Aut}(C)$.

(4) Note first that double coverings correspond to embeddings

$$k(x) \hookrightarrow k(C).$$

If $K = k(x)$ is the unique rational subfield contained in $k(C)$, since $k(x) \subseteq K$, every embedding f^* factors through K

$$\begin{array}{ccc} k(x) & \overset{f^*}{\hookrightarrow} & k(C) \\ \sigma \downarrow & \nearrow g^* & \\ K & & \end{array}$$

and therefore we have that $f^* = g^* \circ \sigma$ for $\sigma \in \mathrm{Aut}(k(x)) = PGL_2(k)$. $\square$

DEFINITION 3.3.1. *For $S \subseteq \mathbb{P}^1$ we will define*

$$\mathrm{Aut}(\mathbb{P}^1, S) = \{\sigma \in \mathrm{Aut}(\mathbb{P}^1) \mid \sigma(S) \subseteq S\}$$

the subgroup of the automorphism group of $\mathbb{P}^1$ fixing S.

COROLLARY 3.3.1. *Let C_i be hyperelliptic curves, S_i be the set of ramification points of the double cover $C_i \xrightarrow{f_i} \mathbb{P}^1$. Then:*

(1) $C_1/\overline{k} \cong C_2/\overline{k} \quad \Leftrightarrow \exists \nu \in PGL_2(\overline{k})$ *such that* $\nu(S_1) = S_2$.

(2) *There is an exact sequence*

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{a} \mathrm{Aut}(C) \xrightarrow{b} \mathrm{Aut}(\mathbb{P}^1, S_1) \longrightarrow 0, \tag{1.3}$$

where $a(1) = \iota$.

Proof: (1) Suppose first that $C_1/\overline{k} \overset{\sigma}{\cong} C_2/\overline{k}$. Considering the associated function fields, we have the following picture

$$\begin{array}{ccc} k(C_2) & \xrightarrow{\sigma^*} & k(C_1) \\ \uparrow \pi_2^* & & \uparrow \pi_1^* \\ k(x) & & k(x) \end{array}$$

Therefore $\sigma^* \circ \pi_2^*$ and π_1^* are two maps from $k(x)$ to $k(C_1)$, thus, by the above proposition, differ by an automorphism $\nu* : k(x) \longrightarrow k(x)$, giving the commutative diagram

$$\begin{array}{ccc} C_1 & \xrightarrow{\sigma} & C_2 \\ \downarrow \pi_1 & & \downarrow \pi_2 \\ \mathbb{P}^1 & \xrightarrow{\nu} & \mathbb{P}^1 \end{array}$$

which clearly sends the image of Weierstrass points of C_1 to the one of C_2.

Conversely, suppose that we have the following picture

$$\begin{array}{ccc} C_1 & & C_2 \\ \downarrow \pi_1 & & \downarrow \pi_2 \\ \mathbb{P}^1 & \xrightarrow{\nu} & \mathbb{P}^1 \end{array}$$

with $\nu(S_1) = S_2$. It will induce a map between $k(C_2)$ to $k(C_1)$ provided by $\nu^* \in \mathrm{Aut}(k(x))$. The function fields of these curves can by given as

$$k(C_1) = k(x)[y] \quad \text{for } y^2 = f(x) = \prod_{i=1}^{2g+2}(x - \alpha_i)$$

$$k(C_2) = k(x)[z] \quad \text{for } z^2 = g(x) = \prod_{i=1}^{2g+2}(x - \beta_i),$$

and we can consider the map

$$\begin{aligned} \sigma^* : \quad k(C_2) &\longrightarrow k(C_1) \\ x &\mapsto \nu^*(x) \\ z^2 &\mapsto \sigma^*(g(x)) = \prod_{i=1}^{2g+2}(\nu^*(x) - \beta_i). \end{aligned}$$

Since $\sigma^* g(x)$ is a degree $2g+2$ polynomial sharing the same roots with $f(x)$, that is the α_i's, we can assume without lost of generalities by adjusting y that $f(x) = \sigma^*(g(x))$. Thus by specifying the image of z (we have the choice between $\sigma^*(z) = y$ and $\sigma^*(z) = -y$) the map σ^* is a well defined morphism.

(2) Note that b is well defined since from the first part of the corollary, every automorphism of C must fix the set of ramification points. The injectivity of a is trivial and $Im(a) = \mathrm{Ker}(b)$ since ι^* is the unique non-trivial automorphism of $k(C)$ over its rational subfield $k(x)$. The surjectivity of b is again immediate from the first part of this corollary. $\square$

4. Moduli spaces

In a sense it is possible to parameterize isomorphism classes of hyperelliptic curves of a given genus with their Weierstrass points. We will try to solve the "Moduli problem" for these objects, *i.e.* we will try to give the parameter space some structure close to the structure of the objects we want to study. Before we dive into the particular case of hyperelliptic curves, we first need to be comfortable with the general settings of the moduli problem. For this section, we will assume that the reader is familiar with the language of schemes and categories.

4.1. General moduli spaces.

To state a moduli problem we can consider several categories $\mathcal{C}$ of schemes. In order to state it correctly, these categories will need to have fibered products and products. To have a notion of continuity in our parameterization, we will work with *families* of objects in $\mathcal{C}$. Recall that families are flat morphisms of schemes $\pi : \mathcal{X} \longrightarrow S$ such that for each $s \in S$ the scheme theorical fiber $\mathcal{X}_s := Spec(k(s)) \times_S \mathcal{X}$ is an object of $\mathcal{C}$. Such a scheme S is called a *parameter space*. Furthermore, we will expect our category to be equipped with an equivalence relation $\sim$ that can be extended to any family parameterized by an object in $\mathcal{PS}$, the category of *parameter spaces*. By solving the moduli problem for $(\mathcal{C}, \sim, \mathcal{PS})$ we will try to parameterize the objects in $\mathcal{C}$ (a subcategory of $\mathcal{PS}$) in a kind of continuous way up to the equivalence relation . Now let

$$\Phi : \mathcal{PS} \longrightarrow (\text{Sets})$$

be the map which associates to each $S \in \mathcal{PS}$ the set $\Phi(S)$ containing all the equivalence classes of families of objects in $\mathcal{C}$ parameterized by S. One can show that this is functorial and we can introduce a first type of moduli space.

DEFINITION 4.1.1. *The functor*

$$\Phi : \mathcal{PS} \longrightarrow (sets),$$

is said to be representable in $\mathcal{PS}$ *if there exists* $\mathcal{M} \in Obj(\mathcal{PS})$ *such that the functor* Φ *is isomorphic to the functor* $\mathrm{Hom}_{\mathcal{PS}}(\ \cdot\ , \mathcal{M})$. *In such a case,* $\mathcal{M}$ *is said to be a fine moduli space for the moduli problem* $(\mathcal{C}, \sim, \mathcal{PS})$.

In particular, this means that for each $S \in Obj(\mathcal{PS})$ there exists a set bijection :

$$\Phi(S) \longleftrightarrow \mathrm{Hom}_{\mathcal{PS}}(S, \mathcal{M}),$$

i.e. each class of families parameterized by S corresponds to one and only one morphism between S and $\mathcal{M}$. Thus, for any family defined over a scheme S, there is a morphism ψ such that the object in the family over the geometric point $s \in S$ will correspond, via the morphism, to a point $\psi(s) \in \mathcal{M}$. Conversely, given any morphism from a scheme in $\mathcal{PS}$ to $\mathcal{M}$, it will be possible to find a family of objects over that scheme with the same correspondence between objects in $\mathcal{C}$ and points in $\mathcal{M}$. One can find in [**4**, §2.1] that we have an equivalent notion of fine moduli space.

DEFINITION 4.1.2. *A fine moduli space for the problem* $(\mathcal{C}, \sim, \mathcal{PS})$ *is an object* $\mathcal{M} \in Obj(\mathcal{PS})$ *together with a family* $\mathcal{U} \longrightarrow \mathcal{M}$ *which is universal in the following sense. For each family* $\pi : \mathcal{X} \longrightarrow S$ *there in an unique morphism* $f \in \mathrm{Hom}_{\mathcal{PS}}(S, \mathcal{M})$ *such that* $\mathcal{X} = S \times_{\mathcal{M}} \mathcal{U} := f^*(\mathcal{U})$.

In the simpler language of varieties, we are seeking a variety $\mathcal{M}$ parameterizing $\mathcal{C}$, a category of varieties. A family over a variety B is a surjective algebraic map $\pi : X \longrightarrow B$ where the fiber $X_b = \pi^{-1}(b)$ is a variety in $\mathcal{C}$. To pose the moduli problem, we consider $\mathcal{C}$ a category of varieties with $\sim$ an equivalence relation that can be extend to $\mathcal{PS}$, the category of the parameter space. In this setting $\mathcal{M}$ will be a fine moduli space for $(\mathcal{C}, \sim, \mathcal{PS})$ if for any variety B in $\mathcal{PS}$ we have a correspondence between morphisms ϕ from B to $\mathcal{M}$ and families $\pi : X \longrightarrow B$. According to this correspondence, for each point $b \in B$, its image $\phi(b)$ in the moduli space will corresponds to the variety X_b in our family. We then have a correspondence between the points on the moduli space and the varieties considered. The possibility to use this correspondence for the inclusion map $N \hookrightarrow \mathcal{M}$ for any subvariety of $\mathcal{M}$ gives a kind of continuity. Note that according to the second version of a fine moduli space, the solution to the problem is a universal family $\pi : \mathcal{U} \longrightarrow \mathcal{M}$ on which each fiber is a variety in the category $\mathcal{C}$.

The functor Φ is not representable in general. Usually, the obstruction is created by objects in $\mathcal{C}$ admitting non-trivial automorphisms. However, more frequently, there exists a coarse solution for this problem.

DEFINITION 4.1.3. *A coarse moduli space for the moduli problem $(\mathcal{C}, \sim, \mathcal{PS})$ is an object $\mathcal{M} \in Obj(\mathcal{PS})$ for which there is a natural transformation of functors,*

$$\Psi_{\mathcal{M}} : \Phi \longrightarrow \mathrm{Hom}_{\mathcal{PS}}(\ \cdot\ , \mathcal{M}),$$

such that:

(1) *For an algebraically closed field $\overline{k}$,*

$$\Psi_{\mathcal{M}} : \Phi_{\mathcal{M}}(Spec(\overline{k})) \longrightarrow \mathrm{Hom}_{\mathcal{PS}}(Spec(\overline{k}), \mathcal{M})$$

is bijective;

(2) *For any $N \in Obj(\mathcal{PS})$ and any natural transformation of functors*

$$\Psi_N : \Phi \longrightarrow \mathrm{Hom}_{\mathcal{PS}}(\ \cdot\ , N),$$

there is an unique transformation of functors

$$\mathcal{K} : \mathrm{Hom}_{\mathcal{PS}}(\ \cdot\ , \mathcal{M}) \longrightarrow \mathrm{Hom}_{\mathcal{PS}}(\ \cdot\ , N),$$

making commutative the following diagram of natural transformations of functors:

$$\begin{array}{ccc} \Phi & \xrightarrow{\Psi_{\mathcal{M}}} & \mathrm{Hom}_{\mathcal{PS}}(\,\cdot\,,\mathcal{M}) \\ & \searrow^{\Psi_N} & \downarrow \mathcal{K} \\ & & \mathrm{Hom}_{\mathcal{PS}}(\,\cdot\,,N). \end{array}$$

In the language of varieties, we still have correspondence between points on the moduli space with varieties in the fixed category. But given a map from $B \in Obj\mathcal{PS}$ to $\mathcal{M}$ there is not necessarily a corresponding family over B. As a matter of fact, the coarse moduli space is as close as possible to be a fine moduli space.

We can consider a simple example of a fine moduli space. Let $\mathcal{C}$ be the category of finite sets, the equivalence relation given by

$$S \sim R \Leftrightarrow |S| = |R|$$

and $\mathcal{PS}$ the category of all sets. The set $\mathbb{N}$ is a fine moduli space for the problem $(\mathcal{C}, \sim, \mathcal{PS})$ and the universal family $\mathcal{U} \longrightarrow \mathbb{N}$ is given by attaching the set $\mathcal{U}_n = \{0, 1, ..., n-1\}$ over the integer $n \in N$. Notice that the presence of non-trivial automorphisms on some of the objects in the category, (finite sets certainly have non-trivial automorphisms) does not necessarily implies that there is no fine solution to the moduli problem.

In general, if there is only a coarse moduli space for the objects we want to study, we can put some extra structure on them to get rid of any non-trivial automorphisms and then often get a fine moduli space. For instance, for the category of curves we can label a sufficient number of points on the curves to avoid automorphisms.

LEMMA 4.1.1. *Let T be a non-trivial automorphism of the genus g curve C, then T has at most $2g+2$ fixed points*

Proof: For any automorphism T, it is clear that $\mathrm{Fix}(T)$, the set of fixed points is a finite set. Choose $P \in C$ such that $T(P) \neq P$ and by the Riemann-Roch theorem we have that

$$\begin{aligned} l(r[P]) &= r - g + 1 + l(K_c - r[P]) \\ &\geq r - g + 1 \geq 2 \quad \text{if} \quad r \geq g + 1. \end{aligned}$$

If we take $r = g+1$ and $f \in \mathcal{L}(r[P])$ non-constant we get $(f)_\infty = nP$ for $1 \leq n \leq g+1$. Consider then $h = f - f \circ T$. We have $(h)_\infty = n[P] + n[T^{-1}(P)]$. Therefore we get that $\deg((h)_0) = 2n \leq 2g + 2$ and since $Fix(T) \subset (h)_0$, we can conclude the proposition. $\square$

Thus, for $n > 2g + 2$, a genus g curve with n marked points does not admit non trivial automorphisms. There are several ways to introduce a *level structure* and we will consider some of them for the particular case of hyperelliptic curves in a later section.

4.2. Moduli space for curves.

For the special case of curves we first fix a base scheme S, usually $S = Spec(k)$ for k a field, and the parameter space $\mathcal{PS}$ is Sch_S, the category of all schemes over S. The objects we are interested in parameterizing are the objects in $\mathcal{C}(g)$, the category of smooth projective curves of genus g over S. The equivalence relation is given by isomorphism of curves. For a fixed scheme S, a *curve of genus g over S* is a morphism of schemes $C \longrightarrow S$ which is proper, flat and such that all geometric fibers are irreducible smooth projective curve of genus g. If C_1 and C_2 are curves over S, they are said to be isomorphic as curves over S if there is an isomorphism

$f : C_1 \longrightarrow C_2$ making the following diagram commutative

$$\begin{array}{ccc} C_1 & \xrightarrow{\text{f}} & C_2 \\ \downarrow & & \downarrow \\ S & = & S. \end{array}$$

One can ask if the functor

$$\Phi_g : \mathrm{Sch}_S \longrightarrow (Sets),$$

defined by:

$$\Phi_g(T) = \{ \text{ Isomorphism classes of curves } \pi : \mathcal{X} \longrightarrow T \ \text{ of genus } g\},$$

is representable, *i.e.*, if there is a scheme $\mathcal{M}_g$ over S such that the functor $\Phi_g(\ \cdot\ )$ is isomorphic to the functor $\mathrm{Hom}_{\mathrm{Sch}_S}(\ \cdot\ , \mathcal{M}_g)$. We remark that there are plenty of curves having non-trivial automorphisms. Therefore, as noted before, we can expect that there is no fine moduli space for this problem. However, it is known [**11**] that this moduli problem only has a coarse solution and the coarse moduli space has dimension $3g - 3$.

For instance, the coarse moduli space of elliptic curves is known as the *Weierstrass absolute invariant* j, also named the j-*line*. For a field of characteristic $p > 3$, we may assume that the elliptic curve has a Weierstrass equation of the form

$$y^2 = x^3 + Ax + B.$$

Then the j-invariant is explicitly given by

$$j = 1728(4A)^3/\Delta \quad \text{where} \quad \Delta = -16(4A^4 + 27B^2).$$

It is an invariant of the isomorphism class of the curve, and it does not depend on the particular equation chosen.

One can easily see that the j-line is not a fine moduli space. For instance we can consider the quadratic twist. The two curves associated to the affine model:

$$y^2 = x^3 + ax + b$$
$$dy^2 = x^3 + ax + b$$

are isomorphic over the the field $\mathbb{Q}(\sqrt{d})$, thus they have the same j-invariant. But with some work, one can show that if d is not a square, the two curves are not isomorphic over the field $\mathbb{Q}$ while they share the same invariant. Furthermore, over an algebraically closed field, one can find in [**29**, III,§1] that two elliptic curves are isomorphic if and only if they have the same j-invariant. For a description of this invariant in characteristic 2 and 3 see [**29**, Appendix A].

The particular case of genus 2 curves, which are all hyperelliptic, has been considered by Igusa in [**10**] and can be given explicitly in every characteristic. Recall that a curve defined over a field of odd characteristic can be described by its Rosenhain normal form:

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3).$$

If the characteristic of the field is 2, the curve C can be given by the *normal forms*

$$y^2 - y = \begin{cases} \alpha x + \beta x^{-1} + \gamma(x-1)^{-1} \\ x^3 + \alpha x + \beta x^{-1} \\ x^5 + \alpha x^3. \end{cases}$$

To define its moduli space, Igusa worked with the *universal normal form*

$$xy^2 + (1 + ax + bx^2)y + x^2(c + dx + x^2) = 0$$

which is valid for every characteristic. Note that now this form depends on four, instead of three variables and one can recover quite easily our previous forms from this one. The moduli space of hyperelliptic curves in characteristic different from two is closely connected with projective invariants of binary sextics. And surprisingly this connection also holds in characteristic 2 if we work with the universal normal form.

For a sextic $u_0x^6 + u_1x^5 + ... + u_6 = u_0 \prod_{i=1}^{6}(x - \alpha_i)$, if we abbreviate $(\alpha_i - \alpha_j)$ by (ij), the following expressions

$$\begin{aligned}
A(f) &= u_o^2 \sum (12)^2(34)^2(56)^2, \\
B(f) &= u_0^4 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \\
C(f) &= u_0^6 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2, \\
D(f) &= u_0^{10} \prod_{i<j} (ij)^2,
\end{aligned}$$

define homogeneous integral invariants and $D(f)$ is the discriminant of the sextic. We can evaluate these expressions for the following polynomial,

$$(1 + ax + bx^2)^2 - ax^3(c + dx + x^2),$$

which is the sextic of Weierstrass points associated to universal normal form.

In characteristic 2, the Weierstrass points behave badly under reduction modulo 2, thus these integral invariants are not adequate. Instead we need to consider *arithmetic invariants* which are rational invariants whose value at the above sextic has integral coefficients as a polynomial in a, b, c, d. Note that according to this new definition, every integral invariant is an arithmetic invariant. Igusa introduced the five basic invariants,

$$\begin{aligned}
&J_2 = 2^{-3}A && J_4 = 2^{-5}3^{-1}(4J_2^2 - B) \\
&J_6 = 2^{-6}3^{-2}(8J_2^3 - 160J_2J_4 - C) && J_8 = 2^{-2}(J_2J_6 - J_4^2) \\
&J_{10} = 2^{-12}D
\end{aligned}$$

and showed that they make sense for every characteristic. The moduli space of genus 2 curves he described is $\mathcal{H}_2 := Spec(R)$, where R is the ring of invariant elements of $\mathbb{Z}[y_1, y_2, y_3, y_4]$ under the transformation $y_i \mapsto \xi^i y_i$, where ξ is a fifthroot of unity,

y_1, y_2, y_3 are some independent variables over $\mathbb{Q}$ and $y_4 = \frac{1}{4}(y_1 y_3 - y_2^2)$. The elements in R are named the *absolute invariants* and we have the following correspondence

$$J_2^{e_1} J_4^{e_2} J_6^{e_3} J_8^{e_4} J_{10}^{-e_5} \longrightarrow y_1^{e_1} y_2^{e_2} y_3^{e_3} y_4^{e_4} y_5^{-e_5},$$

in which the e_i are non-negative integers satisfying $e_1 + 2e_2 + 3e_3 + 4e_4 = 5e_5$. Furthermore, R is an integrally closed noetherien integral domain over $\mathbb{Z}$ with 10 generators that can be given explicitly. For instance we can take

$$\begin{array}{ccccc} J_2^5 J_{10}^{-1}, & J_2^3 J_4 J_{10}^{-1}, & J_2^2 J_6 J_{10}^{-1}, & J_2 J_8 J_{10}^{-1}, & J_4 J_6 J_{10}^{-1}, \\ J_4 J_8^2 J_{10}^{-2}, & J_6^2 J_8 J_{10}^{-2}, & J_6^5 J_{10}^{-3}, & J_6 J_8^3 J_{10}^{-3}, & J_8^5 J_{10}^{-4}. \end{array}$$

4.3. Moduli space for hyperelliptic curves.

Our main concern here is to understand the moduli problem for hyperelliptic curves of a fixed genus. Later on we will consider some particular hyperelliptic curves and we will try to describe the subset of the coarse moduli space associated to these special curves. We consider the functor

$$\Phi_{Hg} : \mathrm{Sch}_S \longrightarrow (\mathrm{Sets})$$

defined by:

$$\Phi_{Hg}(T) = \{ \text{ Isomorphism classes of hyperelliptic curves } \pi : \mathcal{X} \longrightarrow T \text{ of genus } g \}$$

and try to relate it to a coarse moduli space H_g.

In order to get concrete results, we will only consider curves defined over k, an algebraically closed field of odd characteristic. We have seen in our study of hyperelliptic curves that these curves can be associated with the space of non-ordered $(2g+2)$-tuples of distinct points in $\mathbb{P}^1(k)$. These ramification points are the image of the Weierstrass points under the covering of the projective line and we will also refer to them as Weierstrass points. We have seen in Corollary 3.3.1 that two curves over

k are isomorphic if there exists $\mu \in PGL_2(k)$ sending the Weierstrass points of one curve to those of the other.

For any curve, we can label the Weierstrass points to get an element $W' = [\lambda_1, \lambda_2, ..., \lambda_{2g+2}]$ of $\mathbb{P}^1(k)^{2g+2} \setminus \Delta =: H_g^{**}$ where $\Delta = \mathcal{Z}(\prod_{i \neq j}(x_i - x_j))$. The symmetric group Σ_{2g+2} acts on H_g^{**} by permuting the Weierstrass points and $PGL_2(k)$ acts on it componentwise. Therefore these two actions commute and H_g, the parameter space of the hyperelliptic curves, can be described as

$$H_g = (\mathbb{P}^1(k)^{2g+2} \setminus \Delta)/PGL_2(k) \times \Sigma_{2g+2},$$

which is isomorphic to

$$[(\mathbb{P}^1(k)^{2g+2} \setminus \Delta)/PGL_2(k)]/\Sigma_{2g+2}.$$

We can focus for the moment on $H_g^* = [(\mathbb{P}^1(k)^{2g-2} \setminus \Delta)/PGL_2(k)]$ and one can use an appropriate and unique element of $PGL_2(k)$ to force the first three Weierstrass points to be $[0, 1, \infty]$. We get this way a representative for each classes and this representative is described by the remaining $2g - 1$ points. Thus we have

$$H_g^* = (\mathbb{P}^1(k) \setminus \{0, 1, \infty\})^{2g-1} \setminus \Delta',$$

where

$$\Delta' = \{\ [x_1, ...x_{2g-1}] \mid x_i = x_j \text{ for } i \neq j\ \}.$$

This quasi-projective variety is not the space we are looking for. Indeed, a permutation of the labeled points will give different elements in H_g^* but will represent the same hyperelliptic curve. Therefore, to get a better description of H_g, we will need to erase the marking done previously using the action of the symmetric group Σ_{2g+2} on H_g^*.

Proposition 4.3.1. *Let H_g^* be the quasi-projective variety $(\mathbb{P}^1(k) \setminus \{0, 1, \infty\})^{2g-1} \setminus \Delta'$, then there is an action of Σ_{2g+2} on H_g^*.*

Proof: Consider first $x = [x_1, ..., x_{2g-1}] \in H_g^*$, there exists at least one element in $H_g^{**} = \mathbb{P}^1(k)^{2g+2} \setminus \Delta$, say $\lambda = [\lambda_1, ...\lambda_{2g+2}]$, associated to x and such that

$$x_i = \psi(\lambda_{i+3}) \quad \text{for} \quad \psi(x) = \frac{(\lambda_1 - x)(\lambda_3 - \lambda_2)}{(\lambda_3 - x)(\lambda_1 - \lambda_2)} \in PGL_2(k).$$

The permutation $\sigma \in \Sigma_{2g+2}$ acts on x by $x^\sigma = [x_1^\sigma, ...x_{2g-1}^\sigma]$ where

$$x_i^\sigma = \psi^\sigma(\lambda_{i+3}) \quad \text{for} \quad \psi^\sigma(x) = \frac{(\sigma(\lambda_1) - \sigma(x))}{(\sigma(\lambda_3) - \sigma(x))}\frac{(\sigma(\lambda_3) - \sigma(\lambda_2))}{(\sigma(\lambda_1) - \sigma(\lambda_2))} \in PGL_2(k).$$

We need to show that this action is well defined. Indeed suppose that we have two elements in H_g^{**}, say $\lambda = [\lambda_1, ..., \lambda_{2g+2}]$ and $\lambda' = [f(\lambda_1), ..., f(\lambda_{2g+2})]$ for $f \in PGL_2(k)$, which are associates to x. If we consider the action of σ through λ', the element x^σ is given by

$$x_i^\sigma = \psi^{\sigma'}(\lambda_{i+3}) \quad \text{for} \quad \psi^{\sigma'}(x) = \frac{\sigma(f(\lambda_1)) - \sigma(f(x))}{\sigma(f(\lambda_3)) - \sigma(f(x))}\frac{\sigma(f(\lambda_3)) - \sigma(f(\lambda_2))}{\sigma(f(\lambda_1)) - \sigma(f(\lambda_2))}.$$

Since the two action commutes and the cross-ratio is stable under $PGL_2(k)$, the map ψ' can be written as

$$\begin{aligned}
\psi^{\sigma'}(x) &= \frac{f(\sigma(\lambda_1) - f(\sigma(x))}{f(\sigma(\lambda_3)) - f(\sigma(x))}\frac{f(\sigma(\lambda_3)) - f(\sigma(\lambda_2))}{f(\sigma(\lambda_1)) - f(\sigma(\lambda_2))} \\
&= \frac{\sigma(\lambda_1) - \sigma(x)}{\sigma(\lambda_3) - \sigma(x)}\frac{\sigma(\lambda_3) - \sigma(\lambda_2)}{\sigma(\lambda_1) - \sigma(\lambda_2)} \\
&= \psi^\sigma(x).
\end{aligned}$$

One easily verifies that we have $id(x) = x$ and $(\sigma\tau)(x) = \sigma(\tau(x))$. □

Since a finite group acting on a quasi-projective variety leads to a quotient which is also a quasi-projective variety, the set

$$H_g = [(\mathbb{P}^1(k) \setminus \{0, 1, \infty\})^{2g-1} \setminus \Delta']/\Sigma_{2g+2}$$

is also a variety. In fact, it will be the coarse moduli space of our moduli problem. As stated before, there is no fine solution for this problem and one can find a proof of this in [**25**]. Note that the dimension of H_g is $2g-1$ and this agrees with the fact that all genus 2 curves are hyperelliptic.

4.4. Level structure on hyperelliptic curves.

To simplify the moduli space associated to hyperelliptic curves and to be able to parameterize some coverings, we will add some level structure on H_g. For instance, among the Weierstrass points, one can fix a non-ordered m-tuple of points, and consider H_g^m the moduli space of (C,s) where $s \in S_m := \{\ s\ :\ |s| = m \text{ and } s \subset W_C\ \}$, *i.e.*, the genus g hyperelliptic curves together with a choice of m Weierstrass points (not labeled). This new moduli space can be describe as:

$$H_g^m = [([\mathbb{P}^1(k)^{2g+2-m} \times \mathbb{P}^1(k)^m] \setminus \Delta)/PGL_2(k)]/\Sigma_{2g+2-m} \times \Sigma_m,$$

where $PGL_2(k)$ acts componentwize and $\Delta = \mathcal{Z}(\prod_{i\neq j}(x_i - x_j))$.

For a curve C in H_g there are $\binom{2g+2}{m}$ ways to pick a set s of m Weierstrass points, thus the map $\rho : H_g^m \longrightarrow H_g$ has degree $\binom{2g+2}{m}$. This map will be ramified if C admits particular automorphisms. Two elements (C,s_1) and (C,s_2) in H_g^m with $s_1 \neq s_2$ will be isomorphic if there is $\phi \in PGL_2(k)$ that sent W to itself and s_1 to s_2. Remark that if we consider a curve C with a set of Weierstrass points $W = \{\lambda_1, ..., \lambda_{2g+2}\}$ and $\psi \in \mathrm{Aut}(C)$, by Corollary 3.3.1 we have necessarily that $\psi(W) = W$, *i.e.*, the map permutes the Weierstrass points. Since the involution ι is trivial on the Weierstrass points, we will only consider the elements in $\mathrm{Aut}(C)/ < \iota >=: Aut(C)^*$ named the *reduced automorphism group*. From the same corollary, the isomorphism ϕ corresponds to an automorphism in the reduced group that sends s_1 to s_2.

We therefore have an action of $\mathrm{Aut}(C)^*$ on S_m that induces trivially an action on $\rho^{-1}(C)$ the fiber of the map $\rho : H_g^m \longrightarrow H_g$. If $\mathrm{Aut}(C)^*$ is not empty, there will exist elements in the fiber that were a priori distinct but will be associated by $\phi \in \mathrm{Aut}(C)^*$. In this situation, the map ρ will be ramified over the curve C.

LEMMA 4.4.1. *Let $\rho^{-1}(C)$ the fiber of the map $\rho : H_g^m \longrightarrow H_g$ over C and $m \neq 2g+2$, then the action of $\mathrm{Aut}^*(C)$ on $\rho^{-1}(C)$ is faithful.*

Proof: For any automorphism ψ in $\mathrm{Aut}(C)^*$, from Corollary 3.3.1, there exists $x \in W$ such that $\psi(x) \neq x$. If $m \neq 2g+2$ there is at least one set $s \in S_m$ containing x but not $\psi(x)$, thus ψ acts non-trivially on (C, s). Therefore, the kernel of this action is the identity, hence the action is faithful. □

We denote by $\mathrm{Aut}(C)^*_s$ the elements in $\mathrm{Aut}(C)^*$ that send the set $s \in S_m$ to itself and we can state the following.

LEMMA 4.4.2. *Let $\rho^{-1}(C)$ the fiber of the map $\rho : H_g^m \longrightarrow H_g$ over C, then*

1. *the elements of the fiber $\rho^{-1}(C)$ correspond to the orbits of the action of $\mathrm{Aut}(C)^*$ on S_m;*
2. *the stabilizer of $(C, s) \in \rho^{-1}(C)$ (also of $s \in S_m$)in $\mathrm{Aut}(C)^*$ is $\mathrm{Aut}(C)^*_s$.*

Proof: (1) Consider (C, s_1) and (C, s_2) two elements in the fiber of C where $s_1 \neq s_2$, they will correspond to the same element in H_g^m if and only if there is $\phi \in \mathrm{Aut}(C)^*$ such that $\phi(s_1) = s_2$ that is, if and only if they are in the same orbit.

(2) Clear from the definition of $\mathrm{Aut}(C)^*_s$. □

Another way to put a level structure on hyperelliptic curves is to label the Weierstrass points by $\Psi := \{\ \hat{s} \mid \hat{s} : \{1, 2, ..., 2g+2\} \xrightarrow{\cong} Wc\}$. Once the points are labeled, as we have seen, one can send the first three points to $[0, 1, \infty]$ and we get a moduli space encountered before

$$H_g^* = (\mathbb{P}^1(k) \setminus \{0, 1, \infty\})^{2g-1} \setminus \Delta'.$$

The map $\rho_1 : H_g^* \longrightarrow H_g$ has degree $(2g+2)!$ and again this map will be ramified if the curve admits an automorphism beside the hyperelliptic involution. Two elements $(C, \hat{s}_1)$ and $(C, \hat{s}_2)$ in H_g^* with $\hat{s}_1 \neq \hat{s}_2$ will be isomorphic if there is $\phi \in PGL_2(k)$ that sent $\hat{s}_1$ to $\hat{s}_2$, that is if $\phi \in \mathrm{Aut}(C)^*$ and send $\hat{s}_1$ to $\hat{s}_2$. Again the action of $\mathrm{Aut}(C)^*$ on Ψ is faithful and induces naturally an action on $\rho_1^{-1}(C)$. Similarly we have the following:

LEMMA 4.4.3. *Let $\rho_1^{-1}(C)$ the fiber of the map $\rho_1 : H_g^* \longrightarrow H_g$ over C, then:*

(1) *the elements of the fiber $\rho_1^{-1}(C)$ correspond to the orbits of the action of $\mathrm{Aut}(C)^*$ on Ψ;*
(2) *the stabilizer of $(C, \hat{s}) \in \rho_1^{-1}(C)$ in $\mathrm{Aut}(C)^*$ is the identity;*
(3) *the fiber over the curve C consists of $(2g+2)!/|\mathrm{Aut}(C)^*|$ elements.*

Proof: (1) Consider $(C, \hat{s}_1)$ and $(C, \hat{s}_2)$ two elements on the fiber where $\hat{s}_1 \neq \hat{s}_2$, they correspond to the same element in H_g^* if and only if there is $\phi \in \mathrm{Aut}(C)^*$ such that $\phi(\hat{s}_1) = \hat{s}_2$ that is, if and only if $\hat{s}_2 \in Orb(\hat{s}_1, \mathrm{Aut}(C)^*)$.

(2) Since by Corollary 3.3.1, every elements in $\mathrm{Aut}(C)^*$ permutes some of the Weierstrass points, an ordered $2g+2$-tuple $\hat{s}$ is sent to itself only via the identity.

(3) If two different automorphisms α and β in $\mathrm{Aut}(C)$ induce the same permutation of the Weierstrass points, from the exact sequence 1.3 in Corollary 3.3.1, $\alpha\beta^{-1} = \iota$ thus $\alpha = \beta$ in $\mathrm{Aut}(C)^*$. Since each element in the reduced automorphism group acts non-trivially and differently on every $\hat{s} \in \Psi$, every orbit of the group $\mathrm{Aut}(C)^*$ consists of $|\mathrm{Aut}(C)^*|$ elements. Therefore there is $(2g+2)!/|\mathrm{Aut}(C)^*|$ elements the fiber $\rho_1^{-1}(C)$ and the ramification index of these elements is $|\mathrm{Aut}(C)^*|$. $\square$

One can also consider the degree $(2g+2-m)! \cdot m!$ map $\rho_2 : H_g^* \longrightarrow H_g^m$ given first by sending the m first points of $(C, \hat{s})$ to the set $s \in S_m$ and then by forgetting all the labels. Again ramification will occur when the curve has non-trivial automorphisms but only particular automorphisms will produce ramification. The only way to get ramification over $(C,s) \in H_g^m$ is when two different ordering of s, say $\hat{s_1}$ and $\hat{s_2}$ give the same element in H_g^* *i.e.* when there is $\phi \in \mathrm{Aut}(C)_s^*$ such that $\phi(\hat{s_1}) = \hat{s_2}$. Remark that $\mathrm{Aut}(C)_s^*$ acts on S and on S_m and this action induces an action on $\rho^{-1}(C)$, $\rho_1^{-1}(C)$ and $\rho_2^{-1}(C,s)$. Also note that $\mathrm{Aut}(C)^* \setminus \mathrm{Aut}(C)_s^*$ does not induces an action on $\rho_2^{-1}(C,s)$.

LEMMA 4.4.4. *Let $\rho_2^{-1}(C,s)$ the fiber of the map $\rho_2 : H_g^* \longrightarrow H_g^m$, then the elements of the fiber $\rho_2^{-1}(C,s)$ correspond to the orbits of the action of $\mathrm{Aut}(C)_s^*$ on S.*

Proof: Consider $(C,\hat{s}_1)$ and $(C,\hat{s}_2)$ two elements over (C,s). This mean that $\hat{s}_1$ and $\hat{s}_2$ are two different orderings of the Weierstrass points where the m first components are s. They will correspond to the same element if and only if there is $\phi \in \mathrm{Aut}(C)^*$ such that $\phi(\hat{s}_1) = \hat{s}_2$ and ϕ send the first m components to themselves, that is, if and only if they are in the same orbit of $\mathrm{Aut}(C)_s^*$. $\square$

We can compose ρ_2 with ρ to get a degree $(2g+2-m)! \cdot m! \cdot \binom{2g+2}{n} = (2g+2)!$ map which clearly corresponds to ρ_1. The following diagram summarizes the moduli spaces we have considered and the morphisms between them.

$$
\begin{tikzcd}
 & H_g^{**} \arrow[d] \\
 & H_g^* \arrow[dl, "\rho_2"'] \arrow[dd, "\rho_1"] \\
H_g^m \arrow[dr, "\rho"'] & \\
 & H_g
\end{tikzcd}
\qquad
\begin{tikzcd}
 & (\mathbb{P}^1)^{2g+2} \setminus \Delta \arrow[d] \\
 & (\mathbb{P}^1 \setminus \{0,1,\infty\})^{2g-1} \setminus \Delta' \arrow[dl, "\rho_2"'] \arrow[dd, "\rho_1"] \\
([(\mathbb{P}^1)^{2g+2-m} \times (\mathbb{P}^1)^m] \setminus \Delta)/PGL_2 \times (\Sigma_{2g+2-m} \times \Sigma_m) \arrow[dr, "\rho"'] & \\
 & [(\mathbb{P}^1 \setminus \{0,1,\infty\})^{2g-1} \setminus \Delta']/\Sigma_{2g+2}
\end{tikzcd}
$$

Therefore this decomposition provides a better description of the ramification over C. Suppose that $(C, \hat{s}_1)$ and $(C, \hat{s}_2)$ correspond to the same element in $\rho_1^{-1}(C)$, then this identification can be explained by these two situations:

- If the first m components of $\hat{s}_1$ and $\hat{s}_2$ are the same, say s. Thus they have the same basepoint (C, s) in H_g^m. Therefore $\hat{s}_1$ is send to $\hat{s}_2$ with some ϕ in $\mathrm{Aut}(C)_s^*$.
- If the first m components of $\hat{s}_1$ and $\hat{s}_2$ are different. Thus they have different basepoints in H_g^m, say (C, s_1) and (C, s_2) for $s_1 \neq s_2$. Hence $\hat{s}_1$ is sent to $\hat{s}_2$ via an automorphism ϕ that does not fixes s_1 nor s_2. Therefore, ϕ must be in $\mathrm{Aut}(C)^* \setminus (\mathrm{Aut}^*(C)_{s_1} \cup \mathrm{Aut}^*(C)_{s_2})$.

5. Affine group schemes

We have previously seen that $\mathrm{Jac}(C)$ is a particular example of an abelian variety. Let X be an abelian variety over a field k and $X[n]$ the kernel of the multiplication by n map. Then $X[n]$ has a natural srtuctureof an *affine group scheme*. The group law on such a scheme $X[n]$ will induce naturally on $k[X[n]]$, the coordinate ring of the scheme, some k-algebra homomorphisms. Together with this structure, these k-algebras are known as Hopf algebras. In general, one starts with a k-algebra with appropriate structure on it and obtains an affine group scheme. Note that this group scheme will not necessarily come from an abelian variety. By a theorem of Oort, any commutative finite group scheme is a subgroupscheme of $X[n]$, for some abelian variety X and some n.

5.1. Affine group scheme as representable functors.

If we consider R, any k-algebra, there are several ways to get a group from it. For instance, we can consider R with only its additive law, we can also consider $\mathbf{GL}_n(R)$ the $n \times n$ matrices with entries in R and with invertible determinant. In general, given any k-algebra R we would like a group $\mathbf{G}(R)$ and that a given k-algebra homomorphism $\phi : R \longrightarrow S$, will induce a group homomorphism $\mathbf{G}(R) \longrightarrow \mathbf{G}(S)$. Indeed, we want $\mathbf{G}$ to be a covariant functor from k-algebras to groups. Furthermore, if, like in the situation of affine varieties, the elements in $\mathbf{G}(R)$ correspond to solutions in R of some family of polynomials, say $I = (\{f_j\}_{j\in J})$, one can find A a k-algebra and a natural correspondence between $\mathbf{G}(R)$ and $\mathrm{Hom}_k(A, R)$. Note that the converse also holds, every k-algebra A arises in this way from some family of equations. Such functors are called representable and we say that A represents $\mathbf{G}$. Note that if A has finitely many generators it can be written as $k[x_1, ...x_n]/I$, a coordinate ring.

DEFINITION 5.1.1. *An affine group scheme over k is a representable functor from the category of k-algebras to the category of groups.*

There are many examples of affine group schemes, and the most relevant are the following.

- $\mathbf{G}_a$: The additive group assigning to every k-algebra R its underlying additive group. The functor $\mathbf{G}_a$ is represented by $k[x]$.
- $\mathbf{G}_m$: The multiplicative group assigning to every k-algebra R the group R^* of its invertible elements together with its multiplicative law. The functor $\mathbf{G}_m$ is represented (as a scheme)by $k[x, x^{-1}] = k[x, y]/(xy - 1)$.
- μ_n : It assigns to every k-algebra R the multiplicative group $\{\zeta \in R \mid \zeta^n = 1\}$, the n-th roots of unity. The functor μ_n is represented by $k[x]/(x^n - 1)$.
- α_{p^s} : For k a field of characteristic p, it assign to every k-algebra R the additive group $\{x \in R \mid x^{p^s} = 0\}$. The functor α_{p^s} is represented by $k[x]/(x^{p^s})$.
- $\mathbf{GL}_n$: The matrix group, assigning to every k-algebra R the n by n invertible matrices with entries in R. The functor $\mathbf{GL}_n$ is represented by the ring $k[x_{1,1}, x_{1,2}, ..., x_{n,n}, y]/(y \cdot \det(x_{ij}) - 1)$.
- $\mathbf{\Gamma}$: The constant group scheme represented by $A = k^\Gamma$. One can show that if R is a k-algebra with no idempotents except 0 and 1, any element of $\mathrm{Hom}(A, R)$ is given by assigning one element in Γ to the unity of R, thus one can, in a certain way, consider $\mathbf{\Gamma}(R)$ as the group Γ itself.

It is well known that there are plenty of maps between groups. For instance, consider $\det : \mathbf{GL}_n \longrightarrow \mathbf{G}_m$. For each ring R, det gives a map from $\mathbf{GL}_n(R)$ to $\mathbf{G}_m(R)$. This is, in fact, a natural transformation of functors since for any $\phi : R \longrightarrow S$ the following diagram commutes:

$$\begin{array}{ccc} \mathbf{GL}_n(R) & \longrightarrow & \mathbf{G}_m(R) \\ \downarrow & & \downarrow \\ \mathbf{GL}_n(S) & \longrightarrow & \mathbf{G}_m(S). \end{array}$$

This comes from the fact that we have an explicit formula for det involving only polynomials in the matrix entries. In fact, such natural maps arise only from such a situation.

THEOREM 5.1.1. (Yoneda's lemma) *Let $\boldsymbol{E}$ and $\boldsymbol{F}$ be functors represented by k-algebras A and B. Every natural transformation of functors $\boldsymbol{E} \longrightarrow \boldsymbol{F}$ corresponds to k-algebra homomorphisms $B \longrightarrow A$.*

Proof: Since an element in $\mathbf{E}(R)$ corresponds to a morphism $A \longrightarrow R$, for any $\psi : B \longrightarrow A$, the composition $B \longrightarrow A \longrightarrow R$ define an element in $\mathbf{F}(R)$. We get clearly a natural transformation of functors $\mathbf{E} \longrightarrow \mathbf{F}$.

Conversely, we can apply our natural map $\Psi : \mathbf{E} \longrightarrow \mathbf{F}$ to $\mathbf{E}(A)$ corresponding to the identity map $id_A : A \longrightarrow A$. Applying Ψ to it we get an element of $\mathbf{F}(A)$, *i.e.*, a homomorphism $\psi : B \longrightarrow A$. Since any element in any $\mathbf{E}(R)$ comes from a homomorphism $A \longrightarrow R$, and

$$\begin{array}{ccc} \mathbf{E}(A) & \longrightarrow & \mathbf{E}(R) \\ \downarrow & & \downarrow \\ \mathbf{F}(A) & \longrightarrow & \mathbf{F}(R) \end{array}$$

commutes, we see that Ψ is exactly the map defined from ψ in the first step. $\square$

COROLLARY 5.1.1. *The map $\boldsymbol{E} \longrightarrow \boldsymbol{F}$ is a natural equivalence iff $B \longrightarrow A$ is an isomorphism.*

Notice that affine group schemes can also be consider as contravariant functors from k-algebras R to groups if we describe them in terms of their representing obj ects, A.

5.2. Hopf Algebras.

As noted before, the group structure on $\mathbf{G}$ induces naturally some maps on the k-algebra A. This is a well known structure, known as a Hopf algebra. Consider a group $\Gamma := \mathbf{G}(R)$ for some $\mathbf{G}$ and some R. Saying that Γ is a group is equivalent to giving the maps:

$$\begin{aligned} \text{multiplication} \quad m:& \quad \Gamma \times \Gamma \longrightarrow \Gamma \\ \text{unit} \quad u:& \quad \{e\} \longrightarrow \Gamma \\ \text{inverse} \quad i:& \quad \Gamma \longrightarrow \Gamma \end{aligned}$$

such that the following diagrams commute:

$$\begin{array}{ccc} \Gamma \times \Gamma \times \Gamma & \xrightarrow{id \times m} & \Gamma \times \Gamma \\ \downarrow m \times id & & \downarrow m \\ \Gamma \times \Gamma & \xrightarrow{m} & \Gamma \end{array} \qquad \text{(associativity)},$$

$$\begin{array}{ccc} \{e\} \times \Gamma & \xrightarrow{u \times id} & \Gamma \times \Gamma \\ \wr\vert & & \downarrow m \\ \Gamma & = & \Gamma \end{array} \qquad \text{(left unit)},$$

$$\begin{array}{ccc} \Gamma & \xrightarrow{(i,\ id)} & \Gamma \times \Gamma \\ \downarrow & & \downarrow m \\ \{e\} & \xrightarrow{u} & \Gamma \end{array} \qquad \text{(left inverse)}.$$

Suppose now that $\mathbf{G}$ is represented by A; then $A \otimes_k A$ represents $\mathbf{G} \times \mathbf{G}$ and we can apply Yoneda's lemma to get the following k-algebras maps:

$$\begin{aligned} \text{comultiplication} \quad \Delta:& \quad A \longrightarrow A \otimes A \\ \text{counit} \quad \epsilon:& \quad A \longrightarrow k \\ \text{coinverse} \quad \mathrm{S}:& \quad A \longrightarrow A \end{aligned}$$

such that the following diagrams commute:

$$\begin{array}{ccc} A\otimes A\otimes A & \xleftarrow{id\otimes\Delta} & A\otimes A \\ \uparrow \Delta\otimes id & & \uparrow \Delta \\ A\otimes A & \xleftarrow{\Delta} & A \end{array},$$

$$\begin{array}{ccc} k\otimes A & \xleftarrow{\epsilon\otimes id} & A\otimes A \\ \wr\vert & & \uparrow \Delta \\ A & = & A \end{array} \quad\text{and}\quad \begin{array}{ccc} A & \xleftarrow{(\mathrm{S},\ id)} & A\otimes A \\ \uparrow & & \uparrow \Delta \\ k & \xleftarrow{\epsilon} & A \end{array}.$$

Definition 5.2.1. *A k-algebra with specified maps Δ, ϵ, S satisfying the above conditions is called a Hopf algebra.*

One can show that affine group schemes over k correspond to Hopf algebras over k, see [**32**, I,§ 1.4]. Note that in terms of functions, from $f \in A$ where $f : \mathbf{G} \longrightarrow k$ we get $\Delta f \in A \otimes A$ where $\Delta f : \mathbf{G} \times \mathbf{G} \longrightarrow k$ is given by $\Delta f(x, y) = f(xy)$. If we return to the above examples we easily work out the structure of their respective Hopf algebras.

- For $\mathbf{G}_a$, we have

$$\begin{aligned} \Delta :\ \ x &\mapsto (x\otimes 1) + (1\otimes x) = x + y, \\ \epsilon :\ \ x &\mapsto 0, \\ \mathrm{S} :\ \ x &\mapsto -x, \end{aligned}$$

  where $x \otimes 1 =: x$ and $1 \otimes x =: y$.
- For $\mathbf{G}_m$, we have

$$\begin{aligned} \Delta :\ \ x &\mapsto x\otimes x = (x\otimes 1)\cdot(1\otimes x) = xy, \\ \epsilon :\ \ x &\mapsto 1, \\ \mathrm{S} :\ \ x &\mapsto x^{-1}, \end{aligned}$$

where $x \otimes 1 =: x$ and $1 \otimes x =: y$.

- For μ_n, this group scheme is in fact the kernel of the homomorphism $\mathbf{G}_m \longrightarrow \mathbf{G}_m$ given by $x \mapsto x^n$ and the maps on the Hopf algebra $k[x]/(x^n - 1)$ are the same as for $k[x, x^{-1}]$ modulo the ideal.
- For α_{p^s}, this group scheme is in fact the kernel of the homomorphism $\mathrm{Fr}^s : \mathbf{G}_a \longrightarrow \mathbf{G}_a$ given by $x \mapsto x^{p^s}$ and the maps on the Hopf algebra $k[x]/(x^{p^s})$ are the same as for $k[x]$ modulo the ideal. Note that Fr^s is the well known Frobenius map that we will study later.
- For $\mathbf{\Gamma}$, if we denote by e_σ the element in A such that $e_\sigma(\sigma) = 1$ and $e_\sigma(\tau) = 0$ for all the other elements τ in the group, we get that $\{e_\sigma\}_{\sigma\in\Gamma}$ is a basis of A. In this setting we have

$$\begin{aligned} \Delta :\quad e_\sigma &\mapsto \sum_{\delta\in\Gamma}(e_{\sigma\delta} \otimes e_{\delta^{-1}}), \\ \epsilon :\quad e_\sigma &\mapsto \begin{cases} 1 & \text{if } \sigma = id \\ 0 & \text{otherwise,} \end{cases} \\ \mathrm{S} :\quad e_\sigma &\mapsto e_{\sigma^{-1}}, \end{aligned}$$

5.3. Cartier dual.

In addition to the maps Δ, ϵ, rmS, a Hopf algebra A has the following maps:

$$\begin{aligned} \text{ring multiplication} \quad m :&\quad A \otimes A \longrightarrow A \\ k\text{-algebra structure} \quad u :&\quad k \longrightarrow A. \end{aligned}$$

Hence, it seems possible to consider the dual of these Hopf algebras. A group scheme $\mathbf{G}$ is said to be finite if it is represented by A, a finite dimensional vector space over k. First note that taking the dual $N^\vee = \mathrm{Hom}_k(N, k)$ of a finite-rank free module commutes with the usual operations on modules: $(M\oplus N)^\vee \simeq (M^\vee \oplus N^\vee)$, $(M\otimes N)^\vee \simeq (M^\vee \otimes N^\vee)$, $\mathrm{Hom}(M, N) \simeq \mathrm{Hom}(N^\vee, M^\vee)$ and $(M \oplus k)^\vee \simeq M^\vee \oplus k$. Since the operations Hom and $\oplus$ commute with finite direct sums, taking the dual of A still make sense if $\mathbf{G}$ is a finite abelian group scheme. The maps Δ, ϵ, S, m and u induce new maps on the dual which are very similar to some we know:

$$\begin{aligned} m^\vee :&\quad A^\vee \longrightarrow A^\vee \otimes A^\vee, \\ u^\vee :&\quad A^\vee \longrightarrow k, \\ S^\vee :&\quad A^\vee \longrightarrow A^\vee, \\ \Delta^\vee :&\quad A^\vee \otimes A^\vee \longrightarrow A^\vee, \\ \epsilon^\vee :&\quad k \longrightarrow A^\vee. \end{aligned}$$

THEOREM 5.3.1. (Cartier duality). *Let $\boldsymbol{G}$ be a finite abelian group scheme represented by A. Then $A^\vee$ represent another finite abelian group scheme $\boldsymbol{G}^\vee$. Here $(\boldsymbol{G}^\vee)^\vee = \boldsymbol{G}$ and* $\mathrm{Hom}(\boldsymbol{G}, \boldsymbol{H}) \simeq \mathrm{Hom}(\boldsymbol{H}^\vee, \boldsymbol{G}^\vee)$.

We can find a proof of this theorem in [**32**] and it is an easy exercise to show that $(\mathbb{Z}/n\mathbb{Z})^\vee \simeq \mu_n$ and $(\alpha_{p^s})^\vee \simeq \alpha_{p^s}$.

5.4. The Frobenius map.

Given any field map $k \longrightarrow k'$ we can perform a base change and get a group scheme over k' represented by $A \otimes_k k'$. By considering the Frobenius map $\mathrm{Fr}^s : \alpha \mapsto \alpha^{p^s}$ from k to itself, for any affine group scheme $\mathbf{G}$ over a field k of characteristic p, we get a new group scheme denoted $\mathbf{G}^{(p^s)}$. If $\mathbf{G}$ and $\mathbf{G}^{(p^s)}$ are represented by respectively A and $A^{(p^s)} = A \otimes_{k_{\circlearrowleft \mathrm{Fr}^s}} k$, the map from $A^{(p^s)}$ to A given by $a \otimes \alpha \mapsto a^{p^s}\alpha$ gives a group homomorphisms

$$\mathrm{Fr}^s : \mathbf{G} \longrightarrow \mathbf{G}^{(p^s)},$$

again called the Frobenius map. If $A = k[x_1, ..., x_n]/(f_1, ..., f_m)$ then $A^{(p^s)} = k[x_1, ..., x_n]/(g_1, ..., g_m)$ represents $\mathbf{G}^{(p^s)}$ where the g_i are obtained by raising each coefficient of the f_i to the p^s power. Then the morphism Fr^s is given as morphism of k-algebras by

$$\mathrm{Fr}^s : A^{(p^s)} \longrightarrow A, \qquad x_i \mapsto x_i^{p^s} \text{ for } i = 1, ..., m,$$

and corresponds, as a homomorphism of groups, to

$$\mathrm{Fr}^s : \mathbf{G}(S) \longrightarrow \mathbf{G}^{(p^s)}(S), \qquad (s_1, ..., s_n) \mapsto (s_1^{p^s}, ..., s_n^{p^s}).$$

If $\mathbf{G}$ is a finite abelian group scheme, we can apply the same argument to the dual of $\mathbf{G}$ and get the map

$$\mathrm{Fr} : \mathbf{G}^\vee \longrightarrow (\mathbf{G}^\vee)^{(p)},$$

that induces, by duality, a morphism called the *Verschiebung morphism* given by

$$\mathrm{Ver} := \mathrm{Fr}^\vee : \mathbf{G}^{(p)} \longrightarrow \mathbf{G},$$

and such that $\mathrm{Fr}_{\mathbf{G}} \circ \mathrm{Ver}_{\mathbf{G}^{(p)}} = [p]\mathbf{G}^{(p)}$ and $\mathrm{Ver}_{\mathbf{G}^{(p)}} \circ \mathrm{Fr}_{\mathbf{G}} = [p]\mathbf{G}$, see [**5**] for details.

5.5. Étale group schemes.

For k a perfect field of characteristic p and $\mathbf{G}$ a finite commutative abelian scheme represented by A, we will say that $\mathbf{G}$ is *étale* if it becomes a constant group scheme after base change, that is, if $A \otimes_k \overline{k}$ represents a constant group scheme. We have seen that given any finite abelian group one can construct a corresponding constant group scheme. Indeed we have a bijection between these two sets, and if we consider étale group schemes we have again a bijection given by.

$$\left\{ \begin{array}{l} \text{Étale group schemes} \\ \text{over } k \end{array} \right\} \leftrightsquigarrow \left\{ \begin{array}{l} \text{Finite abelian groups } \Gamma \; + \\ \text{an element of } H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(\Gamma)) \end{array} \right\}.$$

Any δ in $\mathrm{Hom}(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(\Gamma))$ will gives an étale group scheme, see [**19**, I,§5] for the equivalence of categories between finite étale group schemes over k and the category of groups endowed with $\mathrm{Gal}(\overline{k}, k)$ action. Two elements δ, δ' will represent the same étale group scheme iff there is $\sigma \in \mathrm{Aut}(\Gamma)$ such that $\delta = \sigma\delta'\sigma^{-1}$ *i.e.* iff they define the same cohomology class.

If $\mathbf{G}$ has order l^r, where l is prime to p, one can show that $\mathbf{G}$ is always étale and therefore $\mathbf{G}^\vee$ will also be étale. On the other hand, if $\mathbf{G}$ has order p^s, it may or may not be étale. We will say that $\mathbf{G}$ is *local* if $\mathbf{G}$ is represented by an artinian local ring A. Since geometric points come from maximal ideals, $\mathbf{G}(\overline{k})$ consists of the identity element only. For instance, in the examples seen before, α_p and μ_p are local group schemes over fields of characteristic p. We will say that a local group scheme of order p^s is *local-étale* if its dual is étale. Also if an étale group has order p^s it is not difficult to show that its dual will necessarily be local, such group schemes are called *étale-local.*

It is now possible to decompose the category of finite commutative group schemes over a perfect field in four categories, see [**31**] for proof and details.

$$(\text{ local-local }) \oplus (\text{ local-étale }) \oplus (\text{ étale-local }) \oplus (\text{ étale-étale }).$$

For each of these categories, we have a non-trivial example given respectively by

$$\alpha_p,\ \mu_p,\ \mathbb{Z}/p\,\mathbb{Z} \text{ and } \ \mathbb{Z}/l\mathbb{Z},$$

where l is any prime different of p, the characteristic of the field k. Moreover, over an algebraically closed field k, every finite commutative group scheme has a composition series whose quotients are one of those group schemes, see [**24**, Lemma 6.1].

5.6. $\mathbf{G}[n]$ as an affine group scheme.

Given any commutative affine group scheme $\mathbf{G}$ of dimension g we can consider the functor from k-algebras to groups

$$\mathbf{G}[n] : R \longrightarrow \mathbf{G}[n](R) = \{x \in \mathbf{G}(R) \mid nx = 0\}.$$

If G is a g dimensional abelian variety, one can prove, see [**19**], that the multiplication by n map is an isogeny and the kernel $\mathbf{G}[n]$ is an affine group scheme represented by a Hopf algebra A of rank n^{2g}. One can also show that $\mathbf{G}[n]$ is étale, that is

$\mathbf{G}[n] \otimes_k k^s \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$, if and only if the characteristic of k is coprime to n. Moreover, if $p = \mathrm{char}(k)$ then

$$|\mathbf{G}[p](k)| \leq p^g,$$

and the kernel of the map $\mathrm{Fr} : \mathbf{G}[p] \longrightarrow \mathbf{G}^{(p)}[p]$ is also an affine group scheme of order p^g.

5.7. Polarization.

In a later classification of $A[p]$ we will assume that these group schemes are self-dual. This duality comes from the fact that we consider principally polarized abelian varieties A, which is always the case when A is the Jacobian of a curve. Without going into great details, we will give some explanations.

For any divisor D in A we consider the line bundle $\mathcal{L} = \mathcal{O}_A(D)$ and $T_x : A \longrightarrow A$ the translation by x map on A, $T_x(y) = x + y$. The dual abelian variety $A^\vee$ parameterizes line bundles on A that are algebraically equivalent to zero. For every x and a line bundle $\mathcal{L}$, we have that $T_x(\mathcal{L}) \otimes \mathcal{L}^{-1}$ is equivalent to zero, hence corresponds to a point on $A^\vee$. We define the map

$$\begin{aligned} \lambda_{\mathcal{L}} : \quad A &\longrightarrow A^\vee \\ x &\mapsto T_x(\mathcal{L}) \otimes \mathcal{L}^{-1} \end{aligned}$$

which is in fact an homomorphism of groups, see [**21**, §6, Corollary 4]. The dual $A^\vee$ of the abelian variety A is $\mathrm{Pic}^0(A)$, where here $\mathrm{Pic}^0(A)$ is the identity component of $\mathrm{Pic}(A)$ and one can show that $(A^\vee)^\vee = A$. Recall that a *polarization* of A is a homomorphism,

$$f : A \longrightarrow A^\vee,$$

where $f = \lambda_{\mathcal{L}}$ for some ample line bundle $\mathcal{L}$ over A/k. The polarization is said to be *principal* if f is an isomorphism.

For a curve C and a point P on it, there exists a particular divisor on the Jacobian of C, named the *theta-divisor*, which is given as follow

$$\Theta = \left\{ \sum_{i=1}^{g-1} P_i - (g-1)P \mid P_i \in C \right\}.$$

Changing the basepoint P results in a translation of Θ and thus the theta divisor is canonical up to translation and one can show that it is ample. Therefore, for $\mathcal{L} = \mathcal{O}_{\mathrm{Jac}(C)}(\Theta)$, the map $\lambda_{\mathcal{L}} : \mathrm{Jac}(C) \longrightarrow \mathrm{Jac}(C)^{\vee}$ is a canonical polarization and one can show that it is an isomorphism, see [**20**, Theorem 6.6] for details.

We only consider self-dual abelian varieties in the next sections. From the exact sequence

$$0 \longrightarrow A[n] \longrightarrow A \xrightarrow{\times n} A \longrightarrow 0,$$

we get by duality theory

$$0 \longrightarrow (A[n])^{\vee} \longrightarrow A^{\vee} \xrightarrow{(\times n)^{\vee}} A^{\vee} \longrightarrow 0.$$

Because $(\times n)^{\vee} = \times n$ we have that $(A[n])^{\vee} = A^{\vee}[n]$ and by self-duality we conclude that $A^{\vee}[n] \cong A[n]$. Since for every finite commutative group scheme $\mathbf{G}$ over k, there exists a canonical perfect pairing $\mathbf{G} \times \mathbf{G}^{\vee} \longrightarrow \mathbf{G}_m$, we obtain

$$A[n] \times (A[n])^{\vee} \longrightarrow \mu_n,$$

which leads in this setting to the *Weil Pairing*

$$A[n] \times A[n] \longrightarrow \mu_n.$$

6. Dieudonné Modules

For the questions that interest us, we may restrict our attention to self-dual p-torsion commutative group schemes of order p^s over k, a perfect field of characteristic p. We will denote the Froebenius morphism on k by σ. In order to study these group schemes, we will often work on an equivalent category: the *covariant Dieudonné modules.*

Given $\mathbf{G}$, a p-torsion commutative group scheme of order p^s, we have a corresponding Dieudonné module $\mathbb{D}(\mathbf{G})$ which is a s-dimensional vector space over k together with two maps: F and V, and an alternating pairing. The formation of these modules commutes with base changes, that is

$$\mathbb{D}(\mathbf{G} \otimes_k L) \cong \mathbb{D}(\mathbf{G}) \otimes_k L.$$

The construction is functorial, see [**5**, Appendix A,5], thus from

$$\mathrm{Fr} : \mathbf{G} \longrightarrow \mathbf{G}^{(p)},$$

there is a linear map:

$$\mathrm{Fr}^* : \mathbb{D}(\mathbf{G}) \longrightarrow \mathbb{D}(\mathbf{G}^{(p)}) = \mathbb{D}(\mathbf{G}) \otimes_{k_{\circlearrowleft \mathrm{Fr}}} k$$

that gives the σ^{-1}-linear map

$$V : \mathbb{D}(\mathbf{G}) \longrightarrow \mathbb{D}(\mathbf{G}).$$

Similarly we get the σ-linear map

$$F : \mathbb{D}(\mathbf{G}) \longrightarrow \mathbb{D}(\mathbf{G})$$

from Verschiebung and the two maps are such that

$$FV = VF = 0,\ F(\lambda v) = \lambda^p F(v) \text{ and } V(\lambda v) = \lambda^{\frac{1}{p}} V(v) \quad \forall \lambda \in k. \tag{1.4}$$

A morphism of Dieudonné modules is a morphism of vector spaces that commutes with V and F. Also, one can show that we have the duality $\mathbb{D}(\mathbf{G}^\vee) = \mathrm{Hom}_k(\mathbb{D}(\mathbf{G}), k) = \mathbb{D}(\mathbf{G})^\vee$.

THEOREM 6.0.1. *The functor $\mathbb{D}$ from the category of finite commutative group schemes of order a power of p over a perfect field k of characteristic p to the category of finite dimensional k-vector spaces equipped with two maps F and V satisfying (1.4) is an equivalence of categories.*

The equivalence can be refined to an equivalence between the self-dual group schemes *i.e.*, group schemes $\mathbf{G}$ equipped with an isomorphism $\lambda : \mathbf{G} \longrightarrow \mathbf{G}^\vee$ such that $\lambda = \lambda^\vee$ and k-vector spaces V equipped with a perfect alternating pairing

$$< \cdot, \cdot >: V \times V \longrightarrow k$$

such that $< Fx, y >=< x, Vy >^\sigma$. This new category will be an useful tool to classify $\mathrm{Jac}(C)[p]$.

For instance, we can consider μ_p and $\mathbb{Z}/p\mathbb{Z}$ which are dual to each other and have order p. One easily verifies that Frobenius acts as zero on μ_p and as the identity on $\mathbb{Z}/p\mathbb{Z}$, thus V acts as an isomorphism on $\mathbb{D}(\mathbb{Z}/p\mathbb{Z})$. Or equivalently, F acts as an isomorphism on $\mathbb{D}(\mu_p)$. Therefore the group μ_p has the Dieudonné module $\mathbb{D}(\mu_p) = k$, where p and V act as zero and F acts as an automorphism of k. The group scheme $\mathbb{Z}/p\mathbb{Z}$ has the Dieudonné module $\mathbb{D}(\mathbb{Z}/p\mathbb{Z}) = k$ where p and F act as zero and V acts as an automorphism of k. Since Verschiebung and Frobenius act as zero on the group scheme α_p, using the equivalence of categories, we have the trivial Dieudonné module $\mathbb{D}(\alpha_p) = k$, where F, V and p act as zero.

6.1. The a-number and the f-number.

Consider $\mathrm{Hom}(\alpha_p, \mathbf{G})$ for any finite commutative group scheme $\mathbf{G}$. This is a finite dimensional vector space. One can prove it directly, see [**5**], or use the equivalence of categories. Indeed for $\phi \in \mathrm{Hom}(\mathbb{D}(\alpha_p), \mathbb{D}(\mathbf{G})) = \mathrm{Hom}(k, \mathbb{D}(\mathbf{G}))$, since $\phi(F(x)) = \phi(V(x)) = 0$ by linearity we would expect to have $F(\phi(x)) = V(\phi(x)) = 0$ for any $x \in k$. Thus if we denote the k-vector space $W = \{\ y \in \mathbb{D}(\mathbf{G}) \mid Fy = Vy = 0\ \} = \mathrm{Ker}(F) \cap \mathrm{Ker}(V)$ we have that:

$$\mathrm{Hom}(\mathbb{D}(\alpha_p), \mathbb{D}(\mathbf{G})) = \mathrm{Hom}(k, W),$$

a k- vector space. We define the *a-number* of the finite commutative group scheme $\mathbf{G}$, as the dimension of this space, *i.e.*,

$$\begin{aligned} a\sharp(\mathbf{G}) &= \dim_k \mathrm{Hom}(\alpha_p, A) \\ &= \dim_k \mathrm{Hom}(k, W) \\ &= \dim_k W. \end{aligned}$$

Furthermore we have that $W \cong k^{a\sharp} \cong (\mathbb{D}(\alpha_p))^{a\sharp}$ as vector spaces and, again by the equivalence of categories, there exists a finite commutative group scheme $\alpha \subset \mathbf{G}$, the *alpha group scheme*, such that $\mathbb{D}(\alpha) = W$ and $\alpha \cong \alpha_p^{a\sharp}$.

We return to our classification of commutative group schemes $\mathbf{G}$ over a perfect field of characteristic p. For any p-torsion group $\mathbf{G}$, it can be decomposed as

$$\mathbf{G} = \mathbf{G}^{l-l} \oplus \mathbf{G}^{l-e} \oplus \mathbf{G}^{e-l}.$$

where $\mathbf{G}^{l-l}$ is its local-local component, $\mathbf{G}^{l-e}$ its local-étale component and $\mathbf{G}^{e-l}$ its étale-local component. We therefore have

$$\mathbb{D}(\mathbf{G}) = \mathbb{D}(\mathbf{G}^{l-l}) \oplus \mathbb{D}(\mathbf{G}^{l-e}) \oplus \mathbb{D}(\mathbf{G}^{e-l}).$$

Note that on $\mathbb{D}(\mathbf{G}^{l-e})$, F is an isomorphism and V is nilpotent and on $\mathbb{D}(\mathbf{G}^{e-l})$, V is an isomorphism and F is nilpotent. Therefore F and V both have kernel only on $\mathbb{D}(\mathbf{G}^{l-l})$ and it follows easily that $a\sharp(\mathbf{G}) = a\sharp(\mathbf{G}^{l-l})$. Moreover, since F and V

are nilpotent we can conclude that $W \neq 0$, hence $a\sharp(\mathbf{G}^{l-l}) > 0$ for any *local* $-$ *local* group scheme. Also, for $\mathbf{G}$ an abelian variety of dimension g, the kernel of the map $\mathrm{Fr} : \mathbf{G}[p] \longrightarrow \mathbf{G}^{(p)}[p]$ has order p^g, thus we have an upper bound for the a-number.

For instance we can find the a-number for all the possible p-torsion groups of the elliptic curves. As stated before, every elliptic curve is principally polarized, thus $E[p]$ is self-dual.

Consider first the case when E is an *ordinary* elliptic curve, that is when $E[p](\overline{k}) \cong \mathbb{Z}/p\,\mathbb{Z}$. By self-duality we have $\mu_p \subset E[p] \otimes_k \overline{k}$ so

$$\mu_p \oplus \mathbb{Z}/p\,\mathbb{Z} \subset E[p] \otimes_k \overline{k}$$

and we get the equality by considering the rank on both sides. Remark that $E[p]$ does not have local-local component thus the a-number of an ordinary elliptic curve is 0.

If E is a *supersingular* elliptic curve, that is when $E[p](\overline{k}) = 0$, then the p-torsion group has no étale-local component, thus, by self-duality, no local-étale component either. Therefore, $E[p]$ is local-local, so $a\sharp(E[p]) > 0$ and by the upper bound we have that $a\sharp(E[p]) = 1$. Thus we have the non-split exact sequence

$$0 \longrightarrow \alpha_p \longrightarrow E[p] \longrightarrow \alpha_p \longrightarrow 0,$$

where the embedded α_p, that we will denote $\mathbb{H}$, is unique and is both in the kernel of Frobenius and Verschiebung. The group scheme $E[p] \otimes_k \overline{k}$ will be denoted $\mathbb{M}$ and one can show that it is independent of E.

One can also show that if we apply twice Frobenius to the group scheme $\mathbf{G}[p]$ of order p^{2g}, we get that $\mathrm{Fr}^2(\mathbf{G}[p])$ is a group scheme of order $p^{g-a\sharp}$.

Another number that will interest us is the integer $f\sharp$ such that

$$p^{f\sharp} = |\mathbf{G}[p](\overline{k})|.$$

It is called the *f-number* of the commutative group scheme $\mathbf{G}[p]$. Remark that the f-number depends only of the étale component, therefore $f\sharp(\mathbf{G}) = f\sharp(\mathbf{G}^{e-l})$. In fact for $\mathbf{G} = A[p]$ the f-number is often defined as

$$\dim_k \bigcap_{i=1}^{\infty} V^i(\mathbb{D}(\mathbf{G})) = \dim_k \mathbb{D}(G^{e-l})$$

since $\mathbb{D}(\mathbf{G}^{e-l})$ is the largest submodule of $\mathbb{D}(\mathbf{G})$ on which V is an isomorphism. (Equivalently, $\mathbf{G}^{e-l}$ is the largest subgroup of $\mathbf{G}$ on which F is an isomorphism.)

For instance, we can find the f-number for our previous example, the p-torsion groups of elliptic curves. Since the p-torsion group of a supersingular curve has no étale-local component, the f-number is 0. For the ordinary case we have that $E[p]^{e-l} = E[p](k) \cong \mathbb{Z}/p\mathbb{Z}$, thus the f-number is 1.

Together with the a-number, the f-number will allow us to describe partially Frobenius and Verschiebung for the finite commutative group schemes that interest us: the p-torsion group of the Jacobian of hyperelliptic curves. The a-number and the f-number should be thought of as (very coarse) discrete invariants we can associate to an abelian variety in positive characteristic.

6.2. Dieudonné modules and cohomology.

As noted before it will be useful to study abelian varieties using Dieudonné modules. Also, using cohomology we will get very concrete tools for our study. Let A

be an abelian variety of dimension g over a perfect field of characteristic p. We can consider two order p^g group schemes, $A[\mathrm{Fr}] \subset A$, the kernel of the Froebenius morphism $\mathrm{Fr} : A \longrightarrow A^{(p)}$ and $A[\mathrm{Ver}] \subset A$, the kernel of the Verschiebung morphism $\mathrm{Ver} : A \longrightarrow A^{(1/p)}$. Together with $A[p]$ we have the following exact sequence:

$$0 \longrightarrow A[\mathrm{Ver}] \longrightarrow A[p] \xrightarrow{\mathrm{Ver}} A^{(1/p)}[\mathrm{Fr}] \longrightarrow 0.$$

This uses that $\mathrm{Fr} \circ \mathrm{Ver} = [p]$ and that both $A[\mathrm{Ver}]$ and $A[\mathrm{Fr}]$ are of order p^g. Applying the covariant Dieudonné functor we get

$$0 \longrightarrow \mathbb{D}(A[\mathrm{Ver}]) \longrightarrow \mathbb{D}(A[p]) \xrightarrow{\mathrm{F}} \mathbb{D}(A^{(1/p)}[\mathrm{Fr}]) = \mathbb{D}(A[\mathrm{Fr}])^{(1/p)} \longrightarrow 0 \tag{1.5}$$

(where F is a linear map). We note that this sequence is nothing else then

$$0 \longrightarrow \mathbb{D}(F) \longrightarrow \mathbb{D} \xrightarrow{\mathrm{F}} \mathbb{D}(V) \longrightarrow 0,$$

where $\mathbb{D} = \mathbb{D}(A[p])$, $\mathbb{D}(F) = \{ x \in \mathbb{D} \mid Fx = 0 \}$, $\mathbb{D}(V) = \{ x \in \mathbb{D} \mid Vx = 0 \}$ and F is now a σ-linear map.

One can also show that there is an isomorphism of $k[F,V]$-modules of $\mathbb{D}$ with $H^1_{dR}(A)$ if A has a polarization prime to p. It is known that the vector space H^1_{dR} has the following filtration

$$0 \longrightarrow H^0(A, \Omega^1_A) \longrightarrow H^1_{dR}(A) \longrightarrow H^1(A, \mathcal{O}_A) \longrightarrow 0,$$

which can be related to (1.5). Indeed, it is not hard to show that Fr acts as zero on differential forms, thus we can associate $\mathbb{D}(F)$ with $H^0(A, \Omega^1_a)$. Also we can identify $\mathrm{Im}(F(\mathbb{D}))$ with $H^1(A, \mathcal{O}_A)$. Assuming that A has principal polarization, we have that

$$\mathbb{D}/\mathbb{D}(F) = \mathrm{Im}(F) = \mathrm{Ker}(V) = \mathbb{D}(V)$$

but notice that the map that identifies $\mathbb{D}/\mathbb{D}(F)$ with $\mathbb{D}(V)$ is σ-linear. Therefore we have the association: $\mathbb{D}(V) \cong H^1(A, \mathcal{O}_A) \otimes_{k_{\circlearrowleft \mathrm{Fr}}} k$ which give the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(A,\Omega^1_A) & \longrightarrow & H^1_{dR}(A) & \longrightarrow & H^1(A,\mathcal{O}_A) & \longrightarrow & 0 \\
 & & \downarrow \ \| \wr & & \downarrow \ \| \wr & & \downarrow \ \| \wr & & \\
0 & \longrightarrow & \mathbb{D}(F) & \longrightarrow & \mathbb{D} & \xrightarrow{\mathrm{F}} & \mathbb{D}(V)\otimes_{k_{\circlearrowleft \mathrm{Fr}}} k & \longrightarrow & 0.
\end{array}$$

Furthermore the Frobenius operator F on $\mathbb{D}(V)$ induces a σ-linear operator on $H^1(A,\mathcal{O}_A)$. There is also a σ-linear operator on $H^1(A,\mathcal{O}_A)$ induced by the map of sheaves $\mathcal{O}_A \longrightarrow \mathcal{O}_A$ given by $x \mapsto x^p$. One can prove, see [**22**], that these two maps agree. We denote this morphism also by F. This sequence has many applications in our study. For instance, it is now possible to express the a-number of $A[p]$ in terms of cohomology. Since $\mathbb{D}(V) = \mathbb{D}(A[\mathrm{Fr}])$ is already the kernel of V we have

$$\begin{aligned}
a\sharp(A[p]) &= \dim_k \mathrm{Ker}(F : \mathbb{D}(V) \longrightarrow \mathbb{D}(V)) \\
&= \dim_k \mathrm{Ker}(F : H^1(A,\mathcal{O}_A)\otimes_{k_{\circlearrowleft \mathrm{Fr}}} k \longrightarrow H^1(A,\mathcal{O}_A)\otimes_{k_{\circlearrowleft \mathrm{Fr}}} k) \\
&= \dim_k \mathrm{Ker}(F : H^1(A,\mathcal{O}_A) \longrightarrow H^1(A,\mathcal{O}_A)).
\end{aligned}$$

Therefore, if A is the Jacobian of a curve C, it will be possible to study properties of the Frobenius morphism, for instance the σ-linear operator induced by F on $H^1(\mathrm{Jac}(C),\mathcal{O}_{\mathrm{Jac}(C)})$. The matrix describing this operator on $H^1(\mathrm{Jac}(C),\mathcal{O}_{\mathrm{Jac}(C)})$ in named *the Hasse-Witt Matrix.* It is known that there is an isomorphism between $H^1(C,\mathcal{O}_C)$ and $H^1(\mathrm{Jac}(C),\mathcal{O}_{\mathrm{Jac}(C)})$, see for instance [**20**, Lemma 9.5]. Therefore it will be possible to describe the Hasse-Witt matrix in terms $H^1(C,\mathcal{O}_C)$ and this is equivalent to studying the Verschiebung operator V on $H^0(C,\Omega^1_C)$.

6.3. The Cartier operator.

We will see in a moment that studying the Verschiebung operator V on $H^0(C,\Omega^1_C)$ is the same as studying the Cartier operator. But before we introduce this operator we need some preliminaries on the theory of differential over fields of positive characteristic. All the proofs related to this topic can be found in [**2**, Chapter 2]

We say that an application $\mathfrak{d}$ of a field k to itself is a *derivation* if it satisfies these two properties

$$\begin{aligned} \mathfrak{d}(x+y) &= \mathfrak{d}(x)+\mathfrak{d}(y), \\ \mathfrak{d}(xy) &= \mathfrak{d}(x)y + x\mathfrak{d}(y) \text{ for } x, y \in k. \end{aligned}$$

One can easily show that the set of elements annihilated by a derivation $\mathfrak{d}$ is in fact a subfield $k(\mathfrak{d})$ containing k^p. A derivation $\mathfrak{d}$ which is null for each element of L, a subfield of k, is said to be a L-*derivation* and we will denote $\mathfrak{g}(k/L)$ the set of all L-derivations.

For k, a finite extension of a field L containing k^p, we call a p-*basis* any minimal system of generators of the extension k/L. Since $[k : L]$ is finite, a p-basis is also finite. A sequence of elements $\{x_i\}_{1\leq i\leq n}$ in k, is a p-basis if and only if the monomials $x_1^{j_1}\cdots x_n^{j_n}$ (for $0 \leq j_k < p$ and $1 \leq k \leq n$) are a basis of k over L as a vector space. Also, if $\{x_i\}_{1\leq i\leq n}$ is a p-basis of the extension k/L, there exists a basis $\{\mathfrak{d}_i\}_{1\leq i\leq n}$ of the k-vector space $\mathfrak{g}(k/L)$ completely determined by the condition

$$\mathfrak{d}_i(x_j) = \delta_{ij} \quad \text{for } 1 \leq i, j \leq n.$$

For each integer r we denote $\Omega^r(k/L)$ the k-vector space of the k-multilinear alternating forms of r variables in $\mathfrak{g}(k/L)$. We denote $\Omega^*(k/L)$ the direct sum of the $\Omega^r(k/L)$, indeed the exterior algebra of $\Omega^1(k/L)$. The elements of $\Omega^*(k/L)$ are called *differentials of k over L*.

For $x \in k$ we denote dx the differential $f \in \Omega^1(k/L)$ given by $f(\mathfrak{d}) = \mathfrak{d}(x)$. The application $x \mapsto dx$ from k to $\Omega^1(k/L)$ is L-linear and we have

$$d(xy) = d(x)y + xd(y).$$

Given a p-basis $\{x_i\}_{1\leq i\leq n}$ we have that $< \mathfrak{d}_i, dx_j >= \delta_{ij}$ for $1 \leq i, j, \leq n$. Thus $\{dx_i\}_{1\leq i\leq n}$ is a basis of $\Omega^1(k/L)$ dual to $\{\mathfrak{d}_i\}_{1\leq i\leq n}$, the basis of $\mathfrak{g}(k/L)$. It is well known that there exists a unique L-linear operator d satisfying the relation

$$d(\omega' \wedge \omega) = d\omega' \wedge \omega + (-1)^r \omega' \wedge d\omega, \qquad d(d(\omega)) = 0,$$

for $\omega' \in \Omega^r(k/L), \omega \in \Omega^*(k/L)$, and extending the application $x \mapsto dx$ from $k = \Omega^0(k/L)$ to $\Omega^1(k/L)$. The kernel of d, that we denote by Z, is a subalgebra of the L-algebra $\Omega(k/L)$ and the image of d, denoted B, is an ideal of Z.

Proposition 6.3.1. *Let $\{x_i\}_{1\leq i\leq n}$ be a p-basis of k over L. The subalgebra Z of the L-algebra $\Omega^*(k/L)$ is the direct sum of the ideal B and the L-algebra generated by the elements $f_i = x_i^{p-1} dx_i$, where $1 \leq j \leq n$.*

For simplicity consider the case $L = k^p$, and let $\{x_i\}_{1\leq i\leq n}$ a p-basis of k on k^p. We know that for all the strictly increasing sequences $(i_1, ..., i_r)$ and $f_i = x_i^{p-1} dx_i$, the monomials $f_{i_1} \wedge ... \wedge f_{i_r}$ are a basis of Z modulo B on k^p. Thus we can write any element $\omega \in Z$ as

$$\omega = d\psi + \sum \eta^p_{i_1,...,i_r} f_{i_1} \wedge ... \wedge f_{i_r} \quad \text{for } \psi, \eta_{i_1,...,i_r} \text{ in } k.$$

The *Cartier operator* $\mathcal{C}$ from Z to $\Omega^*(k) := \Omega^*(k/k^p)$ is defined as

$$\mathcal{C}\omega = \sum \eta_{i_1,...,i_r} dx_{i_1} \wedge ... \wedge dx_{i_r}.$$

We can now focus on the particular situation where k is the function field of a hyperelliptic curve. We change our notation. Let C be a complete non-singular curve over k, an algebraically closed field, defined by the equation

$$C : y^2 = f(x),$$

where $f(x) \in k[x]$ is a degree $2g+1$ polynomial. The field $k(C)$ has a unique subfield $k^p(x^p, y^p) = k(x^p, y^p) = k(C)^p$ over which $k(C)$ is separably generated, e.g., $k(C) = k(C)^p(x)$ for a separably generating transcendental element $x \in k(C) \setminus k(C)^p$. The p-basis of this extension is therefore $\{x\}$. Note that since C is a curve $\Omega^*(k(C)) = k \oplus \Omega^1(k(C))$. We consider $\Omega^1(k(C))$ the set of differential forms of degree 1 on $k(C)$ and $d : k(C) \longrightarrow \Omega^1(k(C))$ the canonical derivation of $k(C)$.

Since $dx \neq 0$ for a separating element $x \in k \setminus k^p$ and since $d\omega = 0$ for every $\omega \in \Omega^1(k(C))$, by Proposition 6.3.1, every ω can be expressed uniquely in the form

$$\omega = d\phi + \eta^p x^{p-1} dx \qquad \text{with } \phi, \eta \in k(C).$$

Thus the Cartier operator is given by

$$\begin{aligned} \mathcal{C} : \Omega^1(k(C)) &\longrightarrow \Omega^1(k(C)), \\ \mathcal{C}\omega &= \eta dx. \end{aligned}$$

It is a well defined σ^{-1}-linear operator and $\mathcal{C}(d\phi) = 0$.

It is well known [**29**, II] that the g-dimensional k-vector space $\Omega^1(k(C))$ of differentials forms of degree one of the first kind of $k(C)$ has the following basis

$$\mathcal{B} = \{\omega_i = \frac{x^i dx}{y} : \ i = 0, ..., g-1 \ \}.$$

Due to the work of Manin [**15**], the images of the ω_i's under the Cartier operator $\mathcal{C}$ are determined in the following way. We can rewrite ω_i as

$$\omega_i = \frac{x^i dx}{y} = x^i y^{-p} y^{p-1} dx = y^{-p} x^i \sum_{j=0}^{N} c_j x^j dx,$$

where the coefficients $c_j \in k$ are obtained from the expansion

$$y^{p-1} = f(x)^{\frac{p-1}{2}} = \sum_{j=0}^{N} c_j x^j, \text{ where } N = \frac{p-1}{2}(2g+1).$$

Then we get for $i = 1, ..., g$,

$$\begin{aligned}\omega_i &= y^{-p}(\sum_{\substack{j \\ i+j+1 \not\equiv\ 0 mod p}} c_j x^{j+i} dx) + \sum_{l \geq 0} c_{(l+1)p-(i+1)} x^{(l+1)p-(i+1)+i} y^{-p} dx \\ &= d(y^{-p} \sum_{\substack{j \\ i+j+1 \not\equiv\ 0 mod p}} \frac{c_j x^{j+i+1}}{j+i+1}) + \sum_{l \geq 0} c_{(l+1)p-(i+1)} \frac{x^{lp}}{y^p} x^{p-1} dx.\end{aligned}$$

Note here that

$$0 \leq l \leq \frac{N+i+1}{p} - 1 = \frac{((p-1)/2)(2g+1)+g}{p} - 1 < g - \frac{1}{2}.$$

Thus we have

$$\mathcal{C}\omega_i = \sum_{l=0}^{g-1} c_{(l+1)p-(i+1)}^{1/p} \frac{x^l}{y} dx.$$

This shows that $H^0(C, \Omega_C^1)$ is closed under the Cartier operator $\mathcal{C}$. Thus, we can represent $\mathcal{C}$ by a matrix. Indeed, if we write $\omega = (\omega_1, ..., \omega_g)$, we have

$$\mathcal{C}\omega = A^{(1/p)}\omega,$$

where $A^{(1/p)}$ is the $g \times g$ matrix with elements in k given as

$$A^{(1/p)} = \begin{pmatrix} c_{p-1}^{1/p} & c_{p-2}^{1/p} & \cdots & c_{p-g}^{1/p} \\ c_{2p-1}^{1/p} & c_{2p-2}^{1/p} & \cdots & c_{2p-g}^{1/p} \\ & \cdots & & \\ c_{gp-1}^{1/p} & c_{gp-2}^{1/p} & \cdots & c_{gp-g}^{1/p} \end{pmatrix}.$$

The usual care as to the meaning of representing a σ^{-1} linear operator by a matrix must be exercised. We note that this formula shows that the Cartier operator $\mathcal{C}$: $\Omega^1(k(C)) \longrightarrow \Omega^1(k(C))$ defines a σ^{-1}-linear operator $H^0(C, \Omega^1_{C/K}) \longrightarrow H^0(C, \Omega^1_{C/K})$ that we denote by the same letter $\mathcal{C}$. If we raise to the p power each of the coefficients of the matrix $A^{(1/p)}$, we get the matrix

$$A = \begin{pmatrix} c_{p-1} & c_{p-2} & \cdots & c_{p-g} \\ c_{2p-1} & c_{2p-2} & \cdots & c_{2p-g} \\ & \cdots & & \\ c_{gp-1} & c_{gp-2} & \cdots & c_{gp-g} \end{pmatrix}.$$

This matrix is called the *Cartier-Manin matrix* associated to the hyperelliptic curve C of genus g defined over k. If $S = (s_{ij})$, is a non-singular $g \times g$ matrix with entries in k and $S^{(p)} = (s_{ij}^p)$, then the change of basis for $H^0(C, \Omega^1_{C/K})$ by S results in the Cartier operator being represented by $S^{(p)}AS^{-1}$.

6.4. The Hasse-Witt matrix.

One can also find in again in [**33**, Lemma D, E] that the Hasse-Witt matrix can be identified with the Cartier-Manin matrix of a given curve C/k.

Indeed if we come back the sequence

$$0 \longrightarrow H^0(\mathrm{Jac}(C), \Omega^1_{\mathrm{Jac}(C)}) \longrightarrow H^1_{dR}(\mathrm{Jac}(C)/k) \longrightarrow H^1(\mathrm{Jac}(C), \mathcal{O}_{\mathrm{Jac}(C)}) \longrightarrow 0,$$

we have that $H^0 := H^0(\mathrm{Jac}(C), \Omega^1_{\mathrm{Jac}(C)}) \cong H^0(C, \Omega^1_C)$ is in duality with $H^1 := H^1(\mathrm{Jac}(C), \mathcal{O}_{\mathrm{Jac}(C)})$ *i.e.*:

$$\begin{aligned} < Fx, y > &= < x, Vy >^\sigma \qquad H^1 = (H^0)^\vee \\ < H^1, H^1 > &= 0 \qquad\qquad < H^0, H^0 >= 0. \end{aligned}$$

In fact, writing the matrix of F on H^1, the Hasse-Witt matrix, corresponds to writing the matrix of V in H^0, the Cartier-Manin matrix. Suppose that $\{\zeta_i\}$ is a basis of H^1 and that $\{\eta_i\}$ is a basis of H^0, then $< \zeta_i, \eta_j >= \delta_{ij}$. Then the coefficients of the Cartier-Manin matrix can be written as

$$c_{ji} =< \sum_{k=1}^{g} c_{ki}\zeta_i, \eta_j >=< F\zeta_i, \eta_j > .$$

On the other hand, since $< F\zeta_i, \eta_j > = < \zeta_i, V\eta_j >^\sigma$, we get that a_{ij}, the coefficients of the Hasse-Witt matrix can be recover

$$a_{ij}^\sigma = < \zeta_i, \sum_{k=1}^{g} a_{kj}\eta_j >^\sigma = < \zeta_i, V\eta_j >^\sigma = c_{ij}.$$

Therefore the matrix $A^{(1/p)}$ found in the above calculations is the Hasse-Witt matrix but usually we will consider the matrix to be A.

6.5. Ordinary, non-ordinary and supersingular abelian varieties.

We have encountered the definition of an ordinary genus 1 curve in our previous example and this definition can be extended to hyperelliptic curves of higher genus.

THEOREM 6.5.1. *Let A be a g-dimensional abelian variety over a perfect field k of characteristic p. The following statements are equivalent:*

(1) $|A[p](\overline{k})| = p^g$
(2) $A[p] \otimes_k \overline{k} \cong g(\mu_P \oplus \mathbb{Z}/p\mathbb{Z})$
(3) *The Frobenius map $H^1(A, \mathcal{O}_A) \longrightarrow H^1(A, \mathcal{O}_A)$ is an isomorphism.*

If these properties hold we say that A is *ordinary*, and otherwise we say it is non-ordinary. One can also prove that $f < g$ if and only if $a > 0$. There is in this theorem other statements about Newton polygon and the formal group of Jac(C). They are not relevant for ours needs but for those who could be interested, the complete version, together with the proof, can be found in [**33**]. A genus g curve C is said to be ordinary if its Jacobian Jac(C) is ordinary. By definition, the f-number of a genus g ordinary curve is g, the a-number must be 0 and the Hasse-Witt matrix has non-zero determinant.

A genus g curve C is said to be *non-ordinary* if its Jacobian Jac(C) is not an ordinary abelian variety. For such a curve, the a-number is greater than 0 and the f-number is less than g. Again, this can be translated in terms of the Hasse-Witt matrix. A hyperelliptic curve defined over a field of characteristic $p > 2$ will be non-ordinary if and only if the Hasse-Witt matrix has zero determinant. The non-ordinary curves can be subdivided into supersingular, superspecial and mixed curves.

An abelian variety A over an algebraically closed field of characteristic $p > 0$ is called *supersingular* if there exists an isogeny $A \sim E^n$, where E is a supersingular elliptic curve. Again we say that a curve is supersingular if its Jacobian is supersingular. If A is supersingular abelian variety then $|A[p]| = 1$ but the converse does not hold if the dimension of A is greater then 2. We call A *superspecial* if it is isomorphic to a product of supersingular elliptic curves. We will say that all the other possible non-ordinary curves are of *mixed type*. Note that if $|\mathrm{Jac}(C)[p]| = p^s$ then the p-torsion group of $\mathrm{Jac}(C)$ will have the component $s(\mu_P \oplus \mathbb{Z}/p\mathbb{Z})$.

6.6. Final sequences and classification of rank $2g$ Dieudonnés modules.

As stated before it is possible to construct Dieudonnés modules from p-torsion commutative group schemes. This construction enables us to classify the objects we want to study. To do so, we consider self-dual group schemes with perfect alternating pairing

$$\mathbf{G} \times \mathbf{G} \longrightarrow \mu_p$$

and we say that these group schemes are *symplectic*. This classification is given by this main theorem.

THEOREM 6.6.1. (F. Oort) *Let k be an algebraically closed field of characteristic p, then there exist, up to isomorphisms, 2^g symplectic commutative group schemes $\boldsymbol{G}$ rank p^{2g} killed by p. Moreover, each such group scheme appears as the p-torsion group scheme of some principally polarized g-dimensional abelian variety over k.*

The theorem comes from the following lemma. In the scope of the equivalence of categories, the classification given in this lemma will also allow us to classify the Dieudonnés modules.

LEMMA 6.6.1. *Let k be an algebraically closed field of characteristic p*

a. *Given a group scheme as in Theorem 6.6.1 there exists a final filtration,*

$$\{0\} = \boldsymbol{G}_0 \subset \boldsymbol{G}_1 \subset \cdots \subset \boldsymbol{G}_i \subset \cdots \subset \boldsymbol{G}_{2g} = \boldsymbol{G},$$

with the following properties:

1. $\operatorname{rank} \boldsymbol{G}_i = p^i$;

2. $\boldsymbol{G}_j^{\vee} = \boldsymbol{G}_{2g-j}$;

3. $\operatorname{Ver}(\boldsymbol{G}_j) = \boldsymbol{G}_{\psi(j)}$ *for a suitable function* $\psi : \{0, ..., 2g\} \longrightarrow \{0, ..., 2g\}$ *called a* final sequence.

b. *The function ψ has the following properties:*

1.' $\psi(0) = 0$ *and* $\psi(i) \leq \psi(i+1) \leq \psi(i) + 1$ *for all i;*

2.' $\psi(i+1) = \psi(i) + 1 \Leftrightarrow \psi(2g - i) = \psi(2g - i - 1)$.

c. *Let ψ a final sequence satisfying* $(1')$ *and* $(2')$, *then it determines the isomorphism class of the group $\boldsymbol{G}$ and every such function comes from some group scheme $\boldsymbol{G}^{\psi}$ over k. There are 2^g such functions determined by their values on* $\{0, ..., g\}$.

d. *The f-number of $\boldsymbol{G}^{\psi}$ is* $\max\{i : 0 \leq i \leq g,\ \psi(i) = i\ \}$. *The a-number of $\boldsymbol{G}^{\psi}$ is given by $g - \psi(g)$.*

Thus there are always 2^g such functions and the final sequence is completely determined if we know its first $g + 1$ values. If we omit the first zero the restriction of ψ on the set $\{1, ..., g\}$ is called the *elementary sequence*.

Example: If $g = 1$, we would expect to have two group schemes. We have seen before that we first have the situation of an ordinary elliptic curve, that is when

$E[p](\overline{k}) \cong \mu_p \oplus \mathbb{Z}/p\,\mathbb{Z}$. The filtration is then the following

$$\{0\} \subset \mu_p \subset (\mu_p \oplus \mathbb{Z}/p\,\mathbb{Z}),$$

where $\mathrm{Ver}(\mu_p \oplus \mathbb{Z}/p\,\mathbb{Z}) = \mu_p$ and $\mathrm{Ver}(\mu_p) = \mu_p$. Therefore the function ψ is given by

i	0	1	2
$\psi(i)$	0	1	1

where the a-number is 0 and the f-number is 1. The only other possible final sequence is given by

i	0	1	2
$\psi(i)$	0	0	1

with 1 as a-number and 0 as f-number. The filtration associated to this function is given as

$$\{0\} \subset \mathbb{H} \subset \mathbb{M}$$

where $\mathrm{Ver}(\mathbb{M}) = \mathbb{H}$, $\mathrm{Ver}(\mathbb{H}) = 0$ and $\mathbb{H} \cong \alpha_p$. This filtration corresponds to the situation of a supersingular elliptic curve.

Note that in general, since the f-number of the ordinary curves is g, the sequences associated to these curves, or rather their Jacobians, are the ones where $\psi(g) = g$. There is only one such final sequence, named the *ordinary sequence*, given by

i	0	1	2	...	g	$g+1$	...	$2g$
$\psi(i)$	0	1	2	...	g	g	...	g

Remark also that this consistent with the fact that $a\sharp(\mathrm{Jac}(C)[p]) = \psi(g) - g = 0$.

It is possible to construct the Dieudonné modules associated to these particular group schemes using final sequences. Let ψ be a final sequence and denote by

$$1 \leq m_1 < m_2 < ... < m_g \leq 2g$$

the set of integers i such that $\psi(i-1) < \psi(i)$ and fill the blanks of the length $2g$ string with

$$1 \leq n_g < n_{g-1} < \ldots < n_1 \leq 2g.$$

Note that the integers in the second set are the integer i such that $\psi(i-1) = \psi(i)$ and we have the following relation: $m_i + n_i = 2g + 1$.

The basis for the Dieudonné module can be given as

$$\{\mathcal{Z}_i, \ldots \mathcal{Z}_{2g}\}.$$

It will be convenient to introduce the following notation

$$X_i := \mathcal{Z}_{m_i}, \quad Y_i := \mathcal{Z}_{n_i}, \quad 1 \leq i \leq g.$$

At this point, we need only to construct V, F and the alternating pairing for the module $\oplus_{i=1}^{2g} k \cdot \mathcal{Z}_i$. The two maps are given by

$$\begin{aligned} V(X_i) &= \mathcal{Z}_i, \qquad V(Y_i) = 0, \\ F(\mathcal{Z}_i) &= 0, \quad F(\mathcal{Z}_{2g-i+1}) = \epsilon Y_i, \quad i = 1, .., g. \end{aligned}$$

Here $\epsilon = 1$ if $Z_{2g-i+1} \in \{Y_1, \ldots, Y_g\}$ and $\epsilon = -1$ otherwise. Finally, the pairing is given by

$$\langle X_i, Y_j \rangle = \delta_{ij} \quad \langle X_i, X_j \rangle = 0 = \langle Y_i, Y_j \rangle.$$

Note that Ker$F$ is spanned by $\mathcal{Z}_1, \ldots \mathcal{Z}_g$, Ker$V$ is spanned by $Y_1, \ldots, Y_g$, and $F \circ V = V \circ F = 0$.

For instance, consider for $g = 2$, the final sequence

i	0	1	2	3	4
$\psi(i)$	0	0	1	1	2

This sequence augments at the second and the fourth position (we do not consider the first zero in the set of integers) thus $m_1 = 2$, $m_2 = 4$ and we have the following data:

ψ	0	1	1	2
	n_2	m_1	n_1	m_2
Basis	Z_1	Z_2	Z_3	Z_4
	Y_2	X_1	Y_1	X_2
V	0	Y_2	0	X_1
F	0	0	Y_2	$-Y_1$

which gives the 4 dimensional Dieudonné module $M = \bigoplus_{i=1}^{4} k \cdot Z_i$ together with V, F and the pairing.

Conversely, one can start with M, a $2g$ dimensional Dieudonné module killed by p with $\mathrm{Im}F = \mathrm{Ker}V$, $\mathrm{Im}V = \mathrm{Ker}F$ and with a symplectic pairing and then construct a final sequence which corresponds, by Lemma 6.6.1 to an group scheme with the needed properties. For such module there is always a V-filtration and a F-filtration. The F-filtration of the module corresponds to the Verschiebung filtration of the group schemes. If we apply it to a Dieudonné module constructed from a final sequence, the filtration will give back the original sequence. If instead we consider the V-filtration we would not necessarily get our original sequence.

So using F we need to construct a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{2g-1} \subset M_{2g} = M$$

where the M_i have dimension i and $F(M_i) = M_{\psi(i)}$. To do so we apply F to M to get $M_{i_1} = M_{\psi(2g)}$, we then again apply F to M_{i_1} to get $M_{i_2} = M_{\psi(i_1)}$ and so on until we do not get new modules. We get this way a partial filtration of Dieudonnés modules

$$0 \subset M_{i_s} \subset \cdots \subset M_{i_1} \subset M,$$

with a portion of the final sequence. We then take $M_i^\vee$, the dual of each of these submodules M_i with respect to the pairing and we apply F on each $M_i^\vee$, on their images, etc. We then take the dual of the new submodules and do this algorithm until its stabilizes. Once nothing new can be obtained with this procedure, there is no guarantee that all the submodules will be reached. If so, we consider the first index which is not reached, say j, and the first submodule containing strictly M_{j-1}, say M_k. We define $M_j = M_{j-1} \oplus kZ_j$ where Z_j is the first generator of M_k not in M_{j-1}. We then take the dual of M_j and apply the algorithm until we get all the submodules, indeed the whole final sequence.

We can find in appendix 1, a program that enables us to work with these Dieudonné modules. From a final sequence or from a type (note that the type is not relevant in our considerations but can be pertinent in other situations) the program constructs the Dieudonné module, its F-filtration and thus give back the sequence. Also given s final sequences it compute each Dieudonné modules M_1, M_2,...M_s, the module $M = \bigoplus_{i=1}^s M_i$ and the final sequence associated to M.

6.7. Ekedahl-Oort stratification.

DEFINITION 6.7.1. *Let ψ be a final sequence and let $\mathcal{A}$ the moduli space of principally polarized abelian varieties. Let E_ψ be the locally closed set of $\mathcal{A}$ with the property that its geometric points x are such that $(\mathcal{A}_x[p], \lambda_x)$ has a final sequence ψ.*

We will need a partial order on the final sequences ψ and it is possible to define one as follows,

$$\psi' \prec \psi \Leftrightarrow \psi'(i) \leq \psi(i) \quad \forall i \leq g.$$

With these definitions we can state the following theorem from F. Oort, see [**23**].

THEOREM 6.7.1. *Let ψ be a final sequence then*

(1) *The sets E_ψ form a stratification of the moduli space $\mathcal{A}$. There exists a set $\Delta(\psi)$ that contains all final sequences $\psi' \prec \psi$, and possibly other sequences such that $\overline{E_\psi}$, the closure of E_ψ, is the union of $E_{\psi'}$ for $\psi' \in \Delta(\psi)$. That is*

$$\overline{E_\psi} = \bigcup_{\psi' \in \Delta(\psi)} E_{\psi'}.$$

(2) *The dimension of E_ψ is*

$$\dim(E_\psi) = |\psi| := \sum_{i=1}^{g} \psi(i).$$

If we come back to the example $g = 1$, the one dimensional ordinary locus of the j-line is the stratum of the elementary sequence $\{0, 1\}$, while the stratum of the sequence $\{0, 0\}$ is the zero dimensional supersingular locus. For $g = 2$, the three dimensional ordinary locus is the stratum of the elementary sequence $\{0, 1, 2\}$. The stratum of $\{0, 1, 1\}$ is two dimensional and the stratum of $\{0, 0, 1\}$ is one dimensional and is open and dense in the supersingular locus. Its closure is a family of Moret-Bailly families meeting transversely at the superspecial locus, which is the stratum of the sequence $\{0, 0, 0\}$.

Remark: In general it is not known which $E_{\psi'}$ is in the boundary of E_ψ. Oort gave an example of $E_{\psi'}$ in the boundary of E_ψ and $\psi' \not\prec \psi$.

CHAPTER 2

Exploration

1. General problem

We have seen that given a genus g hyperelliptic curve C defined over a perfect field of characteristic p, we can associate to it a final sequence of $2g$ integers. This sequence is given by the unique final filtration of $\mathrm{Jac}(C)[p]$. The first thing one can try to describe is the subset of the moduli space H_g that corresponds to a given final sequence ψ, *i.e.* a subset on which every point x, that is every hyperelliptic curve C_x, has that fixed final sequence ψ. Also, one can seek to describe the points corresponding to a union of different sequences. For instance, the non-ordinary curves have sequence belonging to the union of all possible sequences except the ordinary sequence. Another way to define sets in the moduli space of curves is to consider for every curve C the final sequence of a curve D associated to C. For example, one can try to describe the curves having some unramified covering of a fixed degree such that the covering curve has a given sequence ψ. This problem seems very difficult in this generality therefore we fix many parameters to ease our study and finally narrow down to the study of unramified double coverings of hyperelliptic curves and even to unramified covering of genus two curves by an non-ordinary genus three curve. This last problem will be the one we will focus on. For the moment, however, we can give an overview of the general question.

We will consider the affine model,

$$C : y^2 = f(x) = \prod_{i=1}^{2g+1} (x - \lambda_i)$$

of a genus g hyperelliptic curve over k, an algebraically closed field of characteristic $p \neq 2$ with a ramification point at infinity. This model is called the Rosenhain normal form and its associated Hasse-Witt matrix is given explicitly in section 6.4. In this setting, the entries of the matrix $A(C) = (a_{ij})$ are

$$a_{ij} = \text{ The coefficient of the degree } i \cdot p - j \text{ term of } f(x)^{\frac{p-1}{2}} .$$

We consider the moduli space H_g of genus g hyperelliptic curves over k. Given a type ψ we define

$$H_g(\psi) = \{x \in H_g \mid \text{The final sequence of } \mathrm{Jac}(C_x)[p] \text{ is } \psi \},$$

and

$$H_g(N) = \{x \in H_g \mid \text{The final sequence of } \mathrm{Jac}(C_x)[p] \text{ is not the ordinary sequence } \}.$$

We would like to describe these sets as subvarieties of the moduli space H_g. As a matter of fact, we will try to describe them in terms of the Weierstrass points. For instance, the condition for a curve to be non-ordinary can be described by a specific polynomial. Indeed the entries of the Hasse-Witt matrix can be expressed in terms of the coefficients of the Rosenhain normal form. Therefore, the Weierstrass points of the curve need to solve the polynomial equation of the determinant.

2. Unramified degree n coverings

Let $\gamma : D \longrightarrow C$ be an unramified degree n covering of a genus g hyperelliptic curve C. The Hurwitz formula

$$2g_D - 2 = (2g_C - 2)\deg(\rho)$$

gives the genus of the covering curve D. So D needs to be a genus $1 + n(g_C - 1)$ curve. We will denote

$$H_{g,n}(\psi, i) = \left\{ \begin{array}{c} x \in H_g \mid \exists\ i \text{ degree } n \text{ unramified coverings } \gamma : D \to C_x \\ \text{where the sequence of } \mathrm{Jac}(D)[p] \text{ is } \psi \end{array} \right\},$$

and denote

$$H_{g,n}(N, i) = \left\{ \begin{array}{c} x \in H_g \mid \exists\ i \text{ degree } n \text{ unramified coverings of } \gamma : D \to C_x \\ \text{where } \mathrm{Jac}(D)[p] \text{ does not have the ordinary sequence} \end{array} \right\}.$$

We will say that these particular coverings of curves are *non-ordinary* coverings. We would also like to find a moduli space $\mathcal{M}$ for these degree n unramified coverings. To do so, consider the two projection maps

$$\pi_1(\gamma : D \longrightarrow C) = C, \quad \text{and} \quad \pi_2(\gamma : D \longrightarrow C) = D.$$

Consider also $t : \mathcal{M}_{1+n(g-1)} \hookrightarrow \mathcal{A}_{1+n(g-1)}$, the Torelli morphism from the moduli space of genus $1 + n(g - 1)$ curves to the moduli space of dimension $1 + n(g - 1)$ abelian varieties which sends a curve to its Jacobian. If we choose a base points $P_0 \in C$ and consider

$$\begin{array}{ccc} C^g & \longrightarrow & \mathrm{Jac}(C) \\ (P_1, ..., P_g) & \mapsto & \displaystyle\sum_{i=1}^{g} (P_i - P_0). \end{array}$$

The theta divisor discussed in Chapter 1 section 5.7 is the image of $C^{g-1} \times \{P_0\}$ and we have seen that it induces $\lambda_{\mathcal{O}(\Theta)}$, a principal polarization that does not depend on P_0. The Torelli morphism is given by

$$C \mapsto (\mathrm{Jac}(C), \lambda_{\mathcal{O}(\Theta)})$$

and is injective with this polarization. Therefore we have the following picture:

$$\begin{array}{ccccc} \mathcal{M} & \xrightarrow{\pi_2} & \mathcal{M}_{1+n(g-1)} & \xhookrightarrow{t} & \mathcal{A}_{1+n(g-1)} \\ \pi_1 \downarrow & & & & \\ H_g & & & & \end{array}$$

It is known that there is a correspondence between unramified degree n abelian coverings of a curve C and degree n maps to its Jacobian. To get a feeling for the situation we can work over $\mathbb{C}$.

Recall that an unramified degree n abelian cover of C corresponds to a normal subgroup $N \lhd \pi_1(C)$ where $\pi_1(C)/N$ is abelian of cardinality n. This normal subgroup corresponds to exactly one subgroup of index n of $\pi_1^{ab}(C) = H_1(C, \mathbb{Z})$. But $H_1(C, \mathbb{Z}) \cong H_1(\mathrm{Jac}(C), \mathbb{Z})$ for $\mathrm{Jac}(C) = \mathbb{C}^g/\mathcal{L}$ and $\mathcal{L}$ a lattice. Then $H_1(\mathrm{Jac}(C), \mathbb{Z}) = \mathcal{L}$ and the index n subgroup corresponds to a sublattice $\mathcal{J} \subseteq \mathcal{L}$ of index n. Therefore the covering induces a map at the level of abelian varieties $\mathbb{C}^g/\mathcal{J} \longrightarrow \mathbb{C}^g/\mathcal{L}$. Also from any such map $\mathbb{C}^g/\mathcal{K} \longrightarrow \mathbb{C}^g/\mathcal{L}$, we can recover an abelian degree n unramified covering of C.

In fact, this correspondence also holds if the curve is defined over an algebraically closed field of characteristic prime to n. For instance, one can find the following in [**20**, §9]:

THEOREM 2.0.2. *If $J' \longrightarrow \mathrm{Jac}(C)$ is an unramified covering of degree n of* $\mathrm{Jac}(C)$*, then $C' = C \times_{Jac(C)} J' \longrightarrow C$ is an unramified covering of degree n of C and every unramified abelian covering of C is obtained this way. Equivalently, the map* $\pi_1(C, p)^{ab} \longrightarrow \pi_1(\mathrm{Jac}(C), 0)$ *is an isomorphism.*

Therefore, a degree n unramified abelian cover of C is equivalent to a subgroup of order n of $\mathrm{Jac}(C)$. Thus we can deduce that the map π_1 is quasi-finite. We can deduce that the map π_2 is also quasi-finite using the following theorem.

THEOREM 2.0.3. (de Franchis-Severi) *Let D be a non-singular projective curve. Then there are only a finite number of finite separable morphisms $\gamma : D \longrightarrow C$ (taken up to isomorphism) where C ranges through all non-singular projective curves of genus ≥ 2.*

There is an analog of this theorem for Riemann surfaces and a proof of it can be found in [**16**, page 227]. We then have the following.

PROPOSITION 2.0.1. *The map π_1 is a finite morphism and the map π_2 is a quasi-finite morphism.*

Proof: From the above discussion, we have that the two maps are quasi-finite and it remain to show that π_1 is finite. It will be sufficient to show that π_1 is a proper morphism of affine varieties, see [**8**, Ex 4.6, page 106]. For the properness of π_1 we will use the following criterion that can be found in [**8**, § II, Theorem 4.7].

THEOREM 2.0.4. (Valuative criterion of properness) *Let $f : X \longrightarrow Y$ be a morphism of finite type, with X noetherian. Then f is proper if and only if for every valuation ring R with quotient field K and for every morphism of* Spec K *to X and* Spec R *to Y forming a commutative diagram*

$$\begin{tikzcd}
\mathrm{Spec}\ K \arrow[r] \arrow[d, "i"'] & X \arrow[d, "f"] \\
\mathrm{Spec}\ R \arrow[r] \arrow[ur, dotted] & Y
\end{tikzcd}$$

there exists a unique morphism Spec $R \longrightarrow X$ *making the whole diagram commutative.*

Remark that we may consider this criterion for a discrete valuation ring R only, see [**8**, § II, Exercise 4.11]. Therefore, we need to show that in the following diagram

$$\begin{tikzcd} \mathrm{Spec}\ K \arrow[r, "f"] \arrow[d, "i"'] & H_g^2 \arrow[d, "\pi_1"] \\ \mathrm{Spec}\ R \arrow[r, "g"] \arrow[ur, dotted, "h"] & H_g \end{tikzcd}$$

we can define a morphism h.

Notice here that giving a map g is equivalent to giving a family of genus g hyperelliptic curves $C_{/R} \longrightarrow \mathrm{Spec}\ R$. (This is essentially a curve whose equations are defined using coefficients from R and has good reduction modulo $\mathfrak{m}$, where $\mathfrak{m}$ is the unique maximal ideal of R.) The canonical map $i : \mathrm{Spec}\ K \longrightarrow \mathrm{Spec}\ R$ corresponds to taking the generic fiber $C_{/K}$ of $C_{/R}$, $C_{/K} = C_{/R} \otimes_R K$. Indeed, we can think of C as a curve over K. And finally, the map f corresponds to giving an unramified double covering $\gamma_{/K} : D_{/K} \longrightarrow C_{/K}$.

So what we need to show is that we can extend $D_{/K}$ to a curve over R and also extend $\gamma_{/K}$ to a morphism $\gamma_{/R} : D_{/R} \longrightarrow C_{/R}$ such that $\gamma_{/R}$ is a double unramified cover.

We have seen that the double covering $\gamma_{/K}$ corresponds to a sugroup $H_{/K}$ of order 2 in $\mathrm{Jac}(C_{/K})$. Let us denote by $B_{/K}$ the quotient $\mathrm{Jac}(C_{/K})/(H_{/K})$. Since $\mathrm{Jac}(C_{/K})$ is principally polarized, we have the following diagram

$$\begin{tikzcd} D_{/K} \arrow[r, dotted] \arrow[d, dotted, "\gamma_{/K}"] & B^{\vee}_{/K} \arrow[d, "\text{degree } 2"] & & \\ C_{/K} \arrow[r, hook] & \mathrm{Jac}(C_{/K}) & \cong & \mathrm{Jac}(C_{/K}) \arrow[d, "\text{degree } 2"] \\ & & & B_{/K} \end{tikzcd}$$

Since $C_{/R}$ is a smooth curve over a discrete valuation ring, there exists an abelian scheme whose generic fiber is $\mathrm{Jac}(C_{/K})$ and special fiber is $\mathrm{Jac}(C \otimes_R (R/\mathfrak{m}))$ that we denote $\mathrm{Jac}(C_{/R})$. This follows from the representability of the functor $\mathrm{Pic}_{C_{/R}}$, see [**1**, 9.3,Theorem 1].

It is well known that $H_{/K}$ can be extended to a unique subgroup scheme $H_{/R}$ of $\mathrm{Jac}(C_{/R})$. In fact, $\mathrm{Jac}(C_{/K})[2]$ is a finite étale group scheme over R, and $H_{/R}$ is the closure of $H_{/K}$ in $\mathrm{Jac}(C_{/R})$. Since $\mathrm{Jac}(C_{/R})$ is also principally polarized, for $B_{/R} := \mathrm{Jac}(C_{/R})/(H_{/R})$, we have the following

$$\begin{tikzcd}
D_{/R} \arrow[r, dotted] \arrow[d, dotted, "\gamma_{/R}"] & B^\vee_{/R} \arrow[d, "\text{degree } 2"] & \\
C_{/R} \arrow[r, hook] & \mathrm{Jac}(C_{/R}) \arrow[r, phantom, "\cong"] & \mathrm{Jac}(C_{/R}) \arrow[d, "\text{degree } 2"] \\
& & B_{/R}
\end{tikzcd}$$

Thus, it follows that $\gamma_{/R}$ is an unramified double cover. Therefore, since this construction commutes with base change, the morphism $\gamma_{/R}$ is an extension of $\gamma_{/K}$, thus π_1 is proper.

We know that the moduli spaces H_g and H_g^2 are both quotients by a finite group of the variety $H_g^* = (\mathbb{P}^1(k) \setminus \{0,1,\infty\})^{2g-1} \setminus \Delta'$, where Δ' is the fat diagonal. We know that the variety $(\mathbb{P}^1(k) \setminus \{0,1,\infty\})^{2g-1}$ is affine, and since Δ' is a divisor, it follows that H_g^* is also an affine variety. Therefore, since they are quotients of an affine variety by an finite group, we can conclude that H_g and H_g^2 are also affine varieties. $\square$

Given a final sequence ψ we have $E_\psi \subseteq \mathcal{A}_{1+n(g-1)}$ an Ekedahl-Oort stratum. We can pull it back to $\mathcal{M}_{1+n(g-1)}$ via t^*, and again pull back to $\mathcal{M}$ via π_2^*. At this point, with the map π_1, we can describe a cycle of H_g relative to the sequence ψ in the following way: $\pi_{1*}(\pi_2^* t^*(E_\psi)) \subseteq H_g$. Remark that π_{1*} is well define since π_1 is finite. Later on, we will be interested in curves having i particular degree n covers, denoted by $H_{g,n}(\psi, i)$, and in a sense they correspond to points of multiplicity i in $\pi_{1*}(\pi_2^* t^*(E_\psi))$.

One can ask what are the possible degrees of unramified covers of hyperelliptic curves which remain hyperelliptic. Machlachlan proved [**13**] that the only possible degrees of unramified normal extensions of hyperelliptic surfaces are $n = 2$ and $n = 4$. He also proves that for $g > 2$, an unramified extension of degree 2 or 4 of a genus g hyperelliptic surface need not to be hyperelliptic. Machlanchlan's results can be shown very simply by using the properties of Weierstrass points on hyperelliptic Riemann surfaces, see [**3**], and these proofs can be extended to hyperelliptic curves.

3. Unramified degree 2 coverings

For the next discussion, we will restrict ourselves to the particular case of degree two coverings and for the beginning we shall give the ideas that lead to the following theorem.

THEOREM 3.0.5. (Farkas [**3**]) *Let C be an genus $g > 1$ hyperelliptic curve defined over a field of odd characteristic and let $\gamma : D \longrightarrow C$ an unramified degree 2 covering. Then the genus of D is $2g-1$ and there are exactly $\binom{2g+2}{2}$ degree 2 unramified coverings for which D is hyperelliptic. The remaining $2^{2g} - 1 - \binom{2g+2}{2}$ are not. In particular when $g = 2$ all the coverings curves are hyperelliptic.*

The calculation of the genus is straightforward using Hurwitz formula. The map $\gamma : D \longrightarrow C$ induces the following degree 2 maps of abelian varieties

$$\begin{array}{ccc} A & & A^{\vee} \\ f\downarrow & & \uparrow f^{\vee} \\ \mathrm{Jac}(C) & \cong & \mathrm{Jac}(C)^{\vee}. \end{array}$$

Thus $\mathrm{Ker}(f^{\vee}) = \{0, P\}$ for P a 2-torsion point and there is a correspondence between unramified double cover of C and $\mathrm{Jac}(C)[2]$. Since $|\mathrm{Jac}(C)[2]| = 2^{2g}$, we then have $2^{2g} - 1$ different coverings of the curve C. Note that two different covering curves can be isomorphic as curves.

Let $W_C = \{\lambda_1, ..., \lambda_{2g+2}\}$ be the set of Weierstrass points of the curve C. We now construct all the 2-torsion points on $\mathrm{Jac}(C)$. Note that for any $\{\lambda_i, \lambda_j\} \subset W_C$ we have

$$h = \frac{x - \lambda_i}{x - \lambda_j}, \text{ and } (h) = 2\lambda_i - 2\lambda_j$$

thus $\lambda_i - \lambda_j \in \mathrm{Jac}(C)[2]$. Without lost of generality, we let $v \in W_C$ be the point at infinity, thus $f(x)$ has odd degree, and take $s \subseteq W_C$ any set of even cardinality. We consider the divisor of the form

$$D_s = \sum_{\lambda_i \in s} (\lambda_i - v) \in \mathrm{Jac}(C).$$

One easily shows that D_s belongs to $\mathrm{Jac}(C)[2]$. Since there are 2^{2g+1} such divisors and only 2^{2g} non-zero points having order at most 2, there is necessarily some repetition. The following lemma gives us the complete description of $\mathrm{Jac}(C)[2]$, (corresponding to degree 2 unramified double coverings) in terms of the Weierstrass points.

LEMMA 3.0.1. *Let $v \in W_C$, and $s \subseteq W_C$, a set of even cardinality. Let $D_s = \sum_{\lambda_i \in s} (\lambda_i - v)$, a point in* $\mathrm{Jac}(C)[2]$. *Then $D_s = D_t$ if and only if $t = W_C \setminus s$.*

Proof: Note that D_s is defined also for s of odd cardinality and $D_s = D_{s \cup \{v\}} = D_{s \setminus \{v\}}$. Remark also that if $s_1 \cap s_2 = s_3$, then $D_{s_1} + D_{s_2} = D_{(s_1 \cup s_2) \setminus s_3}$, and we may subtract or add v to $(s_1 \cup s_2) \setminus s_3$ to have even cardinality. Therefore $D_s - D_t = D_s + D_t = 0$ if and only if $D_{s\cup t \setminus s\cap t} = 0$, thus showing the lemma is equivalent to show that for a set of even cardinality we have $D_s = 0$ exactly when $s = W_C$ or $s = \varnothing$.

Note first that since $(y^2) = f(x) = 2D_{W_C}$ we have that $(y) = D_{W_C} = 0$. On the other hand, if for $s \neq \varnothing$ we have $D_s = 0$, then there is a function on C, say g, such that $(g) = \sum_{\lambda_i \in s}(\lambda_i - v)$. Therefore, we have $g^2 = f_1(x) := \prod_{\lambda_i \in s\setminus v}(x - \lambda_i)$. If $|s \setminus v| < 2g + 1$ we get a contradiction with the fact that the genus of the curve is g. Since s can't have $2g + 1$ elements, we get that $s = W_C$. $\square$

Therefore all the coverings will correspond to some 2-torsion point given by a divisor D_s. In terms of function fields, such coverings can be given in terms of degree two Galois extensions of the function fields $k(C)$. Recall that:

$$k(C) = k(x)[\sqrt{f}] = k(x)[\sqrt{\textstyle\prod_{k=1}^{2g+1}(x-\lambda_k)}],$$

where the λ_i are in W_C. Thus

$$k(D) = k(C)[\sqrt{h}] = k(C)[z]/(z^2 - h(x)).$$

where $h \in k(C)$ and $(h) = 2D_s$ for some set $s \subset W_C$ of $2r$ elements. This function field can also be described as

$$K(D) = \frac{k(x)[y]}{(y^2 - f(x))} \otimes_{k(x)} \frac{k(x)[z]}{(z^2 - h(x))}.$$

This shows that D is the normalization of $C \times_{\mathbb{P}^1} k(F)$, where F is a curve with function field $\frac{k(x)[z]}{(z^2-h(x))}$. Some automorphisms of D can be given explicitly. The Galois group of the extension is

$$\Gamma = \mathrm{Gal}(k(D)/k(x)) =< \iota, \sigma >\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

where the two generators are given by

$$\iota : \begin{cases} x \mapsto x \\ y \mapsto -y \\ z \mapsto z \end{cases} \qquad \sigma : \begin{cases} x \mapsto x \\ y \mapsto y \\ z \mapsto -z \end{cases} .$$

From Galois theory, the subsets of Γ give us the following three subfields:

$$\begin{tikzcd}
& k(D) & \\
k(C) \arrow[ur, "\sigma"] & k(E) \arrow[u, "\sigma \cdot \iota"'] & k(F) \arrow[ul, "\iota"'] \\
& k(x) \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proposition 3.0.2. *Let C be a genus g hyperelliptic curve defined over a field of odd characteristic and let $s \subset W_C$ with $|s| = 2r$. Then for the unramified double covering $\gamma : D \longrightarrow C$ defined by D_s, there are two other coverings, $\psi : D \longrightarrow F$ and $\epsilon : D \longrightarrow E$, where E and F are hyperelliptic curves of genus respectively $r-1$ and $g-r$.*

Proof: We consider first the subfield fixed by ι:

$$k(F) = k(x)[\sqrt{h}] = k(x)[z]/(z^2 - h(x)).$$

We then have a hyperelliptic curve F with Weierstrass set s, thus of genus $r-1$. On the other hand, if we consider the subfield fixed by $\sigma \cdot \iota$ we get

$$k(E) = k(x)[\sqrt{g}] = k(x)[t]/(t^2 - g(x)),$$

where $g(x) = f(x)/h(x)$ and $t = y/z$. In fact $(g) = 2D_{W_C \setminus s} = 2D_t$ and $|t| = 2(g-r)-2$. Therefore E is also a hyperelliptic curve of genus $g-r$. $\square$

Note that we clearly see the symmetry discussed in Lemma 3.0.1. Indeed, if consider $W_C \setminus s$, instead of s, we get the same covering; we only interchange $k(F)$ with $k(E)$. Therefore, we will only consider the sets s where $|s| \leq g+1$ and the following corollary is almost immediate.

COROLLARY 3.0.1. *Let C be a genus g hyperelliptic curve defined over a field of odd characteristic and let $\gamma : D \longrightarrow C$ be a degree two unramified covering. Then there exists $\binom{2g+2}{2}$ coverings for which D is hyperelliptic. Furthermore one can associate a genus $g-1$ hyperelliptic curve to each such coverings.*

Proof: We have seen that D is an hyperelliptic curves if and only if it is a double covering of the projective line and such covering corresponds to an inclusion $k(t) \hookrightarrow k(D)$. If the genus of the curve D is greater than 3, from the Proposition 3.3.1 seen in the first section, since

$$g_d \geq [k(D) : k(x)] = 4$$

we get $k(x) \subset k(t)$. Thus, by Galois theory, D can only be a double cover of the three curves C, E and F. Therefore one of these curves need to be the projective line. Since $|s| \leq 2g$ the curve with lower genus is F with genus $r-1=0$, thus $|s| = 2r = 2$. The only other possible genus for the curve D is 3 and in this particular situation, $g=2$, $r=1$ and $|s|=2$, therefore F is also the projective line. Since there is $\binom{2g+2}{2}$ way to choose 2 points in W_C we get exactly $\binom{2g+2}{2}$ such coverings and the curve E will necessarily have genus $g-1$. $\square$

Later, we will try to understand the action of Froebenius on $\mathrm{Jac}(D)$. Using the decomposition made in Proposition 3.0.2 it will be possible to decompose this action in three parts.

THEOREM 3.0.6. *Let C be a genus g hyperelliptic curve defined over a finite field of odd characteristic, and $\gamma : D \longrightarrow C$ an unramified double covering.*

(1) *The map*

$$\Psi : \mathrm{Jac}(C) \oplus \mathrm{Jac}(E) \oplus \mathrm{Jac}(F) \longrightarrow \mathrm{Jac}(D)$$

is an isogeny.

(2) *The kernel of Ψ in contained in*

$$\mathrm{Jac}(C)[4] \oplus \mathrm{Jac}(E)[4] \oplus \mathrm{Jac}(F)[4].$$

Proof: (1)Note first that both sides are abelian varieties that have the same dimension

$$g + (r-1) + (g-r) = 2g-1.$$

Thus, it is enough to show that Ψ is surjective. For $\gamma : D \longrightarrow C$ we have

$$\begin{aligned}
\Psi(\mathrm{Jac}(C)) &= \gamma^*(\mathrm{Jac}(C)) \subset \mathrm{Ker}(1-\sigma) =: C', \\
\Psi(\mathrm{Jac}(E)) &= \epsilon^*(\mathrm{Jac}(E)) \subset \mathrm{Ker}(1-\sigma\iota) =: E', \\
\Psi(\mathrm{Jac}(F)) &= \psi^*(\mathrm{Jac}(F)) \subset \mathrm{Ker}(1-\iota) =: F'.
\end{aligned}$$

We then have the following diagram

$$\begin{tikzcd}
C' + E' + F' \arrow[r, phantom, "\overset{\Psi'}{\subset}"] & \mathrm{Jac}(D) \\
\mathrm{Jac}(C) \oplus \mathrm{Jac}(E) \oplus \mathrm{Jac}(F), \arrow[u, "\Phi"] \arrow[ur, "\Psi"] &
\end{tikzcd}$$

where Φ is the composition

$$\mathrm{Jac}(C) \oplus \mathrm{Jac}(E) \oplus \mathrm{Jac}(F) \subset C' \oplus E' \oplus F' \longrightarrow C' + E' + F'.$$

Note here that the elements which are invariant under the automorphisms σ, ι and $\sigma\iota$ are divisor classes. For the needs of the proof we need to show that for an element β in, say C without lost of generality, there is always a representative which is σ-invariant. Indeed consider the divisor δ representing β then

$$\delta - \sigma(\delta) = (f).$$

Since $\sigma^2 = id$ we also get that

$$(\sigma(f)) = \sigma(f) = \sigma(\delta) - \delta = (f^{-1}),$$

which implies that $f \cdot \sigma(f)$ is constant, without lost of generality say equal to 1. We can apply Hilbert's Theorem 90 , see [**12**, Theorem 6.1], to $f \cdot \sigma(f)$. Hence there is a function g such that $g/\sigma(g) = f$. Then

$$[\delta + \sigma(g)] - \sigma[\delta + \sigma(g)] = (f) + \sigma(g) - (g) = 0,$$

thus $(\delta + \sigma(g))$ is a representative of β which is σ-invariant as a divisor. Consider now the exact sequence

$$0 \longrightarrow \mathrm{Jac}(D)[2] \cap C' \longrightarrow C' \xrightarrow{\times 2} 2C' \longrightarrow 0.$$

Since $\mathrm{Jac}(D)[2]$ is finite $2C' \subset C'$ will have finite index. For any $\beta \in C'$ take a σ-invariant representative β' and $\alpha = \gamma_*(\beta') \in \mathrm{Jac}(C)$, thus $\gamma^*(\gamma_*(\beta')) = \beta_1 + \beta'$, where $\sigma(\beta_1) = \beta'$. But since β' is σ invariant $\gamma^*(\gamma_*(\beta')) = 2\beta' \in \Psi(\mathrm{Jac}(C))$. Therefore $2C' \subset \Psi(\mathrm{Jac}(C))$ which implies that $\Psi(\mathrm{Jac}(C)) \subset C'$ will also have finite index. By doing it for F and E we conclude that the image of the map Φ has finite index.

We need to show now that the inclusion Ψ' is surjective. For any δ in $\mathrm{Jac}(D)$ we can write $2\delta = (1+\sigma)\delta + (1-\sigma)\delta$. We get easily that $(1+\sigma)\delta$ is in $\mathrm{Ker}(1-\sigma) = C'$ and we denote $(1-\sigma)\delta$ by δ_1. It is again possible to write $2\delta_1$ as $(1+\iota)\delta_1 + (1-\iota)\delta_1$

where $(1+\iota)\delta_1 \in \mathrm{Ker}(1-\iota) = F'$ and since

$$\begin{aligned}(1-\sigma\iota)(1-\iota)\delta_1 &= (1-\sigma\iota)(1-\iota)(1-\sigma)\delta \\ &= (1-\iota\sigma-\iota-\sigma+\iota^2\sigma+\iota\sigma^2+\iota\sigma-\iota^2\sigma^2)\delta \\ &= (1-\iota\sigma-\iota-\sigma+\sigma+\iota+\iota\sigma-1)\delta = 0\delta = 0,\end{aligned}$$

we get that $(1-\iota)\delta_1$ is in $\mathrm{Ker}(1-\sigma\iota) = E'$. Since $\mathrm{Jac}(D)$ is divisible, there exists $\eta \in \mathrm{Jac}(D)$ such that $\eta = 4\delta$ so we can decompose δ in three parts

$$\delta = 4\eta = (1+\sigma)2\eta + (1-\sigma)(1+\iota)\eta_1 + (1-\sigma)(1-\iota)\eta_1,$$

respectively in C', F' and E'. Since the image of $\Psi = \Phi$ has finite index and is an abelian variety having the same dimension as $\mathrm{Jac}(C)$ we conclude that Ψ is surjective.

(b) Consider now $w = (x, y, z) \in \mathrm{Jac}(C) \oplus \mathrm{Jac}(E) \oplus \mathrm{Jac}(F)$ an element in the kernel of Ψ. Then we have $x + y + z = 0$ and also $\sigma x + \sigma y + \sigma z = 0$. If we add these two equations, since x is σ-invariant, we get

$$0 = 2x + (1+\sigma)y + (1+\sigma)z.$$

Again we get easily that $(1+\sigma)z$ is σ-invariant and furthermore $(1+\sigma)z$ is still in $\mathrm{Jac}(F)$. Indeed σ corresponds to the involution of F thus $\sigma z \in \mathrm{Jac}(F)$, so is $z + \sigma z$.

Since F is an hyperelliptic curve, there is a double covering $\rho : F \longrightarrow \mathbb{P}^1$ that induces $\rho^* : \mathrm{Jac}(\mathbb{P}^1) \longrightarrow \mathrm{Jac}(E)$. By the same argument as above, we have that twice any σ-invariant element lead to an element in $\mathrm{Jac}(\mathbb{P}^1)$ and since $\mathrm{Jac}(\mathbb{P}^1)$ is trivial, we get that

$$2(1+\sigma)z = 0.$$

The same argument hold for $(1+\sigma)y$ and we get:

$$0 = 4x + 2(1+\sigma)y + 2(1+\sigma)z = 4x.$$

By applying the same argument for y, and z, respectively with $\iota\sigma$ and ι we get that $4y = 4z = 0$ which allows us to conclude the theorem. $\square$

It is interesting to describe the p-torsion group of $\mathrm{Jac}(D)$ in terms of this isogeny.

COROLLARY 3.0.2. *For all primes $p > 2$ there is an isomophism between the p-torsion group of* $\mathrm{Jac}(D)$ *and the p-torsion group of* $\mathrm{Jac}(C) \oplus \mathrm{Jac}(E) \oplus \mathrm{Jac}(F)$.

Therefore the action of F on $H^0(\mathrm{Jac}(D), \Omega_{\mathrm{Jac}(D)})$ decomposes in three parts on

$$H^0(\mathrm{Jac}(C), \Omega_{\mathrm{Jac}(C)}) \oplus H^0(\mathrm{Jac}(E), \Omega_{\mathrm{Jac}(E)}) \oplus H^0(\mathrm{Jac}(F), \Omega_{\mathrm{Jac}(F)}).$$

Let $A(X)$ be the Hasse-Witt matrix of X. It is then possible to describe the Hasse-Witt matrix of the curve D in the following way:

$$A(D) = \begin{pmatrix} A(C) & 0 & 0 \\ 0 & A(E) & 0 \\ 0 & 0 & A(F) \end{pmatrix}.$$

From now on we will concentrate on the specific coverings $\gamma : D \longrightarrow C$ for which D is hyperelliptic. Since $|s| = 2$, such a covering corresponds to a choice of two points $\{\lambda_i, \lambda_j\} \subset W_C$. We will denote the polynomial h by h_{ij}, the covering curve by D_{ij} and the genus $g-1$ curve by E_{ij}. Note that two curves D_{ij} and D_{kl} can be isomorphic and recall that E_{ij} has function field

$$k(E_{ij}) = k(x)[\sqrt{\textstyle\prod_{\substack{\lambda_k \in W_C \\ k \notin \{i,j\}}} (x - \lambda_k)}].$$

In this particular situation, we have a correspondence between degree 2 unramified covering and points in H_g^2, the moduli space of genus g hyperelliptic curves with a choice of 2 Weierstrass points. The map ϵ can be translated in terms of moduli space to give the following:

$$\begin{aligned} \epsilon : H_g^2 &\longrightarrow H_{g-1} \\ (C, \{\lambda_i, \lambda_j\}) &\mapsto (W_C \setminus \{\lambda_i, \lambda_j\}). \end{aligned}$$

In terms of moduli space we get this new picture:

$$\begin{array}{ccccc} & & H_{2g-1} & \overset{\mathrm{t}}{\hookrightarrow} & \mathcal{A}_{2g-1} \\ & \nearrow & & & \\ H_g^2 & \xrightarrow{\epsilon} & H_{g-1} & \overset{\mathrm{t}}{\hookrightarrow} & \mathcal{A}_{g-1} \\ \rho \downarrow & & & & \\ H_g & & & & \end{array}$$

We now will focus on a particular subset of H_g^2: the non-ordinary coverings, that we will denote N_g. That is the space on which a geometric point corresponds to $\gamma : D \longrightarrow C$ where $\mathrm{Jac}(D)$ is non-ordinary abelian variety.

Proposition 3.0.3. *The subset N_g of H_g^2 corresponding to unramified degree 2 non-ordinary coverings of a genus g hyperelliptic curve is a divisor.*

Proof: We have seen that H_g^2 is a variety of dimension $2g-1$. Since it has finite cover H_g^* which is irreducible, H_g^2 is also irreducible. We can consider f, the polynomial given by the determinant of the Hasse-Witt matrix. Since our field is algebraically closed $N_g = \mathcal{Z}(f) \neq \varnothing$ is a hypersurface. Thus every irreducible component of the intersection has dimension $\geq 2g-2$ by [**29**, I§7.1]. Since $N_g \subsetneq H_g^2$, it has codimension 1, thus it is a divisor. $\square$

To describe this divisor, we will use the decomposition made in proposition 3.0.6. Considering the Jacobians of the curves C, D_{ij} and E_{ij} we have the following isogeny:

$$\mathrm{Jac}(D_{ij}) \sim \mathrm{Jac}(E_{ij}) \times \mathrm{Jac}(C).$$

And again the action of Verschiebung on $H^0(\mathrm{Jac}(D_{ij}), \Omega_{\mathrm{Jac}(D_{ij})})$ decomposes in two parts on $H^0(\mathrm{Jac}(C), \Omega_{\mathrm{Jac}(C)}) \oplus H^0(\mathrm{Jac}(E_{ij}), \Omega_{\mathrm{Jac}(E_{ij})})$. Thus, the Hasse-Witt matrix can be written as:

$$A(D_{ij}) = \begin{pmatrix} A(C) & 0 \\ 0 & A(E_{ij}) \end{pmatrix}.$$

Therefore, if C is non-ordinary, that is if $det(A(C)) = 0$, necessarily the $\binom{2g+2}{2}$ coverings D_{ij} will also be non-ordinary. This is the trivial way to have non-ordinary covering. If C is ordinary, the only way to have a zero determinant for $A_{D_{ij}}$ will occur when $\det(A(E_{ij})) = 0$, when E_{ij} is non-ordinary.

Hence, it is possible to decompose N_g in the following way. From the projection $\rho : H_g^2 \longrightarrow H_g$ we get $\rho^{-1}(H_g(N))$ a subset of N_g. From the map $\epsilon : H_g^2 \longrightarrow H_{g-1}$ we get $\epsilon^{-1}(H_{g-1}(N))$ which is also a subset of N_g given by

$$W_E \quad \mapsto \left\{ \begin{array}{r} (W_E \cup \{x,y\}, \{x,y\}) \; | W_E = \text{Weierstrass set of the curve E} \\ \text{where} \;\; x, y \notin W_E \text{ are distinct} \end{array} \right\}.$$

Using this decomposition we can write N_g as $\rho^{-1}(H_g(N)) \cup \epsilon^{-1}(H_{g-1}(N))$ and one interesting problem would be to describe the set $\rho^{-1}(H_g(N)) \cap \epsilon^{-1}(H_{g-1}(N))$.

Another decomposition of N_g can be made from Theorem 3.0.6. Indeed, the variety N_g decomposes in two disjoints sets:

$$N_g = N_{gn} \cup N_{go}$$

where

$$\begin{aligned} N_{gn} &= \{ x \in H_g^2 \text{ such that } C \text{ is non-ordinary } \}, \\ N_{go} &= \{ x \in H_g^2 \text{ such that } C \text{ is ordinary and } E_{ij} \text{ is non-ordinary } \}. \end{aligned}$$

Remark that $\rho^{-1}(H_g(N)) = N_{gn}$ and $\epsilon^{-1}(H_{g-1}(N)) \supseteq N_{go}$. Later we will consider curves for which all the degree 2 unramified coverings are non-ordinary in a non-trivial way. We call such curves *maxno*-2 and denote $\widetilde{H_g}$ the subspace of the moduli space H_g consisting of all the maxno-2 curves. Using these decompositions we can try to build all these spaces by induction and the base step will be to understand the situation for genus 1 hyperelliptic curves.

3.1. $H_1(N)$, non-ordinary elliptic curves.

Any elliptic curve E can be given as a set of 4 Weierstrass points say $W_E = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$. One can easily find in the literature, for instance in [**27**], that given two sets of ordered and distinct three points in $\mathbb{P}^1(k)$, say $[a_1, a_2, a_3]$ and $[b_1, b_2, b_3]$ there is an unique $\varphi \in PGL_2(k)$ such that $\varphi(a_i) = b_i$ for $i \in \{1, 2, 3\}$. Therefore, we can label the set of Weierstrass points W_E to get an ordered set, say $W_E^* = [\beta_1, \beta_2, \beta_3, \beta_4]$ and by an appropriate $\varphi \in PGL_2(k)$ we can send W_E^* to $[\ 0, 1, \infty, \lambda]$. λ is the image of the fourth point by φ and this point is called the *cross ratio* of this particular ordering of W_E^*. Notice that in general, given a different ordering, we get a different cross-ratio. We expect 4! possible cross-ratios but luckily several are the same and there is always at most 6 possible values. If the cross ratio of $[a, b, c, d]$ is λ, depending of the ordering of these four points, we get the following cross-ratios:

$$\left\{\lambda,\ 1-\lambda\ , \frac{1}{\lambda}, \frac{(\lambda-1)}{\lambda}, \frac{1}{(1-\lambda)}, \frac{\lambda}{(\lambda-1)}\right\},$$

and we will denote this set by $[\lambda]$. The cross-ratio of four points $A = [a, b, c, x]$ can also be describe as

$$cr(A) := \frac{(x-a)(b-c)}{(x-c)(b-a)}$$

which can be considered as element in $PGL_2(k)$ with the usual special care for the point at infinity. We will denote $\widetilde{cr}$ the map sending W, an unordered set of four distinct points, to its cross-ratio set $[cr(W)]$.

It follows that the Rosenhain form of the elliptic curve can be rewritten as

$$E_\lambda := y^2 = x(x-1)(x-\lambda),$$

for $\lambda \in k - \{0,1\}$. It is also called the *Legendre form.* If we consider the moduli space of elliptic curves, for $\lambda \in k - \{0,1\}$, it is possible with simple calculation to get the j-invariant of E_λ:

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

Of course, by easy calculation, we check that the j-invariant is independent of the choice of the element in $[\lambda]$

Notice that this association respects isomorphism classes since given any $\delta \in PGL_2(k)$, we have $cr([a,b,c,d]) = cr([\delta(a),\delta(b),\delta(c),\delta(d)])$. Also, if two different ordered sets give the same cross ratio there exists $\delta \in PGL_2(k)$ sending one to the other, see [**27**] for more details. One can also find, for instance in [**29**, V§4], that the above association is exactly six-to-one except for two special cases. For $j = 0$ and $j = 1728$ the association is two-to-one and three-to-one, respectively.

Thus, for a genus 1 curve given by $W' = [0,1,\infty,\lambda]$, the Hasse-Witt matrix has only one component, the coefficient of x^{p-1} in $f(x)^m = (x(x-1)(x-\lambda))^m$, where $m = \frac{p-1}{2}$. Easy computations, see [**29**, V§4] for details, give us the one-by-one Hasse-Witt matrix:

$$A(E_\lambda) = \sum_{l=0}^{m} \binom{m}{l}^2 \lambda^l, \qquad m = \frac{p-1}{2}.$$

Therefore, the non-ordinary elliptic curves, also known as the *supersingular* elliptic curves, correspond to the roots of $A(x)$, a degree $\frac{p-1}{2}$ polynomial. Note that if an element in $[\lambda]$ is a root of this polynomial, the five other elements will also be roots of the same polynomial. Also, one can show that up to isomorphism, there are exactly

$$\left[\frac{p}{12}\right] + \varepsilon_p$$

supersingular elliptic curves in characteristic p, where $\varepsilon_3 = 1$, and for $p \geq 5$,

$$\varepsilon_p = 0, 1, 1, 2 \quad \text{if} \quad p \equiv 1, 5, 6, 11 \bmod 12;$$

see [**29**, V.§4] for details.

3.2. N_2, non-ordinary covering of genus 2 hyperelliptic curves.

For C, a genus 2 hyperelliptic curve with an affine model $y^2 = f(x)$, the Hasse-Witt matrix is given by

$$A(C) := \begin{pmatrix} C_{f,p-1} & C_{f,p-2} \\ C_{f,2p-1} & C_{f,2p-2} \end{pmatrix},$$

where the $C_{f,a}$ corresponds to the coefficient of x^a in $f(x)^{\frac{p-1}{2}}$. The non-ordinary curves are the ones for which $C_{f,p-1}C_{f,2p-2} - C_{f,p-2}C_{f,2p-1} = 0$ and the subset $H_2(N)$ is two dimensional. As stated before, all coverings of such curves will be non-ordinary, *i.e.*, $\rho^{-1}(H_2(N)) \subset N_2$.

The non-trivial non-ordinary unramified double coverings arise when the associated genus 1 curve is non-ordinary. Given a ordinary curve C, with Weierstrass points $W_C = \{\lambda_1, ..., \lambda_6\}$, we will have a non-ordinary covering associated to $s_{ij} = \{\lambda_i, \lambda_j\}$ if and only if the cross-ratio of the four points in $W_C \setminus s$ is a root of the degree $\frac{p-1}{2}$ polynomial $A(x)$. That is, if for the multivalued map:

$$\begin{aligned} \epsilon : H_2^2 &\longrightarrow \lambda\text{−line} \\ (C, s_{ij}) &\mapsto \widetilde{cr}(W_C \setminus s_{ij}), \end{aligned}$$

we have that $\epsilon(C, s_{ij})$ is a root of the polynomial $A(x)$.

Definition 3.2.1. *Let C be a genus 2 hyperelliptic curve given by six Weierstrass points $W = \{\lambda_1, ..., \lambda_6\}$. We say that the set $s_{ij} = \{\lambda_i, \lambda_j\}$ is a supersingular set if and only if the elliptic curve given by the remaining four points is supersingular.*

One question we are interested in answering is the following: is it possible that a genus two curve has $\binom{6}{2} = 15$ non-ordinary coverings in a non-trivial way? Or equivalently does there exist a genus 2 maxno-2 curve? If so, does it imply that the curve C is also non-ordinary? In fact,using our previous notation, we are trying to describe

$$\widetilde{H_g} \cap H_2(O) \text{ in } H_2 \text{ or equivalently } \rho^{-1}(\widetilde{H_g}) \cap N_{2o} \text{ in } H_2^2.$$

Explicitly, we are seeking the hyperelliptic curves for which the 15 couples of Weierstrass points are supersingular. As noted before, if a curve admits non-trivial automorphisms, the number of elements in the fiber will be less then 15, therefore less conditions will be needed to be satisfied. We will study this question later, after a better comprehension of the moduli spaces involved.

One can also associate points in H_2^* with double coverings simply by considering the first two points in the Weierstrass ordered set to be in s_{ij}. The association is then given by the map $\epsilon^* = \epsilon \circ \rho_2$ by

$$\begin{aligned} \epsilon^* : H_2^* &\longrightarrow \lambda\text{-line} \\ (C, [a, b, c, d, e, f]) &\mapsto \widetilde{cr}([c, d, e, f]), \end{aligned}$$

Clearly this association in not one-to-one but given a point (C, s) in H_2^2 all the elements $(C, \hat{s})$ in the fiber of $\rho_2 : H_2^* \longrightarrow H_2^2$ will have the same behaviour as (C, s). That mean that (C, s) will corresponds to a supersingular elliptic curve if and only if any element $(C, \hat{s})$ in the fiber corresponds to a supersingular curve. Since the moduli space H_2^* is easier to study then H_2^2, instead of considering (C, s_{ij}), we will consider only one element in its fiber.

Given λ, a root of the polynomial $A(x)$, the elements in H_2^* corresponding to the "supersingular" points will be ${\epsilon^*}^{-1}(\lambda) = [x, y, \lambda_1, \lambda_2, \lambda_3, \lambda_4]$ where x, and y can be almost anything and $[\lambda_1, \lambda_2, \lambda_3, \lambda_4]$ is unique up to PGL_2. Therefore, for all the roots of $A(x)$ we get two dimensional subsets of H_2^* denoted $H_2^*(\lambda)$. These subsets are also disjoint since one element in H_2^* is associated to only one cross ratio via the map ϵ^*. Thus $N_{2o}^* := \rho_2^{-1}(N_{go}) = \cup_{\lambda_i} H_2^*(\lambda_i)$ and our main question turns out to be: Given a curve C, is it possible that all the elements in the fiber of ρ_2 belong to N_{2o}^*?

Consider a point $W_C := \{0, 1, \infty, \lambda_1, \lambda_2, \lambda_3\}$ in H_2 associated to the curve C, then the 15 elements in the fiber $\rho^{-1}(C)$ in H_2^2 are the following:

$$\begin{array}{ccccc}
(W_C,\{\lambda_1,\lambda_2\}) & (W_C,\{0,\lambda_1\}) & (W_C,\{1,\lambda_1\}) & (W_C,\{\infty,\lambda_1\}) & (W_C,\{0,1\}) \\
(W_C,\{\lambda_1,\lambda_3\}) & (W_C,\{0,\lambda_2\}) & (W_C,\{1,\lambda_2\}) & (W_C,\{\infty,\lambda_2\}) & (W_C,\{0,\infty\}) \\
(W_C,\{\lambda_2,\lambda_3\}) & (W_C,\{0,\lambda_3\}) & (W_C,\{1,\lambda_3\}) & (W_C,\{\infty,\lambda_3\}) & (W_C,\{1,\infty\}),
\end{array}$$

Thus, to study these elements (C, s) we have seen that we can, for each of them, study only one element in the fiber $\rho_2^{-1}(C, s)$. Thus to decide if a curve is a maxno-2 curve it will suffice to study this (non unique) set of elements in H_2^*, that we will denote by $W^*(C)$:

$$\begin{array}{ccccc}
[\lambda_1,\lambda_2,0,1,\infty,\lambda_3] & [0,\lambda_1,1,\infty,\lambda_2,\lambda_3] & [1,\lambda_1,0,\infty,\lambda_2,\lambda_3] & [\infty,\lambda_1,0,1,\lambda_2,\lambda_3] & [0,1,\infty,\lambda_1,\lambda_2,\lambda_3] \\
[\lambda_1,\lambda_3,0,1,\infty,\lambda_2] & [0,\lambda_2,1,\infty,\lambda_1,\lambda_3] & [1,\lambda_2,0,\infty,\lambda_1,\lambda_3] & [\infty,\lambda_2,0,1,\lambda_1,\lambda_3] & [0,\infty,1,\lambda_1,\lambda_2,\lambda_3] \\
[\lambda_2,\lambda_3,0,1,\infty,\lambda_1] & [0,\lambda_3,1,\infty,\lambda_1,\lambda_2] & [1,\lambda_3,0,\infty,\alpha_1,\lambda_2] & [\infty,\lambda_3,0,1,\lambda_1,\lambda_2] & [1,\infty,0,\lambda_1,\lambda_2,\lambda_3].
\end{array}$$

To show that a curve C is maxno-2, we will have to check if all the elements in $W^*(C)$ correspond to a supersingular elliptic curve via the map ϵ^*. Using this particular subset of $\rho_1^{-1}(C)$ we can state the following theorem.

THEOREM 3.2.1. *Let k be an algebraically closed field of odd characteristic. Up to isomorphism, there is only a finite number of genus 2 maxno-2 hyperelliptic curves C over k, i.e., curves having 15 supersingular sets of Weierstrass points. Furthermore if the characteristic of k is p, there are at most $\frac{(p-1)(p-3)(p-5)}{2}$ such hyperelliptic curves.*

Proof: In order to get such curve it is necessary that the 15 chosen elements in H_2^*, the elements in $W^*(C)$, correspond to supersingular points. In particular, the three elements

$$\lambda_3^* := [\lambda_1, \lambda_2, 0, 1, \infty, \lambda_3],\ \ \lambda_2^* := [\lambda_1, \lambda_3, 0, 1, \infty, \lambda_2] \text{ and } \lambda_1^* := [\lambda_2, \lambda_3, 0, 1, \infty, \lambda_1]$$

need to correspond to supersingular curves. Therefore, the cross ratio of the last four components, given by $\epsilon^*(\lambda_i^*)$ need to be sent to a root of the polynomial $A(x)$.

The cross ratio maps are quite trivial in this specific case. Indeed, they all send $0,\ 1$ and ∞ respectively to $0,\ 1$ and ∞ thus the three cross ratios need to be the identity. Therefore we have

$$\epsilon^*(\lambda_i^*) = [\lambda_i] \text{ for } \ i = 1, 2, 3.$$

Hence λ_1, λ_2 and λ_3 need to be distinct roots of the degree $\frac{p-1}{2}$ polynomial $A(x)$. Therefore there is at most $\frac{(p-1)(p-3)(p-5)}{2}$ possible ways to fix such set of Weierstrass points. □

Remark: For a genus 2 hyperelliptic curve C, having a Weierstrass set $W_C = \{0, 1, \infty, \lambda_1, \lambda_2, \lambda_3\}$, where λ_1, λ_2, and λ_3 are roots of the polynomial $A(x)$, is a necessary but not a sufficient condition to be a maxno-2 curve. In fact only 3 of the conditions are satisfied and a priori, there is no reason why the set should satisfy the 12 other conditions. If we consider the same choice of 15 elements in H_2^*, the conditions to have 15 supersingular sets is equivalent to having the following roots of the polynomial $A(x)$.

$$\begin{array}{lllll}
\lambda_3 & (\frac{\lambda_3-1}{\lambda_3-\lambda_2}) & (\frac{\lambda_3}{\lambda_3-\lambda_2}) & (\frac{\lambda_3-\lambda_3\lambda_2}{\lambda_3-\lambda_2}) & (\frac{\lambda_1-\lambda_2}{\lambda_3-\lambda_2}) \\
\lambda_2 & (\frac{\lambda_3-1}{\lambda_3-\lambda_1}) & (\frac{\lambda_3}{\lambda_3-\lambda_1}) & (\frac{\lambda_3-\lambda_3\lambda_1}{\lambda_3-\lambda_1}) & (\frac{\lambda_3-1}{\lambda_3-\lambda_2})(\frac{\lambda_1-\lambda_2}{\lambda_1-1}) \\
\lambda_1 & (\frac{\lambda_2-1}{\lambda_2-\lambda_1}) & (\frac{\lambda_2}{\lambda_2-\lambda_1}) & (\frac{\lambda_2-\lambda_2\lambda_1}{\lambda_2-\lambda_1}) & (\frac{\lambda_3}{\lambda_3-\lambda_2})(\frac{\lambda_1-\lambda_2}{\lambda_1}).
\end{array}$$

3.3. Computational attempts.

Several attempts have been done computationally to get a feeling of what can happen. One easy approach is, for a fixed field k, to check all the possible sets of Weierstrass points $W = [0, 1, \infty, \lambda_1, \lambda_2, \lambda_3]$ giving a genus 2 hyperelliptic curve C and check explicitly the number of coverings such that $A(E_{ij})$ is zero. For instance for the field $\mathbb{F}_{3^2}$ each curve has either 0, 2 or 3 supersingular sets. Remark that for $\mathbb{F}_3$ such a curve can not be defined and also note that in this process we consider the same isomorphism class of curves more then once. According to the moduli space of hyperelliptic curve H_2^*, in general, we do the computation $|S_{2g+2}| = 6!$ times for the same class. However it is faster than computing the equivalence classes and we are not interested for the moment in the number of class having such properties. The following results have been provided by Maple and Macaulay2. The two programs can be found in Appendix B and C:

Finite field	Possible numbers of associated supersingular elliptic curves
$\mathbb{F}_5$	0
$\mathbb{F}_7$	9
$\mathbb{F}_{3^2}$	0,2,3
$\mathbb{F}_{11}$	4,5,6
$\mathbb{F}_{13}$	0
$\mathbb{F}_{17}$	0
$\mathbb{F}_{19}$	0,1,2,3,4,6
$\mathbb{F}_{23}$	3,4,5,6,7,8,9,10,12
$\mathbb{F}_{5^2}$	0,1,2,3,4
$\mathbb{F}_{3^3}$	0,1,2
$\mathbb{F}_{29}$	0
$\mathbb{F}_{31}$	2,3,4,5,6,7,9,11
$\mathbb{F}_{37}$	0
$\mathbb{F}_{41}$	0
$\mathbb{F}_{43}$	0,1,2,3,6
$\mathbb{F}_{47}$	0,1,2,3,4,5,6,7,8,9,10
$\mathbb{F}_{7^2}$	0,1,2,3,4,5,6,7,8,9
$\mathbb{F}_{3^4}$	0,1,2,3

One could easily extend these computations for higher genus hyperelliptic curves. One can find in [**26**, Proposition 3.1] that there is a bound on the genus of a non-ordinary hyperelliptic curve.

PROPOSITION 3.3.1. *Let C be a hyperelliptic curve over an algebraically closed field in characteristic p, and suppose the Cartier operator $\mathcal{C}$ has rank m. Then*

$$g_C < (p-1)/2 + mp.$$

For the general situation of non-ordinary hyperelliptic curves, we have that $m \leq g-1$. This bound only allows us to conclude the trivial fact: $g_C \geq 1$. But if we restrict ourselves to a more precise strata we can get non-trivial results. For instance, if we consider supersingular curves, the Cartier operator has rank 0. Thus we have the following equality:

$$g_C < (p-1)/2,$$

and we can conclude, for instance, that there is no supersingular hyperelliptic curve of genus 2 over a field of characteristic 3, no supersingular genus 3 hyperelliptic curve over a field of characteristic smaller than 11, etc. Also given a prime p, if we want to find supersingular hyperelliptic curves over a field of characteristic p, we only have to seek for curves with genus less then $(p-1)/2$.

3.4. Genus 2 hyperelliptic curves with many automorphisms.

We have seen in our study of the moduli spaces H_2 that a curve with many automorphisms, that is a curve with a non trivial reduced group of automorphisms $\mathrm{Aut}(C)^* = \mathrm{Aut}(C)/ < \iota >$, will have less than 15 elements in its fiber $\rho^{-1}(C)$. Therefore, if we are seeking for maxno-2 curves, we shall expect that these curves would have less than 15 conditions to be satisfied, indeed we have the following:

Lemma 3.4.1. *Let C be a genus 2 hyperelliptic curve over k, a finite field of odd characteristic, and let $\phi \in \mathrm{Aut}(C)^*$. The set $\{\lambda_i, \lambda_j\}$ is supersingular if and only if the set $\{\phi(\lambda_i), \phi(\lambda_j)\}$ is supersingular.*

Proof: This is straightforward since ϕ can be considered as an element in PGL_2 and the cross-ratio is stable under such transformations. □

Therefore, these curves deserve a special attention. For instance, if for $W_C = \{0, 1, \infty, \lambda_1, \lambda_2, \lambda_3\}$ the λ_i are roots of the polynomial $A(x)$, in general there will be less then 12 other conditions to be satisfied to get a maxno-2 curve. Igusa in [**10**] gave a description of the curves with many automorphisms. Denote by D_{2n} the dihedral group of order $2n$. A curves with many automorphisms is given by the following set of Weierstrass points:

1: $W = \{0, 1, \infty, \lambda, \mu, \lambda(1-\lambda)^{-1}(1-\mu)\}$ and the reduced group of automorphisms is cyclic of order 2, unless by specialization this case reduces to one of the cases below;

2: $W = \{0, 1, \infty, \lambda, \lambda^{-1}(\lambda-1), (1-\lambda)^{-1}\}$ obtained by specializing μ in (1) to $\lambda^{-1}(\lambda-1)$. The reduced group of automorphisms is D_6, the symmetric group of permutation of three letters, unless by specialization this case reduces to one of the cases below;

3: $W = \{0, 1, \infty, \lambda, \lambda^{-1}, -1\}$ obtained by specializing μ in (1) to λ^{-1}. The reduced group of automorphisms is D_4, the Klein four group, unless by specialization this case reduces to one of the cases below;

4: (For $p \neq 3, 5$) $W = \{0, 1, \infty, 2, 2^{-1}, -1\}$ obtained by specializing λ in (2) or in (3) to 2. The reduced group of automorphisms is D_{12}.

5: $W = \{0, 1, \infty, i, -i, -1\}$ obtained by specializing λ in (3) to $i = (-1)^{\frac{1}{2}}$. If $p \neq 5$, the reduced group of automorphisms is D_4, while for $p = 5$ it is the whole group of projective transformations $PGL_2(\mathbb{F}_5)$;

6: (For $p \neq 5$) $W = \{0, 1, \infty, 1+\zeta, 1+\zeta+\zeta^2, 1+\zeta+\zeta^2+\zeta^3\}$ where ζ is a primitive fifth root of unity. The reduced group of automorphisms is cyclic of order 5.

Note that a similar classification for genus 3 hyperelliptic curves can be found in [**14**, Table 3].

The first candidate for a maxno-2 curve will be the curve C given by $W = \{0, 1, \infty, i, i^{-1}, -1\} = \{\infty, 0, 1, 2, 3, 4\}$ over a field of characteristic 5 having 120 automorphisms (type (5)). One can check that it is a non-ordinary hyperelliptic curve.

There is only one element in the fiber $\rho(C)$, that is, up to isomorphisms, only one associated elliptic curve. Therefore only one check need to be done to verify if the curve is a maxno-2 curve and we easily compute that the elliptic curve is not supersingular. After this particular curve, the curves having the largest number of automorphisms are the curves of characteristic $p \geq 7$ given by $W_C = \{0, 1, \infty, 2, 2^{-1}, -1\}$ (type (4)). Depending on the characteristic of the field over which the curve is defined, this particular curve can be ordinary or not. Computations have been done using Maple and the first example of a curve having 15 supersingular pairs of Weierstrass points have been found for $p = 191$. The curve has affine model

$$C : y^2 = x(x-1)(x-2)(x-96)(x-190),$$

where $2^{-1} = 96$ and, as expected, the Weierstrass points $2, 96$ and 190 are roots of the degree 95 polynomial $A(x)$. Note that there are also 5 other roots of this polynomial that are reached by some cross-ratio of these 6 points. Also, one check that this curve is non-ordinary.

Computations have been done up to characteristic $p = 1000$ for the curves defined over $\mathbb{F}_p$ with automorphisms of type (4), and this is the only example of a maxno-2 curve found. In general, a curve of type (4) defined over $\mathbb{F}_p$ where $2, -1, 2^{-2}$ are roots of the polynomial $A(x)$ has $6, 9$ or 12 supersingular sets. This program can be found in appendix D. For the moment no other maxno-2 curves have been found, and we are still seeking for an ordinary maxno-2 curve.

4. Conclusion

So, after all, what have we done during these last 103 pages? Let us recall the main points we have seen. We focused on some very particular curves, the hyperelliptic curves that are in a sense the generalization of elliptic curves to a higher genus. We saw that these curves have affine models

$$C : y^2 = f(x)$$

and are characterized by their unique involution fixing the set of Weierstrass points. The moduli space H_g of these curves were constructed and we built other moduli spaces with level structures H_g^n and H_g^* in order to handle these objects with more ease.

In order to classify the hyperelliptic curves, we considered the p-torsion group on the Jacobian of these curves. We saw that it is a self dual affine group scheme of rank p^{2g} (where g is the genus of the curve) to which one can associate a Dieudonné module. From a theorem of Oort, there are 2^g different possible p-torsion groups and each can be associated to a final sequence. We focused on two particular types of curves: the ordinary curves, that is the curves for which $\mathrm{Jac}(C)[p](k) = (\mu_P \times \mathbb{Z}/p\mathbb{Z})^g$, and the non-ordinary curves, that is the curves having any other p-torsion group.

One important question raised in this work was the following: How can we translate properties related to the Ekedahl-Oort stratification in terms of the moduli spaces H_g? We looked at the particular situation of unramified coverings of genus g hyperelliptic curves by an other hyperelliptic curve. From [**3**], we saw that the only possible degree of such a cover is 2 or 4. We concentrated our efforts in the situation of degree 2 maps. Recall that such a covering $\gamma : D \longrightarrow C$ leads to two other degree 2 coverings of hyperelliptic curves E and F of genus respectively $g - r$ and $r - 1$ for $1 < r < g - 1$. We showed that there is an isogeny of degree a power of 2 $\Psi : \mathrm{Jac}(C) \oplus \mathrm{Jac}(E) \oplus \mathrm{Jac}(F) \longrightarrow \mathrm{Jac}(D)$ and the p-torsion group of D can be studied via the p-torsion groups of C, E, and F. It would be interesting to see if it is possible to generalize our results for degree 4 coverings.

Again, we narrowed our investigation to the case where F is the projective line, *i.e.*, when D is also a hyperelliptic curve. In this setting, the moduli space of such coverings is H_g^2 and our main concern was the description of N_g, the subspace of the coverings $\gamma : D \longrightarrow C$ for which D is non-ordinary. Using the above isogeny, the elements in N_g arise from two situations: either C is non-ordinary and so $D \longrightarrow C$ belongs to N_{gn}, or C is ordinary and the associated genus $g-1$ curve is non-ordinary and $D \longrightarrow C$ belongs to N_{go}. Thus $N_g = N_{gn} \cup N_{go}$ and from the knowledge of non-ordinary curves of genus g and $g-1$ we can recover N_g. Indeed $N_{go} \subseteq \epsilon^{-1}(H_{g-1}(N))$ and $N_{gn} = \rho^{-1}(H_g(N))$. It would be interesting to find if the codimension of $N_{gn} \cap \epsilon^{-1}(H_{g-1}(N)$ is two or more, we hope to come back to this question in the future.

We studied in detail the situation of non-ordinary curves for genus 1 and degree 2 unramified coverings of genus 2 hyperelliptic curves. Several attempts were done computationally to understand the problem. We proved that $\widetilde{H_2} < \infty$ and found an example of such an element. However, this particular curve is also non-ordinary and we are still seeking for a curve in $\widetilde{H_2} \cap H_2(O)$.

The subspace $\widetilde{H_2}$ has codimension 3 and we could conjecture that, in general, $\widetilde{H_g}$ has codimension 3 in H_g. As stated before, we zoomed in considerably our study of subspaces of H_g related to some Ekedahl-Oort strata. This gives us a lot of open windows for further work. For instance, I think that we could generalize several statements about degree 2 coverings in the situation where D is not a hyperelliptic curve. We could also work with a precise non-ordinary strata instead of all non-ordinary curves, and so on...

Appendix A

Maple program written by Melisande Fortin Boisvert.

This file contains four programs which need several subprograms included at the beginning. The first program, named DM, calculates the length $2g$ final sequence of the Dieudonné module associated to the type given in input. The second program, named DM2, calculates from a length $2g$ final sequence its associated Dieudonné module and constructs the filtration that gives back the final sequence. The third program, named DMC, calculates, for a series of types (the type is an invariant associated to an abelian variety with real multiplication, see [**6**]), their associated Dieudonné modules of rank $2g_i$, takes the direct sum of these Dieudonné modules and then computes the final sequence of all the constructed modules and the final sequence of the direct sum. The fourth program, named DMC 2, calculates, for a series of sequences of length $2g_i$, their associated Dieudonné modules, takes the direct sum of these Dieudonné modules and then computes the final sequence of the new module.

```
> restart;
> with(linalg):
>
Warning, new definition for norm Warning, new definition for trace
```

Subprogram perp: Takes the perp of the length $2g$ vector M[hh].

Input:z=s for the scalar case, z=vector containing the g_i,

M=vector containing the submodules g=g or sum of the g_i, hh=index of the submodule for which we take the perp,

Output:M[2gg-hh] the perp of M[hh].

```
> perp:=proc(hh,gg,MM,z)
> local j,p,i,N,n:
> global M:
> if z=s then
>
>  #Scalar case
>  if hh<>gg then
>   M[2*gg-hh]:=vector(2*gg,1):
>    for j to gg do
>     M[2*gg-hh][j+gg]:=1+M[hh][j] mod 2:
>    od:
>    for j from gg+1 to 2*gg do
>     M[2*gg-hh][j-gg]:=1+M[hh][j] mod 2:
>    od:
>   fi:
>   evalm(M[2*gg-hh]);
>  else
>
>   #Vector case
>   p:=0:
>   N:=vector(2*gg,1):
>    for i to nops(z) do
>    #here gg=+gi z=g=vector
>     if hh<>gg then
>      for j to z[i] do
>       N[p+j+z[i]]:=1+M[hh][p+j] mod 2:
```

```
>       od:
>       for j from g[i]+1 to 2*g[i] do
>        N[p+j-z[i]]:=1+M[hh][p+j] mod 2:
>       od:
>      fi:
>      p:=p+2*z[i]:
>     od:
>     n:=dotprod(N,N);
>     M[n]:=evalm(N):
>   fi;
> end:
```

End of perp program.

Subprogram words: Constructs the sword or the dword associated to a type.

Input: g=integer,

tt=type,

Output:a a sword or (w, wd) a dword.

```
> words:=proc(tt,gg)
> local A,i,j,t;
> global w,wd,a,n:
>
> n:=nops(tt):
> t:=[op(tt),gg+1]:
> if type(n,odd)=true then
>  a:=array(1..2*gg): A:=0:
>  for i from 2 to n+1 do
>   for j from t[i-1] to t[i]-1  do
>     a[j]:=A;
>     a[j+gg]:=A+1 mod 2:
```

```
>   od;
>   A:=A+1 mod 2:
> od:
>
> else
>  w:=array(1..gg):
>  wd:=array(1..gg):
>  A:=0:
>  for i from 2 to n+1 do
>   for j from t[i-1] to t[i]-1  do
>     w[j]:=A;
>     wd[j]:=A+1 mod 2:
>   od;
>   A:=A+1 mod 2:
>  od:
> fi:
>
> end:
```

End of word program.

Subprogram FV: Constructs the matrix MF that will compute F on the submodules M$[h]$.

Input:g=g or sum of the g_i,

n=parity of the type,

ww, wwd=dword,

a=sword,

Output:The matrix MF.

```
> FV:=proc(aa,ww,wwd,nn,gg)
> local i:
```

```
> global V,F,MF,X,M:
>
> MF:=matrix(2*gg,2*gg,0):
> F:=array(1..2*gg):
>
> if type(n,odd)=true then
>  for i to 2*gg-1 do:
>   if a[i]=0 then
>     F[i]:=X[i+1];
>     MF[i+1,i]:=1;
>   else F[i]:=0;
>   fi:
>  od:
>  if a[2*gg]=0 then
>    F[2*gg]:=X[1];
>    M[1,2*gg]:=1;
>  else
>    F[2*gg]:=0:
>  fi;
> else
>  for i to gg-1 do:
>   if w[i]=0 then
>    F[i]:=X[i+1]:
>    MF[i+1,i]:=1:
>   else F[i]:=0:
>   fi:
>   if wd[i]=0 then
>    F[i+gg]:=X[i+1+gg]:
```

```
>    MF[i+1+gg,i+gg]:=1:
>   else F[i+gg]:=0:
>   fi:
>  od:
>  if w[gg]=0 then
>   F[gg]:=X[1]:
>   MF[1,gg]:=1
>  else
>   F[gg]:=0:
>  fi:
>  if wd[gg]=0 then
>   F[2*gg]:=X[gg+1]:
>   MF[gg+1,2*gg]:=1
>  else F[2*gg]=0:
>  fi:
> fi:
>
> end:
>
```

End of the FV program.

Subprogram Vperp: Constructs the first filtration.

Input: $z = s$ for that scalar case, z=vector containing the g_i,

MMF= matrix giving the map F obtained in FV,

$g = g$ or sum of the g_i,

Output:M=vector containing some submodules,

L=vector containing the indices i for which we have the sumbodule $M[i]$.

```
> Vperp:=proc(gg,MMF,z)
> local h, mm, j,i:
```

```
> global L, M,n:
>
> h:=2*gg;
> mm:=vector(2*gg,1):
> L:=[]:
> n:=nops(L):
>
> #begin of the F function
>  while h<>0 do:
>   mm:=multiply(MMF,mm):
>   h:=dotprod(mm,mm):
>   M[h]:=evalm(mm):
>   #takes the perp of M[h] of length 2*g.
>   perp(h,gg,M,z):
>   #end of perp function
>   L:=[op(L),h]:
>   if h<>gg then
>    L:=[op(L),2*gg-h]:
>   fi;
>  od;
>
> end:
```

End of Vperp program.

Subprogram stab: Stabilizes the filtration M under F and perp.

Input: $gg = g$ or sum of the g_i,

MMF=matrix giving the map F,

MM=vector containing the submodules,

LL=vector containing the indices of the submodules,

$z = s$ for the scalar case, z=vector containing the g_i,

Output:MMF=The Matrix stabilized under F and perp.

```
> stab:=proc(gg,MMF,MM,LL,z)
> local L1,h,j,mm,h2,K;
> global L;
>
> L1:=LL:
> K:=LL:
> #We get new modules until we have a stabilization under perp and F.
> #At each loop, if i<=g Mi is stable under F and perp.
> while L1<>[] do
>  h:=L1[1]:
>  if h>gg then
> #beginning of the F function. We stop when we get a M[h] we had before
> #ie when h1 is in L
>    mm:=vector(2*gg,1):
> #h2 is there to keep track of h that we have to test before doing the loop.
>    h2:=h:
>    h:=dotprod(multiply(MMF,MM[h]),multiply(MMF,MM[h]));
>    while member(h,K)=false do:
>      h:=h2:
>      mm:=multiply(MMF,MM[h]):
>      if member(h,K)=false then:
>        K:=[op(K),h]:
>      fi:
>      if h<gg then:
>         if member(2*gg-h,K)=false then:
>          K:=[op(K),2*gg-h]:
```

```
>           L1:=[op(L1),2*gg-h];
>  #begin of perp function
>  #takes the perp of M[h1] of length 2*g.
>           perp(h,gg,MM,z):
>  #end of perp function
>          fi:
>         fi:
>         h:=dotprod(mm,mm):
>         MM[h]:=evalm(mm):
>         h2:=h:
>        od:
> #end of the F function.
>       fi:
> #We delete h1 on the list since it is stable under V and perp.
>       L1:=subsop(1=NULL,L1):
>      od:
>      L:=sort(K);
>
> end:
```

End of stab

Subprogram gap: Fills the first gap in M and then stabilizes M.

Input $gg = g$ or sum of the g_i,

MMF=matrix giving the map F,

MM=vector containing the submodules,

LL=vector containing the indices of the submodules,

$z = s$ for the scalar case, z=vector containing the g_i,

Output:The matrix M.

```
> gap:=proc(gg,MMF,MM,LL,z)
```

```
> local f,k, kj, kk, K;
> global L;
>
> K:=LL:
> for k from 2 to gg+1 do
>   if K[k]<>k-1 then
> #k-1 is the position  in L until there is no gap.
> #So we know M_k-2, to found: M_k-1 and its perps.
> #Conctruction of the M_k-1:
>    f:=evalm(MM[K[k]]-M[k-2]):
>    MM[k-1]:=evalm(MM[k-2]):
>    kj:=1:
>    kk:=0:
>    while kk=0 do
>      kk:=f[kj]:
>      kj:=kj+1:
>    od:
>    MM[k-1][kj-1]:=1:
>    K:=[op(K),k-1]:
> #begin of perp function
> #takes the perp of M[k-1] of length 2*g.
>    perp(k-1,gg,MM,z);
> #end of perp function
>    K:=[op(K),2*gg-(k-1)]:
>    K:=sort(K):
> #begin of stab function
> #Stabilise the sequence together with M[k-1]
> stab(gg,MMF,MM,K,z):
```

```
> #rnd of perp function
>    fi:
>   od:
>  L:=K;
> end:
```

End of the program gap.

Subprogram af: Finds the final sequence, the a-number and the f-number of the elementary sequence.

Input: $gg = g$ or sum of the g_i,

MMF=matrix giving the map F,

MM=vector containing the submodules,

Output:The final sequence, the a-number and the f-number.

```
> af:=proc(gg,MMF,MM)
> local i;
> global PHI,a,f;
> PHI:=vector(2*gg):
> f:=0:
> for i to 2*gg do
>  PHI[i]:=dotprod(multiply(MMF,MM[i]),multiply(MMF,MM[i]));
>  if i=PHI[i] then
>   f:=i
>  fi:
> od:
> a:=gg-PHI[gg]:
> print(Phi,PHI):
> print(fnumber,f):
> print(anumber,a):
> end:
```

End of af function.

Subprogram sequ: Constructs the matrix which give F from one final sequence.

Input:phi=a final sequence,

$g = g$,

Output: The matrix MF.

```
> sequ:=proc(g,phi)
> local i,j,k;
> global mn,nm,MF;
> mn:=vector(2*g,0);
> nm:=vector(2*g,0);
> MF:=matrix(2*g,2*g,0);
> j:=1;
> k:=g-1;
> nm[1]:=2*g;
>  for i from 2 to 2*g do
>   if phi[i]<>phi[i-1] then mn[i]:=j;
>    j:=j+1;
>    else nm[i]:=k+g; k:=k-1;
>   fi:
>  od;
>  nm:=evalm(nm+mn);
> MF:=matrix(2*g,2*g,0);
> for i to g do
>  MF[nm[i],i]:=1
> od:
> end:
```

End of seqn program.

Main program DM: Finds the final sequence, the a-number and the f-number from one type.

Input:tt=type beginning with 1,

$gg = g$ or sum of the g_i,

$zs = s$ for the scalar case,

Output: The final sequence, the a-number and the f-number.

```
> DM:=proc(tt,gg,s)
>   words(tt,gg):
>   FV(a,w,wd,n,gg):
>   Vperp(gg,MF,s):
>   stab(gg,MF,M,L,s):
>   gap(gg,MF,M,L,s):
>   af(gg,MF,M):
>  end:
```

End of DM program.

Example:

```
> g:=8: t:=[1,2,3,6]:
> DM(t,g,s):
          Phi, [0, 0, 1, 2, 2, 3, 3, 4, 4, 5, 5, 6, 6, 6, 7, 8]
                                  fnumber, 0
                                  anumber, 4
```

Main program DM2: Constructs the final sequence, the a-number and the f-number from a final sequence.

Input: z=scalar case,

phi=final sequence,

g=sum of the g_i,

Output: The final sequence, the a-number and the f-number.

```
> DM2:=proc(gg,phi,z)
```

```
>   sequ(gg,phi):
>   Vperp(gg,MF,z):
>   stab(gg,MF,M,L,z):
>   gap(gg,MF,M,L,z):
>   af(gg,MF,M):
>  end:
```

End of the DM2 program.

Verification that the sequence we get is the same as the one we started with.

```
> g:=17; t:=[1,2,4,6,10,11,12,14]; DM(t,g,s);
>

                              g := 17
                  t := [1, 2, 4, 6, 10, 11, 12, 14]
Phi, [0, 0, 1, 2, 2, 2, 3, 4, 4, 4, 5, 6, 7, 8, 9, 9, 9, 10, 11,
     11, 11, 11, 11, 11, 12, 13, 13, 13, 14, 15, 15, 15, 16, 17]
                             fnumber, 0
                             anumber, 8
> evalm(PHI);
>
    [0, 0, 1, 2, 2, 2, 3, 4, 4, 4, 5, 6, 7, 8, 9, 9, 9, 10, 11,
     11, 11, 11, 11, 11, 12, 13, 13, 13, 14, 15, 15, 15, 16, 17]

> DM2(g,PHI,s);

Phi, [0, 0, 1, 2, 2, 2, 3, 4, 4, 4, 5, 6, 7, 8, 9, 9, 9, 10, 11,
      11, 11, 11, 11, 11, 12, 13, 13, 13, 14, 15, 15, 15, 16, 17]
                             fnumber, 0
                             anumber, 8
```

Main program DMC: Finds the final sequence, the a-number and the f-number from many types.

Input:tt=vectors containing the types, all beginning with 1,

gg=sum of the g_i,

onoff=on if we want the elementary sequence of each type,

Output:The final sequence, the a-number and the f-number.

```
> DMC:=proc(tt,gg,onoff)
> local i,a,w,wd,n,W1;
> global W,nn,M, P;
> P:=vector(nops(gg));
> nn:=0;
> W:=[];
> for i to nops(gg) do
>  words(tt[i],gg[i]):
>  FV(a,w,wd,n,gg[i]):
>  if onoff=on
>     then
>    Vperp(gg[i],MF,s):
>    stab(gg[i],MF,M,L,s):
>    gap(gg[i],MF,M,L,s):
>    af(gg[i],MF,M):
>    P[i]:=evalm(PHI);
>  fi:
>  if i>1 then
> W:=stack(augment(op(W),matrix(nn,2*gg[i],0)),
> augment(matrix(2*gg[i],nn,0),op(MF)));
>  else W:=evalm(MF);
>  fi;
```

```
>  nn:=nn+2*gg[i];
> od;
> nn:=floor(nn/2);
> Vperp(nn,W,gg):
> stab(nn,W,M,L,gg):
> gap(nn,W,M,L,gg):
> af(nn,W,M):
>
> end:
```

End of DMC program,

Example:

```
> t:=[[1,2],[1,2]]: g:=[2,3]:
> nops(g);
> DMC(t,g,on);
```

```
                              2
                   Phi, [0, 0, 1, 2]
                       fnumber, 0
                       anumber, 2
                Phi, [0, 1, 1, 2, 2, 3]
                       fnumber, 0
                       anumber, 2
          Phi, [0, 1, 1, 1, 1, 2, 3, 4, 4, 5]
                       fnumber, 0
                       anumber, 4
```

Main program DM2: Constructs the final sequence, the a-number and the f-number from many final sequences.

Input:phi=vector containing all the final sequences,

g=sum of the g_i,

Output: The final sequence, the a-number and the f-number.

```
> DMC2:=proc(gg,phi)
>
> local i,a,w,wd,n,W1;
> global W,nn,M, P;
> nn:=0;
> W:=[];
> for i to nops(gg) do
>   sequ(gg[i],phi[i]):
>  if i>1 then
> W:=stack(augment(op(W),matrix(nn,2*gg[i],0)),
> augment(matrix(2*gg[i],nn,0),op(MF)));
>  else W:=evalm(MF);
>  fi;
>  nn:=nn+2*gg[i];
> od;
> nn:=floor(nn/2);
> Vperp(nn,W,gg):
> stab(nn,W,M,L,gg):
> gap(nn,W,M,L,gg):
> af(nn,W,M):
>
> end:
```

End of DMC2 program.

Example using the output of the previous program.

```
> g; evalm(P[1]);evalm(P[2]);

                              [2, 3]
                           [0, 0, 1, 2]
                        [0, 1, 1, 2, 2, 3]
> DMC2(g,P);

                 Phi, [0, 1, 1, 1, 1, 2, 3, 4, 4, 5]
                            fnumber, 0
                            anumber, 4
```

Appendix B

Maple program written by Melisande Fortin Boisvert.

Given a prime p, it considers all the possible Weierstrass sets of genus 2 hyperelliptic curves defined over $\mathbb{F}_p$. For each of them, the program goes over the 15 pairs of 2 points and check if they are supersingular. The number of supersingular sets is then printed in Liste. Note that this program does not consider the isomorphism classes of hyperelliptic curves. Indeed it computes the number of supersingular sets of a curve more than once. This is not problematic, it's only slows down the calculations.

Input:p=Cardinality of the field over which the curve is defined.

Output:Liste=Possible number of supersingular sets.

```
> p:=11:
> d:=p-1:
> m:=floor ((p-1)/2):
> s:=i->sum('(binomial(m,j))^2*i^j','j'=0..m) mod p:
> liste:=[]:
> mmax:=0:
> for z from 2 to d-2 do
> for y from z+1 to d-1 do
> for x from y+1 to d do
>  A:=[infty,0,1,z,y,x];
>  compteur:=0:
```

```
>    for i from 1 to 3 do
>    for j from i+1 to 4 do
>     for k from j+1 to 5 do
>       for l from k+1 to 6 do B:=[A[i],A[j],A[k],A[l]];
>         if i=1 then
>            lam:=(B[4]-B[2])/(B[3]-B[2]) mod p; else
>            lam:=((B[4]-B[1])*(B[2]-B[3]))/((B[4]-B[3])*(B[2]-B[1]));
>          fi;
>          kk:=s(lam);
>          if kk=0 then compteur:=compteur+1;
>          fi;
>        od;
>       od;
>      od;
>     od;
>   if member(compteur,liste)=false then
>    liste:=[op(liste),compteur]
>   fi;
>   if compteur>mmax then
>    mmax:=compteur; HH:=A:
>   fi:
>   if compteur=15 then
>    print (wow);
>   fi;
>  od:
> od:
>od:
> print(liste):
```

```
[4, 5, 6]
```

Appendix C

Macaulay 2 program written by Melisande Fortin Boisvert.

Given a prime p and an integer s, it considers all the possible Weierstrass sets of genus 2 hyperelliptic curves defined over $\mathbb{F}_{p^s}$. For each of them, the program goes over the 15 pairs of 2 points and checks if they are supersingular. The number of supersingular sets is then printed in List. Note that this program does not consider the isomorphism classes of hyperelliptic curves. Indeed, it computes the number of supersingular sets of a curve more than once. This is not problematic, it only slows down the calculations.

Input: p=Characteristic of k, the field over which the curve is defined,
s=integer such that the cardinality of the k is p^s,
Output:List=Possible number of supersingular sets.

```
p=3
ss=3
F=GF(p^ss,Variable=>a)
d=p^ss-1
m=floor ((p-1)/2)
check=no
maximal=0
List={0} s=i->{aa=0; for j from 0 to m  do
 aa=aa+(binomial(m,j))^2*i^j}; for x from 3 to d-2 do
```

```
  for y from 2 to x-1 do
   for z from 1 to y-1 do
    (A=[infty,0,1,a^z,a^y,a^x];
    compteur=0;
for i from 0 to 2 do
 for j from i+1 to 3 do
  for k from j+1 to 4 do
   for l from k+1 to 5 do
    (B=[A#i,A#j,A#k,A#l],
     if i==0 then (lam=(B#3-B#1)/(B#2-B#1))
       else( lam=((B#3-B#0)*(B#1-B#2))/((B#3-B#2)*(B#1-B#0)));
         s(lam);
         if aa==0 then( compteur=compteur+1) );
         print(compteur);
         if compteur>maximal then
         (maximal=compteur; celui=A; );
          if member(compteur,List)==false
          then  List=append(List,compteur);
          if compteur==15 then check=yes)
print(List)
                                                [0,1,2]
```

Appendix D

Maple program written by Melisande Fortin Boisvert.

For $p \geq 7$, in an interval $[a,b]$ this program considers the genus 2 hyperelliptic curve with a affine model $y^2 = x(x-1)(x+1)(x-2)(1-2^{-1})$defined over $\mathbb{F}_{p^s}$, and having automorphism group of type 4, see chapter 1, section 3.4. The program checks first if the 3 Weierstrass points $-1, 2, 2^{-1}$ are roots of the polynomial $A(x)$. If so, the program makes all the other checks needed to have a curve with the maximal number of supersingular sets. The program also gives the configuration of the supersingular sets in the vector N. For each of the 15 sets, it writes 1 if the set is supersingular either it writes 0. The program also checks if the curve C is ordinary or not.

Input: $[a,b]$=interval for the cardinality of the finite field $\mathbb{F}_p$,
Output:N=vector giving the configuration of the supersingular sets,
compteur=Number of supersingular sets of the curve C,
abba=Determinant of the Hasse-Witt matrix of the curve C.

```
>with(linalg):
>
> for p from 175 to 200 do
>  if isprime(p)=true then
>
>   compteur:=0:
>   m:=floor ((p-1)/2);
```

```
>   s:=i->sum('(binomial(m,j))^2*i^j','j'=0..m) mod p;
Check for the 3 Weierstrass points
  b:=s(2) ;
  if b=0 then
    a:=2^(-1) :
    c:=s(a);
    if c=0 then
     aa:=p-1 mod p:
     d:=s(aa) ;
      if d=0 then
Check for the other cross-ratios
       A:=[infty,0,1,2,a,p-1];
        for i from 1 to 3 do
         for j from i+1 to 4 do
          for k from j+1 to 5 do
           for l from k+1 to 6 do
           B:=[A[i],A[j],A[k],A[l]];
           if i=1 then
            lam:=(B[4]-B[2])/(B[3]-B[2]) mod p;
            else
            lam:=((B[4]-B[1])*(B[2]-B[3]))/((B[4]-B[3])*(B[2]-B[1]));
           fi;
           kk:=s(lam);
         if kk=0 then
         compteur:=compteur+1; N[p]:=[op(N[p]),1];
         else
        Check for the configuration
                    N[p]:=[op(N[p]),0];
```

```
         fi;
        od;
       od;
      od;
     od;
     print(N[p]);
Check if the curve is non-ordinary
              r:=x*(x-1)*(x-2)*(x-(1/2))*(x+1)mod p ;
     pp:=collect(r^m,x):
     f := (i,j) -> coeff(pp,x,i*p-j) mod p:
     HVC:=matrix(2,2,f);
     abba:=det(HVC) mod p;
    print(compteur,p,abba);
   fi:
  fi;
 fi;
 fi;
od;
```

```
                  [179,1,1,1,0,0,0,0,0,0,1,0,0,0,1,1]
                              6, 179, 0
                  [191,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]
                             15, 191, 0
                  [199,1,1,1,0,0,0,0,0,0,1,0,0,0,1,1]
                             6, 199, 12
```

Bibliography

[1] Bosh, S., Lütkebohmet, W., Raynaud, M., *Néron models*, A series of modern surveys in mathematics, 21, Springer-Verlag, Berlin (1990).

[2] Cartier, P., *Question de rationalité des diviseurs en géométrie algébrique*, Bull. Soc. math. France, 86, (1958), 177–251.

[3] Farkas, H. M., *Unramified double coverings of hyperelliptic surfaces*, Journal D'analyse Math. 30, (1976), 150–154.

[4] Gatto, L., *Intersection theory on moduli spaces of curves*, Mathematical Monographs, 61. Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro (2000).

[5] Goren, E. Z., *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph series, 14, AMS, Providence RI (2001).

[6] Goren, E. Z., Oort, F., *Stratifications of Hilbert modular varieties*, Journal of Algebraic Geometry, 9, (2000), 111–154.

[7] Harris, J., Morrison, I, *Moduli of curves*, Graduate Texts in Mathemetics, No. 187, Springer-Verlag, New York (1998).

[8] Hartshorne, R., *Algebraic geometry*, Graduate Text in Mathematics, No. 52, Springer-Verlag, New York (1977).

[9] Hindry, M., Silverman, J.H., *Diophantine geometry*, Graduate Text in Mathemetics, No. 201, Springer-Verlag, New York (2000)

[10] Igusa, J.-I., *Arithmetic variety of moduli for genus two*, Annals of Mathematics., Vol 72, No. 2, (November 1960), 612–649.

[11] Kodaira, K., Spencer, D.C., *On deformations of complex analytic structures, I,II*, Annals of Mathematics., (2), 67, (1958), 328–466.

[12] Lang, S., *Algebra,* Third edition, Addison-Wesley Publishing company, (1999)

[13] Machlanchlan, C., *Smooth coverings of hyperelliptic surfaces*, Quart. J. Math., 22, (1971), 117–123.

[14] Magaard, K., Shaska, T., Shpectorov, S., Völklein, H., *The locus of curves with prescribed automorphism group* ,RIMS , Kyoto Technical Report Series, Communications on Arithmetic Fundamential Groups and Galois Theory, edited by H. Nakamura, (2002).

[15] Manin, J. I., *On the theory of Abelian varieties over a field of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat., 26, (1962), 281–292. (Russian.)

[16] Mazur, B., *Arithmetic on curves*, Bull Amer. Math Soc. (N.S.) , Vol 14, (1986), 207–259.

[17] Mestre, J.-F., *Construction de courbes de genre* 2 *à partir de leurs modules*, Effectives methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., Vol 94, Birkhauser, Boston, MA (1991), 314–334.

[18] Milne, J. S., *Étale cohomology*, Princeton Mathematical Series, Princeton University Press, Princeton N.J. (1980).

[19] Milne, J. S., *Abelian varieties*, Arithmetic geometry, (Storrs, CT, 1984)(G.Cornell and J. H. Silverman, eds.) Springer, New York (1986), 105–150.

[20] Milne, J. S., *Jacobian varieties*, Arithmetic geometry, (Storrs, CT, 1984)(G.Cornell and J. H. Silverman, eds.) Springer, New York (1986), 167–212.

[21] Mumford, D., *Abelian varieties*, Tata Inst. Fund. Res. Stud. Math., vol.5, Oxford University Press, London (1970).

[22] Oda, T., *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) 2, (1969), 63–135.

[23] Oort, F., *A stratification of a moduli space of abelian varieties*, Moduli of Abelian Varieties, C. Faber, G. van der Geer and F. Oort editors, Progr. Math., Vol 195, Birkauser Basel (2001), 345–416.

[24] Oort, F., *Commutative group schemes*, Lecture Notes in Mathematics, No. 15, Springer-Verlag, Berlin (1966).

[25] Ran, Z., *A remark on hyperellliptic curves*, Arch. Math., Vol 57, Basel (1991), 622–624.

[26] Re, R., *The rank of the Cartier operator and linear systems on curves*, Journal of Algebra, 236, (2001), 80–92.

[27] Rees, E. G., *Notes on Geometry*, Universitext, Springer-Verlag, Berlin (1983).

[28] Serre, J.-P., *Courbes algébriques et corps de classes*, Act. scient. Ind., 1264, Herman, Paris (1959).

[29] Silverman, J. H., *The arithmetic of elliptic curves*, Graduate Text in Mathematics, No. 106, Springer-Verlag, New York (1986).

[30] Stichtenoth, H., *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin (1991).

[31] Tate, J., *Finite flat group schemes*, Modular forms and Ferma's last theorem (Boston, MA, 1995), Springer-Verlag, New York (1997), 121–154.

[32] Waterhouse, W. C., *Introduction to affine group schemes*, Graduate text in mathematics, No. 66, Springer-Verlag, New York (1979).

[33] Yui, N., *On the Jacobian variety of hyperelliptic curves over fields of characteristic* $p > 2$, Journal of Algebra, 52, no. 2, (1978), 378–410.