Université Bordeaux 1
Università degli Studi di Padova

MASTER ALGANT

Master thesis

Arithmetic on Jacobians of algebraic curves

Student:
Giulio Di Piazza

Advisor:
Damien Robert

Academic year 2012-2013

Introduction

In the last century, information security became of the utmost importance for human society. Initially it was used for military scope, but with the incoming of personal computers and with the increasing dependence on information technology for commercial and private use, also the general public needed to protect electronic data. Thus cryptography gained popularity.

The symmetric systems, in which the two parties who want to communicate share a common secret key, are the oldest ones. They could be used in a not large organism where the secret keys could be shared without many issues. But with the advent of Internet these systems will no longer be usable for every context.

In 1976 Diffie and Hellman proposed public-key systems. They are based on the so called one-way functions. Such a function is easy to compute, but the inverse cannot be computed in an acceptable time window. The "hard" mathematics problem, as the factorization of the product of two large prime and the Discrete Logarithm Problem, leads to construct a lot of one-way functions. Nowadays there are subexponential algorithms that can attack these "hard" problems over a finite field. So that key size of about 2048 bits are required in order to keep secure information.

In 1985 Koblitz and Miller proposed independently to use elliptic curves and their group law instead of finite fields. Nowadays a good cryptography system based on elliptic curve is exponential in the security parameters and we can use much smaller keys. This is useful, for example, in the availment of small rigid supports like smart cards.

The introduction of elliptic curves in the realm of cryptography pushed many people to study possible applications of other curves and of abelian varieties in general.

In this thesis we give a review on the mathematical background of algebraic curve, in particular we explain the connection between a curve and its Jacobian, which is an Abelian variety. So that for each curve we can define an addition law on its Jacobian, and this is useful for computer applications.

After that, in the third chapter, we give the explicit construction of the addition law on elliptic curves in Weierstrass, Huff and Edwards form. The first is the standard form and the most studied in the literature; the second one was introduced by Huff in 1948 to study diophantine problems; the third one has the faster algorithms, it is one of the most studied models in these last years and it found a lot of application.

In the fourth chapter we present the results needed for the computation of the group law on hyperelliptic curves. We give the definition of Mumford representation for a semi-reduced divisor, that is in short an ideal representation, and the Cantor algorithms for the addition and reduction of a divisor.

In chapter five we describe some example of addition on Jacobians of non-hyperelliptic curves. In particular superelliptic curves, that are triple cover of the projective line, are a first generalization of the addition on hyperelliptic curve; and we describe also the general case of non hyperelliptic curves of genus 3.

After these subcases we show how to compute the addition for general curves. This last argument use an algorithm for the computation of a basis of the Riemann-Roch space of a divisor.

Contents

Chapter 1

Algebraic curves and their Jacobian

The aim of this chapter is to introduce the basic definitions and the results about algebraic curves. We will mainly refer to the books of Fulton [Ful69], Milne [Mil91], and Moreno [Mor93].

For all the thesis we denote by $\mathbb{k}$ an arbitrary perfect field as, for example, $\mathbb{C}, \mathbb{Q}, \mathbb{F}_q$.

1.1 Curves

In the affine space $\mathbb{A}^n(\overline{\mathbb{k}})$, we define the *Zarisky topology* by its open basis

$$\{D_f(\overline{\mathbb{k}}) \mid f \in \overline{\mathbb{k}}[x_1, \cdots, x_n]\},$$

where $D_f(\overline{\mathbb{k}}) = \{P \in \mathbb{A}^n(\overline{\mathbb{k}}) \mid f(P) \neq 0\}$.

The closed subsets are given by

$$V_I = \{P \in \mathbb{A}^n(\overline{\mathbb{k}}) \mid f(P) = 0 \ \ \forall f \in I\}$$

for any ideal I of $\overline{\mathbb{k}}[x_1, \cdots, x_n]$

An *affine variety* is a closed irreducible subset of the affine space $\mathbb{A}^n$.

For the projective space $\mathbb{P}^n(\overline{\mathbb{k}})$ we define as well the *Zarisky topology* by its open basis

$$\{D_f(\overline{\mathbb{k}}) \mid f \in \overline{\mathbb{k}}[X_0, X_1, \cdots, X_n]_h\},$$

where $D_f(\overline{\mathbb{k}}) = \{P \in \mathbb{P}^n(\overline{\mathbb{k}}) \mid f(P) \neq 0\}$ and $\overline{\mathbb{k}}[X_0, X_1, \cdots, X_n]_h$ is the set of homogeneous polynomial in $n+1$ variables.

The closed subsets are given by $V_I = \{P \in \mathbb{P}^n(\overline{\mathbb{k}}) \mid f(P) = 0 \ \ \forall f \in I\}$, where I is an homogeneous ideal in $\overline{\mathbb{k}}[X_0, X_1, \cdots, X_n]$ different from $\langle X_0, \cdots, X_n\rangle$.

A *projective variety* is a closed irreducible subset of the projective space.

A *subvariety* of a variety is a closed irreducible subset in the induced topology.

The *dimension* of a variety V is defined to be the supremum on the lengths of chains $S_0 \supset S_1 \supset \cdots \supset S_n$ of distinct irreducible closed subvariety of V. A variety is called *curve* if it has dimension 1.

In particular, an *affine plane curve* is the set of its $\overline{\mathbb{k}}$-rational points

$$\mathscr{C} := \{(X,Y) \in \mathbb{A}^2(\overline{\mathbb{k}}) \mid f(X,Y) = 0\}$$

for a given $f \in \overline{\mathbb{k}}[X,Y]$.

We say that an affine plane curve is defined over $\mathbb{k}$ if $f \in \mathbb{k}[X,Y]$ and we call $\mathbb{k}$-*rational points* of the curve $\mathscr{C}$ the elements in $\{(X,Y) \in \mathbb{A}^2(\mathbb{k}) \mid f(X,Y) = 0\}$. We require that f is absolutely irreducible (i.e. which remains irreducible over any finite extension of $\mathbb{k}$). This condition ensures that the curve is connected and, of course, irreducible. The degree of $\mathscr{C}$ is the degree of the polynomial f.

In a similar way we define the *projective plane curve* as the set

$$\mathscr{C} := \{[X_0, X_1, X_2] \in \mathbb{P}^2(\overline{\mathbb{k}}) \mid f(X_0, X_1, X_2) = 0\}$$

for a given $f \in \overline{\mathbb{k}}[X_0, X_1, X_2]_h$. It is defined over $\mathbb{k}$ if $f \in \mathbb{k}[X_0, X_1, X_2]_h$ and the set of its $\mathbb{k}$-rational points is $\{[X_0, X_1, X_2] \in \mathbb{P}^2(\mathbb{k}) \mid f(X_0, X_1, X_2) = 0\}$.

Let's introduce the *field of rational functions* $\mathbb{k}(\mathscr{C})$ defined by the quotient field of

$$\mathbb{k}[\mathscr{C}] := \mathbb{k}[X_1, \cdots, X_n]/I.$$

Consider I prime, hence $\mathscr{C}$ irreducible, then we have that $\mathbb{k}[\mathscr{C}]$ is a unique factorization domain. We get an isomorphism between $\mathbb{k}(\mathscr{C})$ and the subfield of elements of degree 0 in the quotient field of $\mathbb{k}[\mathscr{C}]_h$ (the set of homogenueous polynomials), namely every element $\phi \in \mathbb{k}(\mathscr{C})$ can be written as f/g, where f, g are homogeneous polynomials with the same degree. Indeed the homogenization

$$h : \mathbb{k}(\mathscr{C}) \to \mathscr{Q}_0(\mathbb{k}[\mathscr{C}]_h)$$

and the affinization

$$a : \mathscr{Q}_0(\mathbb{k}[\mathscr{C}]_h) \to \mathbb{k}(\mathscr{C}),$$

defined by

$$h(\phi) = X_0^{\deg \phi} \phi(\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}),$$

with $\deg \phi = \deg f_1 - \deg f_0$ if $\phi = f_1/f_0$, and

$$a(\psi(X_0, \cdots, X_n)) = \psi(1, X_1, \cdots, X_n),$$

are isomorphisms of fields, one inverse of the other.

If $\Sigma = \mathbb{k}(\xi, \rho)$, with ξ transcendent over $\mathbb{k}$ and ρ algebraic over $\mathbb{k}(\xi)$, is a field of trascendent degree 1 and f is a minimal polynomial of Σ over $\mathbb{k}$, i.e. the minimal polynomial in $\mathbb{k}[X,Y]$ such that $f(\xi, \rho) = 0$. Then the curve $\mathscr{C}$ defined by f has Σ as its field of rational function. Clearly this construction is equivalent to the previous, indeed $\mathbb{k}(\mathscr{C}) \cong \mathbb{k}(X)[Y]/(f) \cong \Sigma$.

1.2 Points

From now on we will consider only curves.

Let's see now the definition of closed points on a curve and their corresponding valuation. Recall that a *valuation* on a field K is a non trivial homomorphism $\nu : K^\times \to \mathbb{Z}$ satisfying:

$$\nu(xy) = \nu(x) + \nu(y),$$
$$\nu(x+y) \geq \min(\nu(x), \nu(y)).$$

The set $R_\nu = \{x \in K^\times \mid \nu(x) \geq 0\} \cup \{0\}$ forms a discrete valuation ring (DVR) and $\mathfrak{m}_\nu = \{x \in R_\nu \mid \nu(x) > 0\}$ is its maximal ideal. They are uniquely determined by the equivalence class of the valuation (namely $\nu \sim \nu'$ if the topology induced by the metrics $d(x,y) = c^{\nu(x-y)}$ and $d'(x,y) = c^{\nu'(x-y)}$, where $c \in \mathbb{R}_{>1}$, is equivalent). We denote by $\mathbb{k}_\nu$ the residue field $R_\nu/\mathfrak{m}_\nu$. Recall also that the following are equivalent if R_ν has dimension 1:

(i) R_ν is a DVR,
(ii) R_ν is integrally closed,
(iii) $\mathfrak{m}_\nu$ is a principal ideal,
(iv) $\dim_{\mathbb{k}_\nu}(\mathfrak{m}/\mathfrak{m}^2) = 1$,
(v) every non zero ideal is a power of $\mathfrak{m}_\nu$,
(vi) there exists an element t, called the *local uniforming parameter*, such that every non zero ideal is of the form (t^i), with $i > 0$.

If $K = \mathbb{k}(\mathscr{C})$ for some curve $\mathscr{C}$, we call *closed point* of the curve the couple $P_\nu = (R_\nu, \mathfrak{m}_\nu)$. We define the *degree* of a closed point to be $\deg(P_\nu) = [\mathbb{k}_\nu, \mathbb{k}]$.

Remark.

i) If $\mathbb{k}$ is algebraically closed, then all the closed points have degree 1.

ii) We are interested in closed points of degree 1, they are in correspondence with the $\mathbb{k}$-rational point (a,b) such that $f(a,b) = 0$. Indeed we can associated to (a,b) the ring

$$R = \{\phi \in \mathbb{k} | \phi = g/h,\ h(a,b) = 0\}$$

and its ideal

$$\mathfrak{m} = \{\phi \in R | \phi = g/h,\ g(a,b) = 0\}.$$

If (a,b) is not a singular point (i.e. if the partial derivatives respect to x and y are not both 0 in (a,b)), then the pair $(R, \mathfrak{m})$ is a DVR and corresponds to (a,b). Conversely, if $P_\nu = (R_\nu, \mathfrak{m}_\nu)$ is a closed point of degree 1, then $\mathfrak{m}_\nu$ is the ideal generated by $(x-a, y-b)$ for some (a,b) such that $f(a,b) = 0$. If (a,b) is a singular point there may be several closed points corresponding to it.

When it will be strictly necessary we will recall that we are working with closed points.

iii) There exists $d = \deg(P_\nu)$ points $P_1, \cdots, P_d$ over $\mathscr{C}(\overline{\Bbbk})$ lying over P_ν, i.e. the corresponding valuation rings in $\Bbbk(\mathscr{C})$ are the same of the one of P_ν. It is also true that $\nu_{P_1} = \nu_{P_i}$ if and only if $P_i \in G_\Bbbk \cdot P_1$, where $G_\Bbbk = \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Then we have that the order of the orbit $G_\Bbbk \cdot P_1$ equals d.

iv) Fix a closed point $P_\nu = (R_\nu, \mathfrak{m}_\nu)$. For an $f \in R_\nu$, we can think at this function modulo $\mathfrak{m}_\nu^l$, then we get

$$f \equiv \sum_{i=0}^{l-1} a_i t^i \pmod{\mathfrak{m}_\nu^l},$$

with unique elements $a_i \in \Bbbk_\nu$ and t is the uniforming parameter. Hence we can pass to the limit and consider f in the completion $\widehat{R_\nu}$ of R_ν. The ring $\widehat{R_\nu}$ is isomorphic to the ring of power series $\Bbbk_\nu[[t]]$. The field of quotient of $\Bbbk_\nu[[t]]$ is denoted by $\Bbbk_\nu((t))$ and it contains $\Bbbk(\mathscr{C})$ as a dense subset.

Let now $\phi \in \Bbbk(\mathscr{C})$ be a rational function. For every point P, corresponding to a closed point P_ν, we can write ϕ as a formal power series:

$$\phi = \sum_j a_j t^j$$

with $a_j \in \Bbbk_\nu$ and t the local uniforming parameter. We define the *order* of ϕ at P by

$$\mathrm{ord}_P(\phi) = n$$

where n is the smallest exponent of a power of t which appears with coefficient $a_n \neq 0$ in the power series expansion of ϕ.

1.3 Intersection of curves

Let $\mathscr{C}$ and $\mathscr{D}$ be two plane curves with no common components defined over an algebraic closed field $\Bbbk$. Let f and g be the corresponding homogeneous polynomials. Suppose that the curves do not pass through the point $O = (0, 0, 1)$ and that each line passing through O contains at most one point of intersection of $\mathscr{C}$ and $\mathscr{D}$. Let $h \in \Bbbk[X_0, X_1]$ be the resultant of f and g respect the variable X_2. For a point $P = (a, b, c) \in \mathscr{C} \cap \mathscr{D}$ we define the *intersection multiplicity* of $\mathscr{C}$ and $\mathscr{D}$ at P to be

$$m_P(\mathscr{C}, \mathscr{D}) = \mathrm{ord}_{(a,b)} h(X_0, X_1).$$

Theorem 1.3.1 (Bézout). *Let $\mathscr{C}$ and $\mathscr{D}$ be two plane projective curves defined on an algebraically closed field with no common components, then*

$$\sum_P m_P(\mathscr{C}, \mathscr{D}) = \deg \mathscr{C} \cdot \deg \mathscr{D}.$$

Proof. See [Ful69]. □

1.4 Maps

Let $\mathscr{C}$ and $\mathscr{D}$ be two subvarieties of $\mathbb{P}^n$ and $\mathbb{P}^m$ respectively. A *rational map* $F : \mathscr{C} \dashrightarrow \mathscr{D}$ is defined in a open subset of $\mathscr{C}$, and is is such that there exist $m+1$ rational functions $f_0, f_1, \cdots, f_m \in \mathbb{K}(X_0, X_1, \cdots, X_n)$ for which the equality $F(P) = [f_0(P), f_1(P), \cdots, f_m(P)]$ holds. A rational map F is said to be *birational* if it is injective in an open subset of $\mathscr{D}$ and it has a rational inverse. It is clear that the composition of rational maps is still rational.

We can define the pullback operator

$$^* : \mathrm{Rat}_{\mathbb{k}}(\mathscr{C}, \mathscr{D}) \to \mathrm{Hom}_{\mathbb{k}}(\mathbb{k}(\mathscr{D}), \mathbb{k}(\mathscr{C}))$$

form the set of $\mathbb{k}$-rational maps to the set of $\mathbb{k}$-homomorphism of fileds. It is such that $F^*(\phi) = \phi \circ F$ with $\phi \in \mathbb{k}(\mathscr{D})$. Moreover, it is a bijection and $id^*_{\mathscr{C}} = id_{\mathbb{k}(\mathscr{C})}$, $(F \circ G)^* = G^* \circ F^*$.

$$\begin{tikzcd}
 & \mathbb{k} \\
\mathscr{C} \arrow[ur, "\phi\circ F"] \arrow[r, dashed, "F"'] \arrow[d, dotted] & \mathscr{D} \arrow[u, "\phi"'] \arrow[d, dotted] \\
\mathbb{k}(\mathscr{C}) & \mathbb{k}(\mathscr{D}) \arrow[l, "F^*"']
\end{tikzcd}$$

Theorem 1.4.1. *Two curves are birationally equivalent if and only if there exists a $\mathbb{k}$-algebra isomorphism between the corresponding function fields.*

Proof. See [Ful69] and [Wal50] for algebraically closed field or [Mor93] for non-algebraically closed field. □

We define the *degree* of a rational map $F : \mathscr{C} \to \mathscr{D}$ to be

$$\deg(F) = [\mathbb{k}(\mathscr{C}) : F^*(\mathbb{k}(\mathscr{D}))].$$

We have the following result.

Proposition-Definition 1.4.2. *Each non constant rational map $F : \mathscr{C} \dashrightarrow \mathscr{D}$ induces a surjective application from the (closed) points of $\mathscr{C}$ to the (closed) points of $\mathscr{D}$. For every point Q of $\mathscr{D}$ we can assign to every point $P_1, \cdots, P_k$ in the inverse image a positive integer $m_{P_i}(F)$, called* multiplicity of ramification*, such that $\sum_i m_{P_i} F \mathrm{deg} P_i = \deg(F)$ and $t = t_i^{m_{P_i}(F)}$, where t and t_i are the* local uniforming parameters *of Q and P_i.*

The points with multiplicity bigger than 1 are called *points of ramification* for F and we can define the *ramification* of F in P to be $ram_P(F) = m_P(F) - 1$, and the *total ramification* to be $ram(F) = \sum_{P \in \mathscr{C}} ram_P(F) \deg P$.

1.5 Divisors

We introduce now the fundamental instrument for studying curves.

The *group of divisors* of the curve $\mathscr{C}$ is the free group generated by its (closed) points. Let's denote it by

$$\mathrm{Div}(\mathscr{C}) = \{\mathcal{D} : \mathcal{D} = \sum_P d_P P,\ d_P \in \mathbb{Z},\ d_P \text{ almost everywhere zero}\}$$

where $d_P := \mathrm{ord}_P\mathcal{D}$ is called the *order* of P in $\mathcal{D}$. We shall call support of $\mathcal{D}$ the set $\{P : \mathrm{ord}_P\mathcal{D} \neq 0\}$.
For $\mathcal{D}, \mathcal{D}' \in \mathrm{Div}(\mathscr{C})$ we shall say that $\mathcal{D} \leq \mathcal{D}'$ if and only if $\mathrm{ord}_P\mathcal{D} \leq \mathrm{ord}_P\mathcal{D}'$ $\forall\ P \in \mathscr{C}$.
We call *effective* a divisor $\mathcal{D}$ such that $\mathcal{D} \geq 0$.
Lastly we define the *degree* of the divisor $\mathcal{D}$ to be

$$\mathrm{deg}\mathcal{D} = \sum_P \mathrm{ord}_P\mathcal{D} \deg P.$$

and finally we denote with $\mathrm{Div}_0(\mathscr{C})$ the subgroup of divisors of degree 0.

Remark. Since every points in the orbit $G_{\Bbbk} \cdot P$, with $P \in \mathscr{C}_{\overline{\Bbbk}}$, correspond to a single closed point in $\mathscr{C}_{\Bbbk}$, then a divisor $\mathcal{D}$ over $\mathscr{C}_{\overline{\Bbbk}}$ can be viewed as divisor of $\mathscr{C}$ if and only if it is fixed by every element in $G_{\Bbbk}$, i.e. $g \cdot \mathcal{D} = \mathcal{D}$ for all $g \in G_{\Bbbk}$, if and only if for every point $P \in \mathscr{C}_{\overline{\Bbbk}}$ the points on the orbit $G_{\Bbbk} \cdot P$ appears in $\mathcal{D}$ with the same degree.

The divisor of a rational function $\phi \in \Bbbk(\mathscr{C})$ is called *principal divisor* and it is given by

$$\mathrm{div}(\phi) = \sum_P \mathrm{ord}_P(\phi)P.$$

We have $\deg(\mathrm{div}(\phi)) = 0$, hence the set $\mathrm{PDiv}(\mathscr{C})$ of all principal divisor is a subgroup of $\mathrm{Div}_0(\mathscr{C})$.

From now on, if not specified, the support of a divisor will be composed only of closed points of degree 1, i.e. $\Bbbk$-rational points.

1.6 Differentials

Let K be a field lying over $\Bbbk$. Consider the product $K \otimes_{\Bbbk} K$ and the linear application $\pi : K \otimes_{\Bbbk} K \to K$, such that $\pi(a \otimes b) = ab$.
Observe that $I = \ker(\pi)$ is a linear combination of elements of the type $1 \otimes b - b \otimes 1$, indeed if $\sum_i a_i \otimes b_i \in \ker(\pi)$, then

$$\sum_i a_i \otimes b_i = \sum_i (a_i \otimes b_i - a_i b_i \otimes 1) = \sum_i (a_i \otimes 1)(1 \otimes b_i - b_i \otimes 1) = \sum_i a_i(1 \otimes b_i - b_i \otimes 1).$$

Define now the *space of differential* of K to be

$$\Omega_{\Bbbk}(K) = I/I^2.$$

The set $\Omega_{\Bbbk}(K)$ is a $\Bbbk$-vector space and a K-vector space.
This space is equipped with a $\Bbbk$-linear map

$$d : K \to \Omega_{\Bbbk}(K)$$

defined by $d(a) = [1 \otimes a - a \otimes 1]$. The following holds:

(i) $d(k) = 0$ for every $k \in \Bbbk$
(ii) $d(ab) = ad(b) + bd(a)$ (Leibniz rule)
(iii) if $b \in K^{\times}$, then $d(\frac{1}{b}) = -\frac{d(b)}{b^2}$
(iv) for $f \in \Bbbk[X]$ we have $d(f(X)) = \sum_i \frac{\partial f}{\partial X_i}(X)d(X_i)$.

In our case let $K = \Bbbk(\mathscr{C})$ and define $\Omega(\mathscr{C}) = \Omega_{\Bbbk}(\Bbbk(\mathscr{C}))$, it is called *differential space* of the curve $\mathscr{C}$.

The field $\Bbbk(\mathscr{C})$ has trascendental degree 1 over $\Bbbk$, then every two element $\phi, \psi \in \Bbbk(\mathscr{C})$ are algebraically dependent, so there exists a polynomial $g(x, y)$ such that $g(\phi, \psi) = 0$. We have

$$g_x(\phi, \psi)d\phi + g_y(\phi, \psi)d\psi = 0,$$

$$d\phi = -\frac{g_y(\phi, \psi)}{g_x(\phi, \psi)}d\psi,$$

where $g_x = \frac{\partial g}{\partial x}$.
Therefore every element $d\phi$ is a multiple (over $\Bbbk(\mathscr{C})$) of a given non zero element. It follows that $\Omega(\mathscr{C})$ is a one dimensional vector space over $\Bbbk(\mathscr{C})$.

As in the case of rational function we can define the *divisor of a differential*: fix a point P_ν, for every differential $\omega \in \Omega(\mathscr{C})$ we can write

$$\omega = \sum_j b_j t^{j-1} dt;$$

define the *order* at P_ν to be the smallest exponent n of a power of t which appears with coefficient $b_n \neq 0$ in the power series expansion of ω. And define also

$$\mathrm{div}(\omega) = \sum_P \mathrm{ord}_P(\omega)P$$

and $W = \{\mathrm{div}(\omega) \mid \omega \in \Omega(\mathscr{C})\}$

Since the dimension of $\Omega(\mathscr{C})$ is 1, then the degree of a divisor of a differential is always the same. This suggests to define the *genus* g of the curve to e the integer such that

$$\deg(\omega) = 2g - 2.$$

1.7 Divisors under rational maps

Assume now that the field of constant of the function field $\Bbbk(\mathscr{C})$ is $\Bbbk$, it means $\overline{\Bbbk} \cap \Bbbk(\mathscr{C}) = \Bbbk$. Let $F : \mathscr{C} \to \mathscr{D}$ be a rational map and let Q be a point of $\mathscr{D}$, we can construct a divisor in $\mathscr{C}$ defined by

$$F^*(Q) = \sum_{P \in \mathscr{C},\, F(P)=Q} m_P(F)P,$$

we can extend by linearity to the group of all divisors

$$F^* : \mathrm{Div}(\mathscr{D}) \to \mathrm{Div}(\mathscr{C}).$$

We have $\deg(F^*\mathcal{D}) = \deg(F)\deg(\mathcal{D})$, hence F^* can be resticted to the application $F^* : \mathrm{Div}_0(\mathscr{D}) \to \mathrm{Div}_0(\mathscr{C})$. Moreover we can further restrict it to the subgroup of principal divisors, indeed

$$F^*(\mathrm{div}(\phi)) = \mathrm{div}(F^*\phi).$$

For a canonical divisor, we observe that the function F induce a $\Bbbk$-linear application $F^* : \Omega(\mathscr{D}) \to \Omega(\mathscr{C})$ that send $d(\psi)$ in $d(F^*\psi)$. We have

$$\mathrm{div}\left(F^*\omega\right) = F^*\left(\mathrm{div}(\omega)\right) + Ram(F),$$

where $Ram(F) = \sum_P ram_P(F)P$. Passing on degrees we get

Theorem 1.7.1 (Hurwitz)**.** *Let $F : \mathscr{C} \dashrightarrow \mathscr{D}$ be a rational map. Let ω be a differential in $\Omega(\mathscr{C})$. Then*

$$\deg\left(\mathrm{div}(F^*\omega)\right) = \deg(F)\deg\left(\mathrm{div}(\omega)\right) + ram(F).$$

Proof. See [Mor93] for finite field or [Ful69] for algebraically closed field. □

1.8 Linear systems

Two divisors $\mathcal{D}, \mathcal{D}'$ are *linearly equivalent* ($\mathcal{D} \sim \mathcal{D}'$) if there exists a rational function ϕ such that $\mathcal{D} - \mathcal{D}' = \mathrm{div}(\phi)$. We denote by $|\mathcal{D}|$ the equivalence class of $\mathcal{D}$ restricted on the effective divisors, namely

$$|\mathcal{D}| = \{\mathcal{E} \in \mathrm{Div}(\mathscr{C}) : \mathcal{E} \geq 0,\ \mathcal{E} \sim \mathcal{D}\},$$

and we shall call it *complete linear system* of $\mathcal{D}$ (it is empty if $\deg \mathcal{D} < 0$).

We define the *Riemann-Roch space* as

$$\mathscr{L}(\mathcal{D}) = \{\phi \in \Bbbk(\mathscr{C}) : \mathrm{div}(\phi) + \mathcal{D} \geq 0\}.$$

There is a natural bijection $\mathbb{P}(\mathscr{L}(\mathcal{D})) \leftrightarrow |\mathcal{D}|$ that send χ to $\mathrm{div}(\chi) + \mathcal{D}$.

We shall call *linear system* every projective subspace G of $|\mathcal{D}|$, we use the notation $G \leq |\mathcal{D}|$. The *degree* of G is the degree of every element in G, it is denoted by $\deg(G)$; and the *dimension* of G is the dimension as projective subspace, it is denoted by $d(G)$.
In the same way, for the complete linear system $|\mathcal{D}|$, we introduce

$$\ell(\mathcal{D}) = \dim_{\Bbbk}\mathscr{L}(\mathcal{D}),\ \ d(\mathcal{D}) = \dim|\mathcal{D}|$$

hence $d(\mathcal{D}) = \ell(\mathcal{D}) - 1$.

We denote by $B(\mathcal{D})$ the *base locus* of the divisor $\mathcal{D}$ that is by definition the intersection of all effective divisors in the complete linear system $|\mathcal{D}|$, in other words it is the divisor such that $B(\mathcal{D}) \leq \mathcal{E}$ holds for every $\mathcal{E} \in |\mathcal{D}|$. We have $\mathscr{L}(\mathcal{D}) = \mathscr{L}(\mathcal{D} - B(\mathcal{D}))$. We say that a complete linear system is *without base points* if $B(\mathcal{D}) = 0$.

1.9 Riemann theorem, Riemann-Roch theorem

The following theorems are the fundamental results in the realm of curves and their divisors. They give us a link between the degree and the dimension of a complete linear system. These theorems will be often used in the whole text without being mentioned. The reader can find the proof in [Ful69] and [Wal50] for algebraically closed field, and in [Mor93] for finite field.

Theorem 1.9.1 (Riemann)**.** *For every divisor $\mathcal{D}$ we have*

$$\deg(\mathcal{D}) - d(\mathcal{D}) \leq g.$$

Theorem 1.9.2 (Riemann-Roch)**.** *The gap in the Riemann theorem is given by $\ell(\omega - \mathcal{D})$ for every $\omega \in W$. Hence*

$$\ell(\mathcal{D}) = \deg(\mathcal{D}) + 1 - g + \ell(\omega - \mathcal{D})$$

in other words

$$d(\mathcal{D}) = \deg(\mathcal{D}) - g + \ell(\omega - \mathcal{D}).$$

We say that a divisor $\mathcal{D}$ is *special* if $\ell(\omega - \mathcal{D}) > 0$.

Remark. Using the Riemann-Roch theorem it is easy to prove that $d(W) = g-1$.

1.10 Abelian varieties

In this section we introduce the notion of abelian variety, that is a projective curve with a group law defined on its points. Abelian varieties are indeed very useful for cryptographic application. We will have that a Jacobian curve is an abelian variety.

An *algebraic group* $\mathscr{D}$ over a field $\Bbbk$ is an absolutely irreducible variety defined over $\Bbbk$ together with:

i) the addition morphism
$$m : \mathscr{D} \times \mathscr{D} \to \mathscr{D}$$

ii) the inverse morphism
$$i : \mathscr{D} \to \mathscr{D},$$

iii) and a neutral element
$$0 \in \mathscr{D}$$

satisfying the usual group laws. We shall use the notations $P \oplus Q := m(P, Q)$ and $\ominus P := i(P)$.

We can extend the group law in $\mathscr{D}_{\mathbb{L}}$, for an extension field $\mathbb{L}/\Bbbk$, via the evaluating morphism defined over $\Bbbk$. In particular the group law extends in a unique way in $\mathscr{D}_{\overline{\Bbbk}}$.

Lemma 1.10.1. *Every algebraic group is nonsingular.*

Proof. For any variety we can find an open set in which the variety is non singular. By the translation isomorphism $t_a : P \mapsto m(P, a)$ we have that every open subset of $\mathscr{D}$ is nonsingular. Hence every algebraic group is automatically nonsingular. □

A projective algebraic group $\mathscr{A}$ is called *abelian variety.*

Remark. We could define abelian varieties to be a complete connected algebraic group. This implies the projectivity, but the proof is not immediate, and it is not necessary in this context.

Theorem 1.10.2 (Rigidity)**.** *Let $\alpha : \mathscr{A} \times \mathscr{B} \to \mathscr{C}$ be a regular map, and assume that $\mathscr{A}, \mathscr{B}, \mathscr{C}$ are projective varieties. If there are three points $a \in \mathscr{A}, b \in \mathscr{B}, c \in \mathscr{C}$ such that*

$$\alpha(\mathscr{A} \times \{b\}) = \alpha(\{a\} \times \mathscr{B}) = \{c\},$$

then $\alpha(\mathscr{A} \times \mathscr{B}) = \{c\}$.

Proof. See [Mil91]. □

Corollary 1.10.3. *Every regular map $\alpha : \mathscr{A} \to \mathscr{B}$ of abelian varieties is the composite of a homomorphism with a translation*

Proof. After a translation by $-\alpha(0)$ we can always assume that $\alpha(0) = 0$. Let $\phi : \mathscr{A} \times \mathscr{A} \to \mathscr{B}$ be the regular map given by $\phi(a_1, a_2) = \alpha(a_1+a_2)-\alpha(a_1)-\alpha(a_2)$. Then $\phi(\mathscr{A} \times 0) = \phi(0 \times \mathscr{A}) = 0$. This means that α is an isomorphism. □

Corollary 1.10.4. *The group law on an abelian variety is commutative.*

Proof. A group is commutative if and only if the inverse map i is an homomorphism. By definition the inverse map of an abelian variety is a regular map, and it send 0 to 0. We can conclude applying the precedent corollary. □

We explain now what happen to the homomorphism group $\mathrm{Hom}_{\Bbbk}(\mathscr{A}, \mathscr{B})$ under base change. Let $\mathbb{L}/\Bbbk$ be a field extension and let $\mathscr{A}_{\mathbb{L}}, \mathscr{B}_{\mathbb{L}}$ be the abelian varieties obtained by scalar extension. The Galois group $G_{\mathbb{L}} = \mathrm{Aut}_{\mathbb{L}}\left(\overline{\mathbb{L}}\right)$ acts in a natural way on $\mathrm{Hom}_{\Bbbk}(\mathscr{A}, \mathscr{B})$. We have:

i) if $\mathbb{L}_0$ is the algebraic closure of $\Bbbk$ in $\mathbb{L}$, then $\mathrm{Hom}_{\mathbb{L}}(\mathscr{A}_{\mathbb{L}}, \mathscr{B}_{\mathbb{L}}) = \mathrm{Hom}_{\mathbb{L}_0}(\mathscr{A}_{\mathbb{L}_0}, \mathscr{B}_{\mathbb{L}_0})$,

ii) for any $\mathbb{L}$ contained in $\overline{\Bbbk}$ we have $\mathrm{Hom}_{\mathbb{L}}(\mathscr{A}_{\mathbb{L}}, \mathscr{B}_{\mathbb{L}}) = \mathrm{Hom}_{\overline{\Bbbk}}(\mathscr{A}_{\overline{\Bbbk}}, \mathscr{B}_{\overline{\Bbbk}})^{G_{\mathbb{L}}}$.

Proposition 1.10.5. *Let $\phi \in \mathrm{Hom}_{\Bbbk}(\mathscr{A}, \mathscr{B})$.*

i) $\mathrm{Im}(\phi)$ *is an abelian subvariety of $\mathscr{B}$ by restriction of the addition law,*

ii) $\ker(\phi)$ *is a closed subset of $\mathscr{A}$ and it contains a maximal absolutely irreducible subvariety* $\mathrm{Ker}(\phi)^0$ *containing $0_{\mathscr{A}}$, it is called the connected component of the unity of* $\mathrm{Ker}(\phi)$*,*

iii) we have $\dim(\mathrm{Im}(\phi)) + \dim(\ker(\phi)^0) = \dim(\mathscr{A})$*.*

Proof. See [Mil91] □

1.11 Isogenies and $[n]$-torsion points

We define an *isogeny* to be a surjective morphism with finite kernel between two abelian varieties $\mathscr{A}$ and $\mathscr{B}$. In this case we say that $\mathscr{A}$ is isogenous to $\mathscr{B}$. It is an equivalence relation.

Theorem 1.11.1. *For a morphism $\alpha : \mathscr{A} \to \mathscr{B}$ of abelian varieties, the following are equivalent:*

i) *α is an isogeny,*

ii) $\dim \mathscr{A} = \dim \mathscr{B}$ *and α is surjective,*

iii) $\dim \mathscr{A} = \dim \mathscr{B}$ *and* $\ker(\alpha)$ *is finite.*

Proof. See [Mil91] Proposition 7.1. □

The *degree* of an isogeny $\alpha : \mathscr{A} \to \mathscr{B}$ is the degree as a regular map, i.e. $[\Bbbk(\mathscr{A}) : \alpha^*(\Bbbk(\mathscr{B}))]$. If α is separable, i.e. $\Bbbk(\mathscr{A})/\alpha^*(\Bbbk(\mathscr{B}))$ is a separable extension, then α is unramified. If moreover $\Bbbk$ is algebraically closed, then every fibre has exactly $\deg(\alpha)$ points.

Let $[n] : \mathscr{A} \to \mathscr{A}, a \mapsto na = a + \cdots + a$ be the integer multiplication on $\mathscr{A}$ Denote by $\mathscr{A}[n]$ the kernel of $[n]$, its points are called *n-torsion points.*

Theorem 1.11.2. *Let $\mathscr{A}$ be an abelian variety of dimension g. The integer multiplication $[n]$ is an isogeny of degree n^{2g}. It is separable, hence it is unramified, if $\Bbbk$ has characteristic 0 or is has characteristic $p \neq 0$ such that $p \nmid n$. In these case we have $\mathscr{A}_{\overline{\Bbbk}}[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$.*
For $n = p^s$ we have $\mathscr{A}_{\overline{\Bbbk}}[p^s] \simeq (\mathbb{Z}/p^{st}\mathbb{Z})$, with $t \leq g$ independent on s.

We call the integer t the *p-rank* of the abelian variety $\mathscr{A}$. If $t = g$ the variety is called *ordinary.* If $\mathscr{A}$ is an elliptic curve, i.e. it is an abelian variety of dimension 1, it is called supersingular if $t = 0$. In general an abelian variety is called *supersingular* if it is isogenous to a product of supersingular elliptic curves.

Proof. See [Mil91] or [MRM70]. We need to use ample divisors. □

1.12 Jacobians

In this section we will describe the Jacobian of an algebraic curve. Theorem 1.12.1 will be very useful in the whole thesis, it gives us a way to represent a point of the Jacobian. Unfortunately this representation is still not unique in general.

Let $\mathscr{C}$ be an (absolutely) irreducible curve over a field $\Bbbk$. In an algebraic closed field $\overline{\Bbbk}$ we can define the *Picard group*

$$\mathrm{Pic}^0_{\mathscr{C}_{\overline{\Bbbk}}} := \mathrm{Div}_0(\mathscr{C}_{\overline{\Bbbk}})/\mathrm{PDiv}(\mathscr{C}_{\overline{\Bbbk}}).$$

Let $G_{\mathbb{k}}$ be the Galois group $\mathrm{Aut}_{\mathbb{K}}(\overline{\mathbb{K}})$. It acts in a natural way on $\mathrm{Pic}^0_{\mathscr{C}_{\overline{\mathbb{k}}}}$ and we define

$$\mathrm{Pic}^0_{\mathscr{C}} := (\mathrm{Pic}^0_{\mathscr{C}_{\overline{\mathbb{k}}}})^{G_{\mathbb{k}}}.$$

More generally, if $\mathbb{L}$ is a field extension of $\mathbb{k}$ inside $\overline{\mathbb{k}}$, we have $\mathrm{Pic}^0_{\mathscr{C}_{\mathbb{L}}} = (\mathrm{Pic}^0_{\mathscr{C}_{\overline{\mathbb{k}}}})^{G_{\mathbb{L}}}$.

We would like to construct an abelian variety $\mathscr{J} = \mathrm{Jac}(\mathscr{C})$ such that

$$\mathscr{J}_{\mathbb{L}} = \mathrm{Pic}^0_{\mathscr{C}_{\mathbb{L}}}.$$

Assume that $\mathscr{C}$ is a nonsingular, absolutely irreducible, projective curve of genus $g > 0$. Assume also that it has a $\mathbb{k}$-rational point at infinity P_∞, and suppose for simplicity that it is $(0, 1, 0)$.

Theorem 1.12.1. *For every $\mathbb{k}$-rational divisor $\mathcal{D}$ of degree 0 there exists an effective $\mathbb{k}$-rational divisor $\mathcal{E}$ of degree g such that $\mathcal{E} - gP_\infty \sim \mathcal{D}$, it is in the divisor class of $\mathcal{D}$.*

Proof. Take $\mathcal{D}' \sim \mathcal{D}$. Write $\mathcal{D}' = \mathcal{D}_1 - \mathcal{D}_2$, with $\mathcal{D}_1, \mathcal{D}_2$ effective divisors. Fix an m such that $m - \deg(\mathcal{D}_2) > g$. By Riemann-Roch theorem there exists a function f_1 such that $\mathrm{div}(f_1) + mP_\infty - \mathcal{D}_2$ is effective. We can replace $\mathcal{D}'$ by $\mathcal{D}' + \mathrm{div}(f_1)$ and assume that $\mathcal{D}' = \mathcal{D} - kP_\infty$ with $k = \deg \mathcal{D}$ and $\mathcal{D}$ effective. If $k \leq g$ we proved the theorem, otherwise we consider the divisor $\mathcal{D} - (k - g)P_\infty$. It has degree bigger than g, then there exists a function f such that $\mathcal{D} - (k-g)P_\infty + \mathrm{div}(f)$ is effective, therefore $\mathcal{D} - kP_\infty + \mathrm{div}(f) \sim \mathcal{D}$ and it is equal to $(\mathcal{D} - (k-g)P_\infty + \mathrm{div}(f)) - gP_\infty$ as required. □

Remark. Suppose that $g > n = [\mathbb{k}(\mathscr{C}) : \mathbb{k}(x)]$. If $\mathcal{E}$ contains in its support points at infinity then the divisor

$$\mathcal{E}' - (*)P_\infty = \mathcal{E} - \{\text{points at infinity in } \mathrm{supp}(\mathcal{E})\} - (*)P_\infty$$

is in the same class of $\mathcal{E} - gP_\infty$. Now if $\mathcal{E}'$ contains all the points in the set $\Sigma P = \{P_i \mid P_i = \sigma_i P,\ \sigma_i \in \mathrm{Gal}(\mathbb{k}(\mathscr{C})/\mathbb{k}(x))\}$, then $x_{P_i} = x_P$ for each P_i, and $\mathrm{div}(x - x_P) = \Sigma P - nP_\infty$, hence

$$\mathcal{E}' - (*)P_\infty \sim (\mathcal{E}' - \Sigma P) - (*)P_\infty = \mathcal{E}'' - (*)P_\infty.$$

Note that $\deg \mathcal{E}'' \leq \deg \mathcal{E}$.

We call a divisor in the form $\mathcal{E} - (*)P_\infty$ *reduced along* P_∞ if $\mathcal{E}$ does not contain any sets ΣP and any points at infinity.

We construct the g-fold cartesian product $\mathscr{C}^g$ as follow. Take $\mathscr{C}_a$ a (nonempty) affine part of $\mathscr{C}$, let $(x_1, \cdots, x_n)$ be the affine coordinates. Let $\mathscr{C}_{a,i}$ a copy of $\mathscr{C}_a$ of coordinates $(x^i_1, \cdots, x^i_n)$. The variety $\mathscr{C}^g_a$ is define to be the cartesian product of the $\mathscr{C}_{a,i}$, hence it can be embedded in an affine space of coordinates $(x^1_1, \cdots, x^1_n, \cdots, x^g_1, \cdots, x^g_n)$. The projective variety $\mathscr{C}^g$ is defined by glueing.

Let S_g be the symmetric group acting on $\{1, \cdots, g\}$. It acts in a natural way on $\mathscr{C}^g$ permuting the coordinates $(x^1, \cdots, x^g)$. Finally we have a projective variety $S_g \setminus \mathscr{C}^g$.

For a field $\mathbb{L}$ between $\mathbb{k}$ and $\overline{\mathbb{k}}$ let $\mathcal{P}$ be a point of $S_g \setminus \mathscr{C}_{\mathbb{L}}$ represented by $(P_1, \cdots, P_g)$. For every $\sigma \in G_{\mathbb{L}} = \mathrm{Gal}(\overline{\mathbb{k}}/\mathbb{L})$ we have $\sigma\mathcal{P} = \mathcal{P}$, hence there exists a permutation $\pi \in S_g$ such that $(\sigma P_1, \cdots, \sigma P_g) = (P_{\pi(1)}, \cdots, P_{\pi(g)})$. This mean that the formal sum $P_1 + \cdots + P_g$ is an effective divisor of degree g.

We get a map $\phi : S_g \setminus \mathscr{C}^g \to \mathrm{Pic}^0_{\mathscr{C}_{\mathbb{L}}}$ defined by

$$\phi_{\mathbb{L}}(\mathcal{P}) = P_1 + \cdots + P_g - gP_\infty.$$

Finally we can define the structure of variety on $\mathscr{J}_{\mathbb{L}} = \mathrm{Pic}^0_{\mathscr{C}_{\mathbb{L}}}$.

Remark. The point $\mathcal{P}_\infty = (P_\infty, \cdots, P_\infty)$ is sent via ϕ to the neutral element of the algebraic group $\mathscr{J}$.

Chapter 2

Classification

In this chapter we describe the curves according to the genus. We will consider always curves with at least a $\mathbb{k}$-rational point.

We refer to the the appendix of the book of Mumford [Mum99] and to [Cai10].

2.1 Rational maps associated to a linear system

Let $\varphi : \mathscr{C} \to \mathbb{P}^n$ be a rational map, we say that it is *nondegerate* if the image is not contained in any hyperplane of $\mathbb{P}^n$. We call it *dominant* if it cannot be a projection of any map of the type $\phi : \mathscr{C} \to \mathbb{P}^m$, with $m > n$.

For a given divisor $\mathcal{D}$ consider the associated complete linear system $|\mathcal{D}|$. Take a linear system $G \leq |\mathcal{D}|$ and assume that it has no base points. Then there is a bijection

$$\left\{\begin{array}{l}\text{Linear system}\\ \text{(i) without f.p.}\\ \text{(ii) projective dim. } n\\ \text{(iii) degree } r\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Rational maps}\\ \text{(i) nondegenerate}\\ \text{(ii) } \mathscr{C} \to \mathbb{P}^n\\ \text{(iii) degree of the image } r\end{array}\right\} /\text{projectivity},$$

which can be restricted to a bijection

$$\left\{\begin{array}{l}\text{Linear system}\\ \text{(i) complete}\\ \text{(ii) projective dim. } n\\ \text{(iii) degree } r\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Rational maps}\\ \text{(i) dominant}\\ \text{(ii) } \mathscr{C} \to \mathbb{P}^n\\ \text{(iii) degree of the image } r\end{array}\right\} /\text{projectivity}.$$

Indeed, a given linear system G is a projective subspace of $\mathbb{P}(\mathscr{L}(\mathcal{D}))$, then we can fix a projective basis $\varphi_0, \cdots, \varphi_n$ of G. The element $(\varphi_0, \cdots, \varphi_n) \in \mathbb{P}^n(\mathbb{k}(\mathscr{C}))$ is the map that we want to. Note that every basis of G gives the same map up to projectivity of $\mathbb{P}^n(\mathbb{k})$.

2.2 Genus 0

A projective curve $\mathscr{C}$ has genus 0 if and only if there exists a point P such that $d(P) = 1$. Then the curve $\mathscr{C}$ is birational to the projective line $\mathbb{P}^1$. Indeed the map $\mathscr{C} \to \mathbb{P}^1$ is nonconstant and it has a unique pole (it is dominant), hence birational.

2.3 Genus 1

Let $\mathscr{C}$ be a curve of genus 1. Since $d(rP) = r - g + \ell(W - rP) = r - 1$ for $r \geq 1$, the space $\mathscr{L}(rP)$ is given by the bases

$$\begin{aligned} \langle 1 \rangle_{\Bbbk} \quad & if \quad r = 1, \\ \langle 1, \phi \rangle_{\Bbbk} \quad & if \quad r = 2, \\ \left\langle 1, \phi, \phi' \right\rangle_{\Bbbk} \quad & if \quad r = 3, \\ \left\langle 1, \phi, \phi', \phi^2 \right\rangle_{\Bbbk} \quad & if \quad r = 4, \\ \left\langle 1, \phi, \phi', \phi^2, \phi\phi' \right\rangle_{\Bbbk} \quad & if \quad r = 5, \\ \left\langle 1, \phi, \phi', \phi^2, \phi\phi', \phi^3 \right\rangle_{\Bbbk} \quad & if \quad r = 6. \end{aligned}$$

Note that also ϕ'^2 is in $\mathscr{L}(6P)$, therefore there exists a linear relationship between ϕ'^2, ϕ^3 and other terms. Put now $\phi = X, \phi' = Y$, hence there exists a cubic relationship over the affine plane. Then we can say that every curve of genus 1 is birationally equivalent to a smooth curve $\mathscr{E}$ of degree 3. Note that we used the divisor $\mathcal{D} = 3P$ and its corresponding rational map $\mathscr{C} \to \mathbb{P}^2$ of degree 3, where $2 = d(3P)$.

If we use the divisor $\mathcal{D} = 4P$, instead of the divisor $3P$, we obtain a different classification of the curve: an intersection of two quadrics in the three dimensional projective space. Indeed let $X = \phi, Y = \phi', Z = \phi^2$; the first relation is defined by $Z = X^2$ and the second one depends on a linear relationship between XZ and Y^2 and other terms that appear in $\mathscr{L}(6P)$.

A curve of genus 1 is called *elliptic curve* if it has a $\Bbbk$-rational point.

Construction of the sum

For every nonzero effective divisor $\mathcal{D}$, since the genus of $\mathscr{E}$ is 1 and the divisors of positive degree are nonspecial, we have $d(\mathcal{D}) = \deg(\mathcal{D}) - 1$. If $\mathcal{D} + Q \sim nO \sim \mathcal{D} + Q'$ then $d(nO - \mathcal{D}) = \deg(nO - \mathcal{D}) - 1 = 0$. We can find out only one function in $\mathscr{L}(nO - \mathcal{D})$ up to multiplicative constants, then the zero is unique. In particular $Q \sim Q'$ implies $Q = Q'$.

Fix a point O for every two points P, Q we defined the sum $P \oplus Q$ in such a way: since $d(3O - P - Q) = 0$ there exists a unique (up to constant) rational function ϕ such that $\operatorname{div}(\phi) = P + Q + P * Q - 3O$, for a unique point $P * Q$; we can do it two times and set

$$P \oplus Q = O * (P * Q).$$

It is easy to see that it is an abelian group with O as neutral element.

If the curve is represented by its cubic embedding in the plane then the rational function ϕ must have three zeros on the elliptic curve, hence it has degree 1, therefore it is a line. We will see the explicit construction in the next chapter.

2.4 Genus 2

A canonical divisor $\mathcal{K} = \mathrm{div}(\omega)$ has $\deg \mathcal{K} = 2g - 2 = 2$ and $d(\mathcal{K}) = 1$. Then the corresponding projective map $\kappa : \mathscr{C} \to \mathbb{P}^1$, called the *canonical map*, has degree 2. We say that a curve for which exists a rational map $\mathscr{C} \to \mathbb{P}^1$ of degree 2 is an *hyperelliptic curve.*
Then every curve of genus 2 is an hyperelliptic curve.

2.5 Canonical maps and hyperelliptic curves

More generally we have that a rational map $\phi : \mathscr{C} \to \mathbb{P}^n$ defined by a divisor $\mathcal{D}$ is:

i) *injective* if $\ell(\mathcal{D} - P - Q) = \ell(\mathcal{D}) - 2$ for every $P \neq Q$ in $\mathscr{C}$;

ii) an *immersion* if $\ell(\mathcal{D} - P - Q) = \ell(\mathcal{D}) - 2$ for every P, Q in $\mathscr{C}$.

And we call the divisor $\mathcal{D}$ *very ample* if (ii) holds.
Indeed if $\phi(P) = \phi(Q)$ and $P \neq Q$ we have

$$\mathscr{L}(\mathcal{D} - P - Q) = \mathscr{L}(\mathcal{D} - P) = \mathscr{L}(\mathcal{D} - Q);$$

moreover if $\mathscr{L}(\mathcal{D} - 2P) = \mathscr{L}(\mathcal{D} - P)$ this mean that every function in $\mathscr{L}(\mathcal{D})$ that have zeros (with order bigger than the necessary for $\mathcal{D}$) in P has order 2 (more than the necessary) in P, so that the differential of these functions (with respect the uniforming parameter) has a zero (more than the necessary) in P and it is not an immersion.

A canonical divisor $\mathcal{K} = \mathrm{div}(\omega)$ has no base point for $g \geq 1$, i.e. for every point P we have $\ell(\mathcal{K} - P) = \ell(\mathcal{K}) - 1$, indeed $\ell(\mathcal{K}) - 1 = g - 1$ and

$$1 = \ell(P) = \deg(P) + 1 - g + \ell(\mathcal{K} - P).$$

The canonical map $\kappa : \mathscr{C} \to \mathbb{P}^{g-1}$ could be an immersion or not. The latter case implies that for P, Q in $\mathscr{C}$ we have $\ell(\mathcal{K} - P - Q) = \ell(\mathcal{K}) - 1 = g - 1$. By Riemann-Roch we have also

$$\ell(\mathcal{K} - P - Q) = g - 3 - \ell(P + Q),$$

so that $\ell(P + Q) = 2$. Then there exists a birational map $\mathscr{C} \to \mathbb{P}^1$ of degree 2, hence the curve is hyperelliptic.

2.6 Genus ≥ 3

For a genus $g \geq 3$ we can have either hyperelliptic curves, if the canonical map is not an immersion, or nonhyperelliptic curves if the canonical map is an immersion. Then, in the latter case, every canonical divisor $\mathcal{K} = \operatorname{div}(\omega)$ is very ample.

Considering the canonical map $\kappa : \mathscr{C} \to \mathbb{P}^{g-1}(\mathbb{k})$, for every homogeneous polynomial $F \in \mathbb{k}[X_0, \cdots, X_{g-1}]_m$ (the set of homogeneous polynomial of degree m) we can define the divisor in $\mathscr{C}$ of F to be

$$\operatorname{div}_{\mathscr{C}} F = \operatorname{div}\left(\frac{F}{\psi} \circ \kappa\right),$$

where $\psi \in \mathbb{k}[X_0, \cdots ; X_{g-1}]_m$ is a function such that the zeros in $\kappa(\mathscr{C})$ are different from the zeros in $\kappa(\mathscr{C})$ of F (for example it could be m times an hyperplane).

We have $\operatorname{div}_{\mathscr{C}} F \sim m\mathcal{K}$ and therefore a linear application

$$\Phi_m : \mathbb{k}[X_0, \cdots, X_{g-1}]_m \to \mathscr{L}(m\mathcal{K}), \quad F \to \frac{F}{\psi} \circ \kappa.$$

The kernel of this application is given by the functions that are identically zero on $\kappa(\mathscr{C})$, hence they give equations for $\kappa(\mathscr{C})$.

Using $\ell(m\mathcal{K}) = \deg(m\mathcal{K}) - g + 1 = 2(g-1)m - (g-1)$ we have

$$\dim_{\mathbb{k}} \ker(\Phi_m) \geq \underbrace{\binom{m+g-1}{m}}_{\text{dim of } \mathbb{k}[X_0,\cdots,X_{g-1}]_m} + \underbrace{(g-1) - 2(g-1)m}_{-\text{ dim of } \mathscr{L}(m\mathcal{K})}.$$

Genus 3.

$$\begin{aligned} \dim_{\mathbb{k}} \ker(\Phi_m) \geq \quad & 6 - 8 + 2 = 0 && \text{if } m = 2; \\ & 10 - 12 + 2 = 0 && \text{if } m = 3; \\ & 15 - 16 + 2 = 1 && \text{if } m = 4. \end{aligned}$$

We have at least one eqution of degree 4. Then *the projective curves of genus 3 are either hyperelliptic or birational to a smooth plane curve of degree 4.*

Genus 4.

$$\begin{aligned} \dim_{\mathbb{k}} \ker(\Phi_m) \geq \quad & 10 - 12 + 3 = 1 && \text{if } m = 2; \\ & 20 - 18 + 3 = 5 && \text{if } m = 3. \end{aligned}$$

We have at least one equation of degree 2 and one independent equation of degree 3. Then *the projective curves of genus 4 are either hyperelliptic or birational to a smooth intersection of a quadric and a cubic.*

Genus $\geq$ 5. For $g \geq 5$ we have three type of curves: hyperelliptic, smooth intersection of quartics in $\mathbb{P}^{g-1}$ or triple ramified covers of the Riemann' sphere.

2.7 Hyperelliptic representation

Assume now that we are working on an algebraic closed field $\Bbbk$ of odd characteristic. Let $\mathscr{C}$ be an hyperelliptic curve of genus g. By definition there exists a rational map $x : \mathscr{C} \to \mathbb{P}^1$ of degree 2. By Hurwitz formula the total ramification is $2g+2$, hence there exist $2g+2$ ramification points of ramification 1, the so called Weierstrass points. We denote these points with $P_1, \cdots, P_{2g+2}$. Let $\operatorname{div}_\infty(x) = Q + R$, we can assume, up to projectivity of the line, that Q and R are not Weierstrass points.
We define $a_i = x(P_i)$ and the map $\iota : \mathscr{C} \to \mathscr{C}$ to be the map that exchange the inverse images of the rational map x. Obviously we have $\iota^2 = id_{\mathscr{C}}$.
We look now at the divisor $\mathcal{D} = (g+1)Q + (g+1)R$. By Riemann-Roch we have $\ell(\mathcal{D}) = \deg(\mathcal{D}) - g + 1 = g + 3$.
Since $\iota(\mathcal{D}) = \mathcal{D}$ we can consider the endomorphism $\iota^* : \mathscr{L}(\mathcal{D}) \to \mathscr{L}(\mathcal{D})$, it is clear that ${\iota^*}^2 = id$, hence it is diagonalisable with eigenvalue ± 1. We can decompose $\mathscr{L}(\mathcal{D})$ in $\mathscr{L}(\mathcal{D})^+ \oplus \mathscr{L}(\mathcal{D})^-$ where $\mathscr{L}(\mathcal{D})^+ = \langle 1, x, \cdots, x^{g+1} \rangle$ has dimension $g+2$ and $\mathscr{L}(\mathcal{D})^- = \langle y \rangle$, with $\iota^*(y) = -y$, has dimension 1.
Fix $f(x) = \prod_{i=1}^{2g+2}(x - a_i)$. We want to prove that $y^2 = cf(x)$ for some nonzero $c \in \Bbbk$. In order to do this we show that the corresponding divisor of y^2 and $f(x)$ are the same, so that the quotient function is a constant. We have:

$$\operatorname{div}(y) = \sum_i P_i - \mathcal{D}$$

because $y(P_i) = -y(P_i)$, hence $\deg(\operatorname{div}_0(y)) = 2g+2$ (we are working in odd characteristic), and the only possible pole are Q and R with $g+1$ as maximum degree; on the other hand

$$\operatorname{div}(f(x)) = \sum_i \operatorname{div}_0(x - a_i) - \sum_i \operatorname{div}_\infty(x - a_i) = 2\sum_i P_i - 2\mathcal{D}.$$

We proved the following

Proposition 2.7.1. *A projective curve is hyperelliptic of genus g if and only if it is birationally equivalent to a projective plane curve of the form $y^2 = f(x)$, where f has degree $2g+2$ and it has no double roots.*

Remark.

i) If we assume that $\operatorname{div}_\infty(x) = 2P$, with P a Weierstrass point, then we can prove with the same argument that every hyperelliptic curve is birationally equivalent to a projective plane curve of the form $y^2 = f(x)$, where f has degree $2g+1$ and it has no double roots.

ii) In a field of characteristic 2 we can show that any hyperelliptic curve is birational to a projective plane curve of the form $y^2 + h(x)y = f(x)$, with $\deg(h) \leq g$ and $\deg(f) = 2g+1$.

Chapter 3

Arithmetic on Elliptic curves

Throughout this chapter we present some examples of elliptic curves. We study if an elliptic curve can be expressed with a particular polynomial according to the base field $\Bbbk$ and we give some explicit formulæ for the computation of the addition law. For the first section we will mainly refer to [Coh+10], for the second to [JTV10] and for the third to [BL07a], [Ber+08], [Are+11], and [BL07b].

We give some explicit formulæ for the addition law. It is very important to find fast algorithm that could save some field operation for computing addition on elliptic curve. Here the symbols **I**, **M**, and **S** stand for the running time for an inversion, a multiplication, and a square in the field $\Bbbk$. We always neglect the running time of additions.

3.1 Weiestrass curves

An elliptic curve over $\Bbbk$ is in the *Weierstrass form* if it satisfies the equation

$$\mathscr{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with the condition of nonsingularity, i.e. the partial derivativs $2y_1 + a_1x_1 + a_3$ and $3x^2 + 2a_2x + a_4 - a_3y$ do not vanish simultaneously. Let

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - 4a_2a_6 + a_2a_3^2 - a_4^2 \end{aligned}$$

In a field of characteristic different from 2 we can consider the isomorphic curve

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

given by the isomorphism $y \mapsto y - (a_1x + a_3)/2$.
If moreover the characteristic is different from 3, then we can apply the isomorphism $x \mapsto \big(x - (\frac{b_2}{4})/3\big)$ and we can consider equations in which the coefficient of x^2 is zero.

The addition law of two points P and Q in an arbitrary field $\Bbbk$ is given in the classical way:

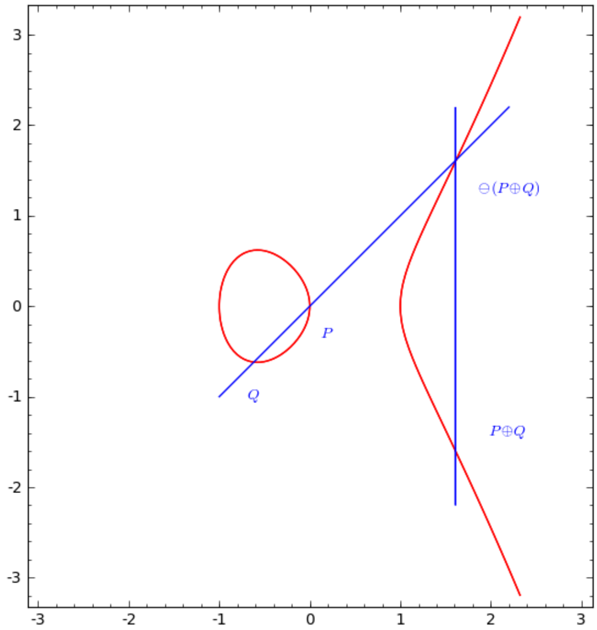

Figure 3.1: Addition law on Weierstrass curves

i) find the line passing through P and Q (if $P = Q$ find the tangent line);

ii) find the third $\tilde{R}$ point of intersection;

iii) repeat (i) and (ii) for $\tilde{R}$ and the fixed flex P_∞, the (unique) point at infinity.

This gives the sum $R = P \oplus Q$. Figure 3.1 describes this construction. The opposite point of a given point (x_1, y_1) is $(x_1, -y_1 - a_1x_1 - a_3)$, the neutral element is the unique point at infinity $P_\infty = [0, 1, 0]$.
We compute now the sum explicitly. Take $P = (x_1, y_1) \neq Q = (x_2, y_2)$ with $x_1 \neq x_2$. We want to compute $R = P \oplus Q = (x_3, y_3)$. The slope of the line passing through P and Q is

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2},$$

the equation of the line is given by

$$l : y = \lambda x + \frac{x_1y_2 - x_2y_1}{x_1 - x_2}.$$

We denote the constant term by μ. The intersection of l and $\mathscr{E}$ gives us the equation

$$(\lambda x + \mu)^2 + (a_1x + a_3)(\lambda x + \mu) = x^3 + a_2x^2 + a_4x + a_6$$

and then the equation

$$f(x) = x^3 + (a_2 - a_1\lambda - \lambda^2)x^2 + (a_4 - 2\lambda\mu - a_3\lambda - a_1\mu)x + a_6 - \mu^2 - a_3\mu = 0.$$

We already know two different roots of f in $\Bbbk$, so the third one is still in $\Bbbk$. The coefficient of x^2, multiplied by -1, equals the sum of the roots of f, then

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

and $\tilde{y}_3 = \lambda x_3 + \mu$, where $(x_3, \tilde{y}_3) = \ominus R$. Hence

$$R = (x_3, -\lambda x_3 - \mu - a_1 x_3 - a_3).$$

If $P = Q$ we can do the same thing with the slope given by implicit derivatives. Finally we have

$$\begin{aligned}
\ominus P &= (x_1, -y_1 - a_1 x - a_3), \\
P \oplus Q &= (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -\lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3), \text{where} \\
\lambda &= \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } P \neq \pm Q \\[2ex] \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} & \text{if } P = Q \end{cases}
\end{aligned}$$

In characteristic different from 2 and 3 we can assume that $\mathscr{E}$ is given by the equation $y^2 = x^3 + a_4 x + a_6$. The formulæ for adding and doubling points require respectively $\mathbf{I} + 2\mathbf{M} + \mathbf{S}$ and $\mathbf{I} + 2\mathbf{M} + 2\mathbf{S}$. For cryptographic applications we always need to compute a scalar multiplication of a point, in order to do this we need to recursively add a point after doubling. The next formulæ gives us a faster way to compute $[2]P \oplus Q = (P \oplus Q) \oplus P$, saving one multiplication:

$$\begin{array}{lll}
A = (x_2 - x_1)^2, & B = (y_2 - y_1)^2, & C = A(2x_1 + x_2) - B, \\
D = C(x_2 - x_1), & E = D^{-1}, & \lambda = CE(y_2 - y_1), \\
\lambda_2 = 2y_1 A(x_2 - x_1)E - \lambda, & x_4 = (\lambda_2 - \lambda)(\lambda_2 + \lambda) + x_2, & y_4 = (x_1 - x_4)\lambda_2 - y_1,
\end{array}$$

where we assume that $P \neq \pm Q$ and $[2]P \neq -Q$. It needs $\mathbf{I} + 9\mathbf{M} + 2\mathbf{S}$.

Affine coordinates

In case $\Bbbk$ has characteristic bigger than 3 then an elliptc curve can be given by the equation $\mathscr{E} \ : \ y^2 = x^3 + a_4 x + a_6$. We can write simplified formulæ for the addition law.

Addition. Let $P = (x_1, y_1), Q = (x_2, y_2)$ be two points on the elliptic curve $\mathscr{E}$ such that $P \neq \pm Q$, then the point $P \oplus Q = (x_3, y_3)$ can be computed by

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}, \qquad x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

It requires $\mathbf{I} + \mathbf{M} + \mathbf{S}$.

Doubling. Let $P = (x_1, y_1)$ be a point on the elliptic curve $\mathscr{E}$ and write $[2]P = (x_3, y_3)$, then put

$$\lambda = \frac{3x_1^2 + a_4}{2y_1}, \qquad x_3 = \lambda^2 - 2x_1, \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

It requires **I** + 2**M** + **S**.

Projective coordinates

In projective coordinates the equation for $\mathscr{E}$ becomes $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$.

Addition. Let $P = [X_1, Y_1, Z_1], Q = [X_2, Y_2, Z_2]$ be two points on $\mathscr{E}$ such that $P \neq \pm Q$, then the point $P \oplus Q = [X_3, Y_3, Z_3]$ can be computed by

$$A = Y_1 \cdot Z_2, \quad B = X_1 \cdot Z_2, \quad C = Z_1 \cdot Z_2, \quad D = Y_2 \cdot Z_1 - A, \quad E = X_2 \cdot Z_1 - B,$$

$$F = E^2, \quad G = E \cdot F, \quad H = F \cdot B, \quad I = D^2 \cdot C - G - 2H,$$

$$X_3 = E \cdot I, \quad Y_3 = D \cdot (H - I) - GA, \quad Z_3 = G \cdot C$$

It requires 12**M** + 2**S**. Note that if one of the inputs is already in affine coordinates, i.e. has form $[X_1, Y_1, 1]$, then the requirements decrease to 9**M** + 2**S**.

Doubling. Let $P = [X_1, Y_1, Z_1]$ be a point on the elliptic curve $\mathscr{E}$ and let $[2]P = [X_3, Y_3, Z_3]$, then put

$$A = a_4Z_1^2 + 3X_1^2, \quad B = Y_1 \cdot Z_1, \quad C = X_1 \cdot Y_1 \cdot B, \quad D = A^2 - 8C,$$

$$X_3 = 2B \cdot D, \quad Y_3 = A \cdot (4C - D) - 8Y_1^2 \cdot B^2, \quad Z_3 = 8B^3$$

It requires 7**M**+5**S**.

Jacobian coordinates

In jacobian coordinates the point $[X_1, Y_1, Z_1]$ on the elliptic curve $\mathscr{E}$ corresponds to the affine point $(X_1/Z_1^2, Y_1/Z_1^3)$ if $Z_1 \neq 0$, so that the equation of the elliptic curve $\mathscr{E}$ becomes

$$Y^2 = X^3 + a_4Z^4 + a_6Z^6.$$

The neutral element is $(1, 1, 0)$ and the opposite of $[X_1, Y_1, Z_1]$ is $[X_1, -Y_1, Z_1]$.

Addition. Let $P = [X_1, Y_1, Z_1], Q = [X_2, Y_2, Z_2]$ be two points on $\mathscr{E}$ such that $P \neq \pm Q$, then the point $P \oplus Q = [X_3, Y_3, Z_3]$ can be computed by

$$U_2 = Z_1^2, \quad U_3 = Z_1 \cdot U_2, \quad V_2 = Z_2^2, \quad V_3 = Z_2 \cdot V_2,$$

$$A = X_1 \cdot V_2, \quad B = X_2 \cdot U_2, \quad C = Y_1 \cdot V_3, \quad D = Y_2 \cdot U_3, \quad E = B - A,$$

$$F = D - C, \quad G = E^2, \quad H = E \cdot G, \quad I = A \cdot G,$$

$$X_3 = -H - 2I + F^2, \quad Y_3 = -C \cdot H + F \cdot (I - X_3), \quad Z_3 = Z_1 \cdot Z_2 \cdot E.$$

It takes 12**M** + 4**S**. If one of the inputs is already in affine coordinates, then the requirements decrease to 8**M** + 3**S**.

Doubling. Let $P = [X_1, Y_1, Z_1]$ be a point on the elliptic curve $\mathscr{E}$ and let $[2]P = [X_3, Y_3, Z_3]$, then put

$$A = Y_1^2, \quad B = 3X_1^2 + a_4 Z_1^4, \quad C = 4X_1 \cdot A$$

$$X_3 = -2C + B^2, \quad Y_3 = -8A^2 + B \cdot (C - X_3), \quad Z_3 = 2Y_1 \cdot Z_1.$$

It requires 4**M** + 6**S**. Note that if a_4 is small then its multiplication can be neglected; note that for $a_4 = -3$ we can use $B' = 3X_1^2 - 3Z_1^4 = 3(X_1 - Z_1^2)(X_1 + Z_1^2)$ leading to the requirement 4**M** + 4**S**.

Chudnovky-Jacobian coordinates

In order to improve the addition in Jacobian coordinates we can represent a point $[X_1, Y_1, Z_1]$ with the quintuple $(X_1, Y_1, Z_1, Z_1^2, Z_1^3)$. The formulæ for addition and doubling are the same for jacobian coordinates, but the complexity descreases to 11**M** + 3**S** and 5**M** + 6**S** respectly.

Modified Jacobian coordinates

We can represent the point $[X_1, Y_1, Z_1]$ in jacobian coordinates with the quintuple $(X_1, Y_1, Z_1, a_4 Z_1^4)$. The formulæ are essentially the same. In the doubling formula we can add $D = 8A^2$ so that $Y_3 = -D + B(C - X_3)$ and $a_4 Z_3^4 = 2D(a_4 Z_1^4)$. This new algorithm takes 13**M** + 6**S** for the addition and 4**M** + 4**S** for doubling.

3.2 Huff's curves

Let $\Bbbk$ a field of characteristic different from 2. An elliptic curve over $\Bbbk$ is in Huff form if it satisfies the equation

$$\mathscr{E} : ax(y^2 - 1) = by(x^2 - 1),$$

or in projective coordinates

$$\mathscr{E} : aX(Y^2 - Z^2) = bY(X^2 - Z^2),$$

where $a^2 \neq b^2$ and $ab \neq 0$ (this guaranties the smoothness). It has three points at infinity, respectively $[1, 0, 0], [0, 1, 0], [a, b, 0]$.

The addition law of two points P and Q is defined likewise the law for the Weierstrass form:

i) find the line passing through P and Q (if $P = Q$ find the tangent line);

ii) find the third $\tilde{R}$ point of intersection;

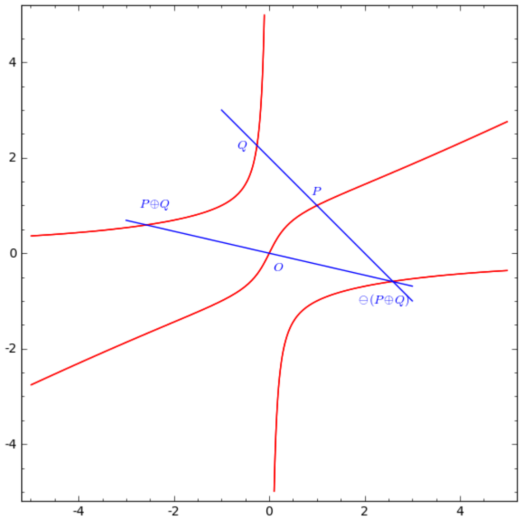

Figure 3.2: Addition law on Huff curves

iii) repeat (i) and (ii) for $\tilde{R}$ and the fixed flex $O = [0, 0, 1]$.

Figure 3.2 describes this construction.
In particular the inverse of a point $[X, Y, Z]$ is $[X, Y, -Z]$.
For the points at infinity we have:

$$\begin{aligned}
[X, Y, Z] \oplus [1, 0, 0] &= [Z^2, -XY, XZ] \\
[X, Y, Z] \oplus [0, 1, 0] &= [-XY, Z^2, YZ] \\
[X, Y, Z] \oplus [a, b, 0] &= \begin{cases} [a, b, 0] & \text{if } [X, Y, Z] = [0, 0, 1] \\ [YZ, XZ, -XY] & \text{otherwise} \end{cases}
\end{aligned}$$

Affine formulæ

We now study the explicit formulæ for the affine plane. Let as usual $y = \lambda x + \mu$ be the secant line passing through the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. So that $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ and $\mu = y_1 - \lambda x_1$.
In order to find $P \oplus Q$, i.e. the opposite the third point of intersection of the line with the Huff's curve, we must solve the equation

$$ax((\lambda x + \mu)^2 - 1) = b(\lambda x + \mu)(x^2 - 1)$$

and then

$$\lambda(a\lambda - b)x^3 + \mu(2a\lambda - b)x^2 + (\lambda b - a)x + \mu b = 0.$$

We get

$$\begin{cases} x_1 + x_2 - x_3 = \dfrac{\mu(2a\lambda - b)}{\lambda(a\lambda - b)} \\ \\ y_3 = \lambda x_3 - \mu \end{cases}$$

Now, starting from the equation of the curve, we have

$$ax_1(y_1^2-1)=by_1(x_1^2-1) \text{ and } ax_2(y_2^2-1)=by_2(x_2^2-1).$$

Multiplying the first equation by y_2 and the second by y_1 and subtracting we get

$$y_1y_2(ax_1y_1-ax_2y_2-bx_1^2-b+bx_2^2+b)-ax_1y_2+ax_2y_1=0$$

and then

$$y_1y_2(x_1+x_2)(a(y_1-y_2)-b(x_1-x_2))=a(x_2y_1-ax_1y_2)(y_1y_2-1). \tag{3.1}$$

If we instead multiply the first equation by x_2 and the second by x_1 and we subtract, then we get

$$ax_1x_2(y_1^2-y_2^2)+b((x_1+x_2)(y_1-y_2)-x_1y_1+x_2y_2)=b(y_1x_1^2x_2-y_2x_2^2x_1)$$

and then

$$(ax_1x_2(y_1+y_2)+b(x_1+x_2))(y_1-y_2)=b(x_1y_1-x_2y_2)(x_1x_2+1). \tag{3.2}$$

Coming back to the addition formula, we substitute the value of λ and μ in $x_1+x_2-x_3$, and then

$$x_3=x_1+x_2+\frac{(x_1y_2-x_2y_1)(2a(y_1-y_2)-b(x_1-x_2))}{(y_1-y_2)(a(y_1-y_2)-b(x_1-x_2))},$$

we use (3.1) and we get

$$\begin{aligned}
x_3 &= x_1+x_2-\frac{(2a(y_1-y_2)-b(x_1-x_2))y_1y_2(x_1+x_2)}{a(y_1y_2-1)(y_1-y_2)}\\
&= x_1+x_2-\frac{x_2y_1-x_1y_2}{y_1-y_2}-\frac{(x_1-x_2)y_1y_2}{y_1y_2-1}\\
&= \frac{x_1y_1-x_2y_2}{y_1-y_2}-\frac{(x_1-x_2)y_1y_2}{y_1y_2-1}.
\end{aligned}$$

Now we could use (3.2) and we get

$$\begin{aligned}
x_3 &= \frac{ax_1x_2(y_1+y_2)+b(x_1+x_2)}{b(x_1x_2+1)}-\frac{(x_1-x_2)y_1y_2}{y_1y_2-1}\\
&= \frac{(x_1+x_2)(1+y_1y_2)}{(1+x_1x_2)(1-y_1y_2)}.
\end{aligned}$$

By symmetry we can compute y_3 and we get finally

$$\begin{cases}
x_3=\dfrac{(x_1+x_2)(1+y_1y_2)}{(1+x_1x_2)(1-y_1y_2)}\\[2ex]
y_3=\dfrac{(y_1+y_2)(1+x_1x_2)}{(1-x_1x_2)(1+y_1y_2)}
\end{cases}$$

Note that the parameters a, b, λ, μ are not involved. Moreover we can use this formula for the doubling. Note also that it is defined for $x_1x_2 \neq \pm 1, y_1y_2 \neq \pm 1$.

Projective formulæ

In order to avoid inversion we can use projective coordinates. We have

$$\begin{cases} X_3 = (X_1Z_2 + X_2Z_1)(Z_1Z_2 + Y_1Y_2)^2(Z_1Z_2 - X_1X_2) \\ Y_3 = (Y_1Z_2 + Y_2Z_1)(Z_1Z_2 + X_1X_2)^2(Z_1Z_2 - Y_1Y_2) \\ Z_3 = (Z_1^2Z_2^2 - X_1^2X_2^2)(Z_1^2Z_2^2 - Y_1^2Y_2^2) \end{cases}$$

In particular we can use the following algorithm

$$A = X_1 \cdot X_2, \quad B = Y_1 \cdot Y_2, \quad C = Z_1 \cdot Z_2,$$
$$D = (X_1 + Z_1) \cdot (X_2 + Z_2) - A - C, \quad E = (Y_1 + Z_1) \cdot (Y_2 + Z_2) - B - C,$$
$$F = (C - A) \cdot (B + C), \quad G = (C - B) \cdot (A + C),$$
$$H = D \cdot (B + C), \quad I = E \cdot (A + C),$$
$$X_3 = H \cdot F, \quad Y_3 = I \cdot G, \quad Z_3 = G \cdot F.$$

It needs 12**M**.

For a doubling we can use the squaring instead of the multiplication in A, B, C, D, E, hence it needs 7**M** + 5**S**. We can speed up the doubling in case **S**$>\frac{3}{4}$**M** with the following

$$A = X_1 \cdot Y_1, \quad B = X_1 \cdot Z_1, \quad C = Y.1Z_1, \quad D = Z_1^2,$$
$$E = (B - C) \cdot (B + C), \quad F = (A - D) \cdot (A + D),$$
$$G = (A - D) \cdot (B - C), \quad H = (A + D) \cdot (B + C),$$
$$X_3 = (G - H) \cdot (E + F), \quad Y_3 = (G + H) \cdot (E - F), \quad Z_3 = (E + F) \cdot (E - F).$$

It takes 10**M** + **S**.

Theorem 3.2.1. *Let $P = [X_1, Y_1, Z_1]$ and $P = [X_2, Y_2, Z_2]$. Then the addition formula is valid provided that $X_1X_2 \neq Z_1Z_2$ and $Y_1Y_2 \neq Z_1Z_2$.*

Proof. We already know the the affine formula is valid whenever $x_1x_2 \neq 1$ and $y_1y_2 \neq 1$, so that the formula is valid when $X_1X_2 \neq \pm Z_1Z_2, Y_1Y_2 \neq \pm Z_1Z_2$. We remark that adding $[1, 0, 0]$ or $[0, 1, 0]$ with an other point, the formula gives $[0, 0, 0]$, that is not a well defined point in the projective space. Adding the point $[a, b, 0]$ to an other point $[X_1, Y_1, Z_1] \notin \{O, [1, 0, 0], [0, 1, 0]\}$, this formula gives $[-Y_1Z_1, -X_1Z_1, X_1Y_1]$: the correct answer. □

Remark.

1. In order to avoid these cases we can fix a point $R = [X_3, Y_3, Z_3]$ on the Huff curve and compute $P \oplus Q = (P \oplus R) \oplus (Q \oplus -R)$ if P and Q are different from $[1, 0, 0]$ and $[0, 1, 0]$; it will works for a general R.

2. The points at infinity $[1,0,0], [0,1,0]$ and $[a,b,0]$ are the points of 2-torsion. Adding $[a,b,0]$ to any of the points $[\pm 1, \pm 1, 1]$ transforms it into its inverse, hence these four points are solutions of $[2]P = [a,b,0]$ and so are of order 4. These eight points form a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Corollary 3.2.2. *Let P a point of odd order in the Huff curve $\mathscr{E}$, then the addition formula is complete in the subgroup generated by P.*

Proof. Note first that the points at infinity cannot be in $\{P\}$ since they are of order 2. The same for the points $[\pm 1, \pm 1, 1]$ that are of order 4. Now, pick two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ in $\{P\}$. Suppose that $x_1 x_2 = \pm 1$. We have $ax_1(y_1^2 - 1) = by_1(x_1^2 - 1)$, this implies $a\frac{1}{x_1}(y_1^2 - 1) = by_1(1 - \frac{1}{x_1^2})$, hence $\pm ax_2(y_1^2 - 1) = -by_1(x_2^2 - 1)$. It follows that $\mp y_2(y_1^2 - 1) = y_1(y_2^2 - 1)$, hence $y_2 = \mp y_1$ or $y_2 = \pm\frac{1}{y_1}$. In all cases one of $P_1 \oplus P_2$ or $P_1 \ominus P_2$ has order 2, that is a contradiction. Likewise, $y_1 y_2 = \pm 1$ leads to a contradiction. □

Theorem 3.2.3. *Every elliptic curve $\mathscr{E}$ over a perfect filed $\mathbb{k}$ of odd characteristic is birationally equivalent over $\mathbb{k}$ to an Huff curve if and only if it contains a subgroup isomorphic to $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. We already know that an huff curve has a subgroup isomorphic to the group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Conversely let φ be the isomorphism that goes from G to $\mathscr{E}$ and use the notation $\mathscr{A}_{ab} = \varphi(a,b)$. So that $A_{10}, A_{11}, A_{31}, A_{30}$ are the 4-torsion points in the subgroup isomorphic to G. Doubling these points we obtain a unique point in G of order 2, namely $R = A_{20}$. Call $Q = A_{21}$ and $P = A_{01}$ the remaining points of order 2 in G.

We have $P \oplus R \ominus Q \ominus O = O$, then there exists a rational function x such that $\operatorname{div}(x) = Q + O - P - R$, we can assume that $x(A_{10}) = 1$. Likewise, there exists a rational function y such that $\operatorname{div}(y) = P - R - Q + O$ and $y(A_{10}) = 1$.

The function $x - 1$ has the same pole as x. So that $\operatorname{div}(x-1) = A_{10} + X - P - R$, we have $X = P \oplus R \ominus A = R \oplus A_{31} = A_{11}$. so that $x(A_{11}) = 1$. Likewise $y(A_{31}) = 1$.

Consider now the map $\iota : S \mapsto \ominus S$ for every point S in the elliptic curve. For every rational function f, denote by $\iota^* f$ the function $f \circ \iota$. This is an endomorphism of the space $\mathscr{L}(\cdot)$, such that $\iota^{*2} = id$. Since $\mathscr{L}_1 = \mathscr{L}(P + Q - R - O)$ has dimension 1 over $\mathbb{k}$ (by Riemann-Roch, using the fact that $P + Q - R - O$ is principal), it follows that $\iota^*_{|\mathscr{L}_1} = \pm 1$. If $\iota^* x = x$ then $x(A_{30}) = x(A_{10}) = 1$, but this contradicts the previous computation on $\operatorname{div}(x-1)$, hence we have that $\iota^* = -1$. Note that $x(A_{10}) = x(A_{11}) = 1$ implies $x(A_{31}) = x(A_{30}) = -1$, and we have $\operatorname{div}(x+1) = A_{31} + A_{30} - P - R$. In the same way we obtain $\operatorname{div}(y+1) = A_{11} + A_{30} - Q - R$.

Finally we consider the rational functions $u = x(y^2 - 1)$ and $v = y(x^2 - 1)$.

We have

$$\begin{aligned}
\mathrm{div}(u) &= \mathrm{div}(x) + \mathrm{div}(y-1) + \mathrm{div}(y+1) \\
&= (Q + O - P - R) + (A_{10} + A_{31} - R - Q) + (A_{11} + A_{30} - Q - R) \\
&= A_{10} + A_{11} + A_{31} + A_{30} + O - P - Q - 3R \\
&= (P + O - Q - R) + (A_{10} + A_{11} - P - R) + (A_{31} + D_{30} - P - R) \\
&= \mathrm{div}(y) + \mathrm{div}(x-1) + \mathrm{div}(x+1) \\
&= \mathrm{div}(v).
\end{aligned}$$

Then there exist a and b in $\mathbb{k}^\times$ such that $au = bv$, hence such that

$$ax(y^2 - 1) = by(x^2 - 1).$$

It remains to prove that the map that send a point S of the elliptic curve in $[x(S), y(S), 1]$ is injective. Suppose that there exist two points S and S' with the same image $[x_0, y_0, 1]$, then the two rational functions $x - x_0$ and $y - y_0$ have divisors respectively $S + S' - P - R$ and $S + S' - Q - R$, hence $P \oplus R = S \oplus S' = Q \oplus R$, that is a contradiction. □

3.3 Edwards and Twisted Edwards curves

Fix a field $\mathbb{k}$ of characteristic different from 2. An *Edwards elliptic curve* is given by the equation

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

where $cd(1 - dc^4) \neq 0$. Edwards shows that every elliptic curve over a number field could be transformed to an Edwards curve of the form $x^2 + y^2 = c^2(1 + x^2y^2)$, but some elliptic curves over finite field require a field extension for the transformation. See [Edw07] for further details.

In order to compute the addition law explicitly we restrict to finite fields.

Edwards and Weierstrass curves

The following theorem shows a way to represent elliptic curves in Edwards elliptic form.

Theorem 3.3.1. *Let $\mathscr{E}$ be an elliptic curve over $\mathbb{k}$ such that $\mathscr{E}$ has an element of order 4, then there exists $d \in \mathbb{k}, d \notin \{0, 1\}$ such that the curve $x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent over $\mathbb{k}$ to $\mathscr{E}$; if moreover $\mathscr{E}$ has a unique element of order 2, then there d is a nonsquare.*

Proof. Let's start with an elliptic curve $\mathscr{E}$ in Weierstrass form. Since the characteristic of the field is different from 2, we can assume that $\mathscr{E}$ has the form $s^2 = r^3 + a_2r^2 + a_4r + a_6$.
Let P be the point of order 4. Up to translation, we can assume that $2P = (0, 0)$ and thus $a_6 = 0$.

Write $P = (r_1, s_1)$. Note that there is a line passing through $O = (0,0)$ and tangent at P, that is $s_1 = \lambda r_1$ where λ is the slope $(3r_1^2 + 2a_2 r_1 + a_4)/2s_1$.
The point P satisfies the equation of the curve, i.e. $s_1^2 = r_1^3 + a_2 r_1^2 + a_4 r_1$. Then we have $r_1^3 = a_4 r_1$, hence $r_1^2 = a_4$, because $r_1 \neq 0$.
Combining these results we obtain

$$a_2 = \frac{s_1^2 - r_1^3 - a_4 r_1}{r_1^2} = 2\frac{1+d}{1-d} r_1,$$

where $d = 1 - 4r_1^3/s_1^2$.
Note that $d \neq 1$, since $r_1 \neq 0$; note also that $d \neq 0$, otherwise the equation for $\mathscr{E}$ would be $s^2 = r^3 + 2r_1 r^2 + r_1^2 r = r(r + r_1)^2$, but this is not an elliptic curve.
If d is a square, then there exists an other $\Bbbk$-rational point of order 2, namely $(r_1(\sqrt{d}+1)/(\sqrt{d}-1), 0)$.

Consider now the elliptic curve

$$\mathscr{E}' \ : \ \frac{r_1}{1-d} s^2 = r^3 + a_2 r^2 + a_4 r,$$

it is isomorphic to $\mathscr{E}$ because $\frac{r_1}{1-d} = \left(\frac{s_1}{2r_1}\right)^2$ is a square in $\Bbbk$.
Substitute $u = r/r_1$ and $v = s/r_1$ and we get a homothetic new coordinate system with $P = (1, s_1/r_1)$, hence $r_1 = 1 = a_4$. Then $\mathscr{E}'$ becomes

$$\mathscr{E}'' \ : \ \frac{1}{1-d} s^2 = r^3 + 2\frac{1+d}{1-d} r^2 + r.$$

Now we show that the curve $x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to $\mathscr{E}''$ via the rational map $(s,r) \mapsto (x,y) = (2r/s, (r-1)/(r+1))$. The inverse function is $(x,t) \mapsto (r,s) = ((1+y)/(1-y), 2(1+y)/(1-y)x)$. In both maps there are only finitely many exceptional point. In a similar way, putting $1/d$ for d and $-u$ for u, we can show that $x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to $\mathscr{E}''$. □

Remark. For $d = \bar{d}\bar{c}^4$ we have that the curve $x^2 + y^2 = 1 + dx^2y^2$ is isomorphic to the curve $\bar{x}^2 + \bar{y}^2 = \bar{c}^2(1 + \bar{d}\bar{x}^2\bar{y}^2)$ via $\bar{x} = \bar{c}x,\ \bar{y} = \bar{c}y$. Note that if $\Bbbk$ is a finite field, then at least 1/4 of the possibilities of $\bar{d} \in \Bbbk^\times$ gives us a 4-power $d/\bar{d}$.

Addition on Edwards curves

The addition law on an Edwards curve $x^2+y^2 = c^2(1+dx^2y^2)$, with $cd(1-dc^4) \neq 0$, is given by

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \longmapsto \begin{pmatrix} \dfrac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)} \\ \\ \dfrac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \end{pmatrix}$$

the neutral element is $(0, c)$, and the inverse of (x_1, y_1) is $(-x_1, y_1)$. This addition law is defined when $dx_1x_2y_1y_2 \notin \{+1, -1\}$.

Now we give two result involving the addition law. The first says that the birational equivalence between an elliptic curve in Weierstrass form and the Edwards curve preserves the group law. The second says that the addition law is complete when d is nonsquare.

Theorem 3.3.2. *Let $e = 1 - dc^4$ and let $\mathcal{E}$ be the elliptic curves*

$$\frac{1}{e}v^2 = u^3 + \frac{4}{e-2}u^2 + u.$$

Then $\mathcal{E}$ is birationally equivalent to $x^2 + y^2 = c^2(1 + dx^2y^2)$ via

$$(x, y) \longmapsto \left(\begin{array}{c} u \\ v \end{array} \right) = \left(\begin{array}{c} \dfrac{c+y}{c-y} \\ \dfrac{2c(c+y)}{(c-y)x} \end{array} \right)$$

and this rational map preserves the group law (for the points in which it is defined).

Proof. The birational equivalence is given by essentially the same computation as in Theorem 3.3.1.
We need to show that the addition law is preserved.

The proof for the particular cases involving the points $(0, c), (0, -c)$ on the Edwards curve, hence the points $P_\infty, (0, 0)$ on the Weierstrass curve, can be done analysing each possibility.

In general, after the assumption that $x_1x_2x_3 \neq 0$, we can distinguish two cases: $(u_1, v_1) = (u_2, v_2)$ and $u_1 \neq u_2$. In both cases it can be proved by a straightforward computation, the former using the doubling, the latter using the addition. □

Theorem 3.3.3. *If d is not a square in $\Bbbk$ then the group law is complete, i.e. for every two points $(x_1, y_1), (x_2, y_2)$ on the Edwards curve $x^2 + y^2 = c^2(1 + dx^2y^2)$ we have $\epsilon = dx_1y_1x_2, y_2 \notin \{+1, -1\}$.*

Proof. Suppose by contradiction that $\epsilon \in \{+1, -1\}$. We have

$$dx_1^2y_1^2(x_2^2 + y_2^2) = c^2(dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2) = c^2(1 + dx_1^2y_1^2) = x_1^2 + y_1^2$$

then

$$\begin{aligned} (x_1 + \epsilon y_1)^2 = x_1^2 + y_1^2 + 2\epsilon x_1y_1 &= dx_1^2y_1^2(x_2^2 + y_2^2) + 2dx_1^2y_1^2x_2y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) \\ &= dx_1^2y_1^2(x_2 + y_2)^2. \end{aligned}$$

If $x_2 + y_2 \neq 0$, then d is a square. In a similar way, if $x_2 - y_2 \neq 0$, then d is a square. If both $x_2 + y_2 \neq 0$ and $x_2 - y_2 \neq 0$ then $x_2 = y_2 = 0$, hence $d = 0$. In all cases we have a contradiction. □

Twisted Edwards and Montgomery curves

We define now the *Twisted Edwards curves* to be the elliptic curves defined by

$$\mathscr{E}_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

for distinct element $a, d \in \Bbbk$. The twisting map $(x, y) \mapsto (\bar{x}, \bar{y}) = (\sqrt{a}x, y)$ defined form $\mathscr{E}_{E,a,d}$ to $\mathscr{E}_{E,1,d/a}$ is an isomorphism over $\Bbbk(\sqrt{a})$, hence $\mathscr{E}_{E,a,d}$ is isomorphic to an Edwards curve if a is a square in $\Bbbk$.

A *Montgomery curve* is an elliptic curve of the form

$$\mathscr{E}_{M,A,B} : Bv^2 = u^3 + Au^2 + u$$

with $A \neq \pm 2$.

The following theorems give us a way to represent Montgomery curve with Edwards curves.

Theorem 3.3.4. *Every twisted Edwards curve over $\Bbbk$ is birationally equivalent over $\Bbbk$ to a Mongomery curve and vice versa. In particular the coefficients are $A = 2(a + b)/(a - d)$, $B = 4/(a - d)$, resp. $a = (A + 2)/B$, $b = (A - 2)/B$, and the maps are given by*

$$\begin{aligned}(x, y) \mapsto (u, v) &= ((1 + y)/(1 - y), (1 + y)/(1 - y)x),\\ (u, v) \mapsto (x, y) &= (u/v, (u - 1)/(u + 1)).\end{aligned}$$

Proof. Using the first map we have

$$\left(\frac{1+y}{1-y}\right)^3 + A\left(\frac{1+y}{1-y}\right)^2 + \left(\frac{1+y}{1-y}\right)^3 = B\left(\frac{1+y}{1-y}\right)^3 \frac{1}{x^2}$$

this is equivalent to

$$\frac{x^2}{B}\left((1 + y)^2 + A(1 - y^2) + (1 - y)^2\right) = (1 - y^2)$$

and then to

$$\frac{A+2}{B}x^2 + y^2 = 1 + \frac{A-2}{B}x^2y^2.$$

that is a twisted Edwards curve with $a = (A + 2)/B$, $b = (A - 2)/B$. The other map is clearly the inverse rational map. Moreover

$$2\frac{a+d}{a-d} = \frac{\frac{A+2}{B} + \frac{A-2}{B}}{\frac{A+2}{B} - \frac{A-2}{B}} = A, \quad \frac{4}{a-d} = \frac{4}{\frac{A+2}{B} - \frac{A-2}{B}} = B.$$

□

Proposition 3.3.5. *If $\Bbbk$ is a finite field with $\#\Bbbk \equiv 3 \pmod 4$ then every Montgomery curve $\mathscr{E}_{M,A,B} : Bv^2 = u^3 + Au^2 + u$ over $\Bbbk$ is birationally equivalent over $\Bbbk$ to an Edwards curve.*

Proof. We divide the proof in three distinct cases:

1. If $(A+2)/B$ (resp. $(A-2)/B$) is a square then the Montgomery curve has a point of order 4, namely $(1, \sqrt{(A+2)/B})$ (resp. $(-1, \sqrt{(A-2)/B})$).

2. If $(A+2)/B$ and $(A-2)/B$ are nonsquare, then $(A+2)(A-2)$ is a square. Note that, since $(A+2)/B$ is not a square, then $\mathscr{E}_{M,A,B}$ is a nontrivial quadratic twist of $\mathscr{E}_{M,A,A+2}$. Note also that $\mathscr{E}_{M,A,A+2}$ has three points of order 2, namely $(0,0), (\frac{1}{2}(-A \pm \sqrt{(A+2)(A-2)}), 0)$ and a point of order 4, namely $(1,1)$, so that $\mathscr{E}_{M,A,A+2}$ contains a subgroup isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Then $\#\mathscr{E}_{M,A,A+2} \equiv 0 \pmod 8$ and

   $$\#\mathscr{E}_{M,A,A+2} + \#\mathscr{E}_{M,A,B} = 2\#\Bbbk + 2 \equiv 0 \pmod 8.$$

   Note that the curve $\mathscr{E}_{M,A,B}$ cannot have more than three point of order 2, hence it cannot contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then it has an element of order 4.

In both cases it has an element of order 4 and then, because of Theorem 3.3.1 it is birational to an Edwards curve. □

Theorem 3.3.6. *If $\Bbbk$ is a finite field with $\#\Bbbk \equiv 1 \pmod 4$ and $\mathscr{E}_{M,A,B}$ is a Montgomery curve such that $(A+2)(A-2)$ is a square, let δ be a nonsquare in $\Bbbk$. Then exactly one of $\mathscr{E}_{M,A,B}$ and $\mathscr{E}_{M,A,\delta B}$ is birationally equivalent to an Edwards curve.*

Proof. We have $\#\mathscr{E}_{M,A,B} + \#\mathscr{E}_{M,A,\delta B} = 2\#\Bbbk + 2 \equiv 4 \mod 8$, and both $\mathscr{E}_{M,A,B}$ and $\mathscr{E}_{M,A,\delta B}$ contain a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ since $(A+2)(A-2)$ is a square in $\Bbbk$. Then exactly one of $\#\mathscr{E}_{M,A,B}$ and $\#\mathscr{E}_{M,A,\delta B}$ is divisible by 4 but not by 8. Hence exactly one has a point of order 4. □

Geometric interpretation

The sum of two points $(x_1, y_1), (x_2, y_2)$ on the twisted Edwards curves of equation $ax^2 + y^2 = 1 + dx^2y^2$ is given by

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \longmapsto \begin{pmatrix} \dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \\ \\ \dfrac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \end{pmatrix}$$

The neutral element is $O = (0,1)$; the inverse of a point (x_1, y_1) is $(-x_1, y_1)$. Denote by O' the point $(0,-1)$, it has order 2. Denote also by I_1 and I_2 the two point at infinity $[1,0,0]$ and $[0,1,0]$.

Before we start to show the explicit formulæ for addiction and doubling we describe the geometric interpretation of the addition law. Since the Edwards curves have degree 4, we cannot use the line passing through the two points that we want to add, because it leads us to find 2 other points. We use instead conics passing through three fixed points.

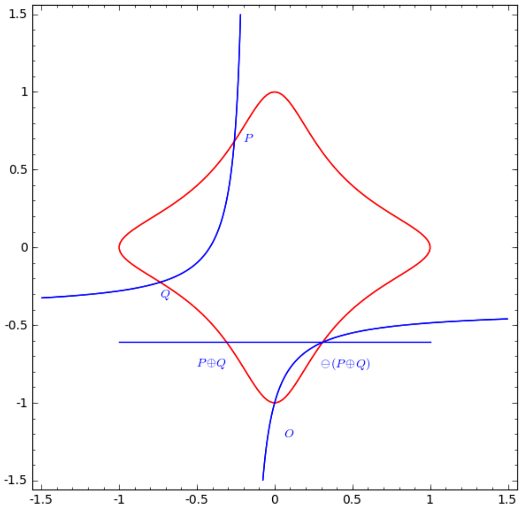

Figure 3.3: Addition law on Edwards curve

We know that a conic is uniquely determined by five points (with multiplicity) on the conic. Fix now the three points O', I_1, I_2. Evaluating a generic conic $aYZ + bXY + cXZ + dX^2 + eY^2 + fZ^2$ at O', I_1 and I_2 we see that a conic passing through these points must have the form

$$\mathscr{C} \ : \ a(Z^2 + YZ) + bXY + cXZ = 0, \tag{3.3}$$

with $[a, b, c] \in \mathbb{P}^2$. Now if we want to add P_1 and P_2 in the Edwards curve we only need to find the conic of the previous form passing through P_1 and P_2. Since the two points at infinity are singular points of multiplicity 2, the conic intersect the curve in $O' + P_1 + P_2 + 2I_1 + 2I_2 + R$, where R will be the inverse point of $P_1 \oplus P_2$. Indeed, if we call ℓ_R, ℓ_0 the two line given by $Z_RY - Y_RX$, and X, then we get

$$\begin{aligned} \operatorname{div}\left(\frac{\mathscr{C}}{\ell_R \ell}\right) &\sim (O' + P_1 + P_2 + 2I_1 + 2I_2 + R) \\ &\quad -(R + (\ominus R) - 2I_2) - (O + O' - 2I_1) \\ &\sim P_1 + P_2 - (\ominus R) - O, \end{aligned}$$

then, by the unicity of the group law with a given neutral element on an elliptic curve, we have $P_1 \oplus P_2 = \ominus R$.

The following theorem shows how to compute the equation of the conic $\mathscr{C}$.

Theorem 3.3.7. *Let $\mathscr{E}$ be the twisted Edwards curve $ax^2 + y^2 = 1 + dx^2y^2$. Let $P_1 = [X_1, Y_1, Z_1]$ and $P_2 = [X_2, Y_2, Z_2]$ be two affine points on $\mathscr{E}$. Let $\mathscr{C}$ the conic of form 3.3 passing through O', I_1, I_2, P_1 and P_2; if some of these points are equal we consider that $\mathscr{C}$ intersect $\mathscr{E}$ with at least that multiplicity at the corresponding points. Then the coefficient $[a, b, c]$ of 3.3 are determined as follows:*

- *If* $P_1 \neq P_2$ *and* $P_1, P_2 \neq O'$*, then*

$$\begin{aligned} a &= X_1X_2(Y_1Z_2 - Y_2Z_1), \\ b &= Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y_1), \\ c &= X_1X_2Z_1^2 - X_1Y_1Z_2^2 - Y_2Y_1(X_2Z_1 - X_1Z_2). \end{aligned}$$

- *If* $P_1 \neq P_2$ *and* $P_2 = O'$*, then*

$$a = -X_1, \quad b = Z_1, \quad c = Z_1.$$

- *If* $P_1 = P_2$*, then*

$$\begin{aligned} a &= X_1Z_1(Z_1 - Y_1), \\ b &= dX_1^2Y_1 - Z_1^3, \\ c &= Z_1(Z_1Y_1 - aX_1^2). \end{aligned}$$

Proof. Straightforward computations, see [Are+11]. □

Arithmetic

Now we give some explicit formulæ for the addition law on Edwards and Twisted Edwards curves in projective coordinates. The symbols **M, S, a, b,** and **c** represent the time needed by the platform to compute respectively the multiplication, the squaring, the multiplication by a, b, and c.

Arithmetic on Edwards curves

Let $\mathcal{E}$ be an Edwards curve of equation $x^2 + y^2 = c^2(1 + dx^2y^2)$.

Addition on Edwards curves. The following computes the coordinates of the point $[X_3, Y_3, Z_3] = [X_1, Y_1, Z_1] \oplus [X_2, Y_2, Z_2]$:

$$A = Z_1 \cdot Z_2; \quad B = A^2; \quad C = X_1 \cdot X_2; \quad D = Y_1 \cdot Y_2;$$

$$E = d \cdot C \cdot D; \quad F = B - E; \quad G = B + E;$$

$$X_3 = A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D);$$

$$Y_3 = A \cdot G \cdot (D - C); \quad Z_3 = c \cdot F \cdot G.$$

It takes 10**M** + **S** + **c** + **b**. If the platform computes squaring much faster that multiplication, say **S**/**M**< 3/4, we can compute $A(B - E), A(B + E)$ and $(B - E)(B + E)$ as linear combination of $A^2, B^2, E^2, (A + B)^2, (A + E)^2$; this replaces 10**M** + **S** by 7**M** + 5**S**.

Doubling on Edwards curve. In order to compute the doubling we can rewrite $c(1+dx_1^2y_1^2)$ as $(x_1^2+y_1^2)/c$, $c(1-dx_1^2y_1^2)$ as $(2c^2-(x_1^2+y_1^2))/c$, and $2x_1y_1$ as $(x_1+y_1)^2-x_1^2-y_1^2$, then we have

$$\begin{aligned} 2(x_1,y_1) &= \left(\frac{2x_1y_1}{c(1+dx_1^2y_1^2)}, \frac{y_1^2-x_1^2}{c(1-dx_1^2y_1^2)}\right) \\ &= \left(\frac{2cx_1y_1}{(x_1^2+y_1^2)}, \frac{c(y_1^{-}2x_1^2)}{.}2c^2-(x_1^2+y_1^2)\right) \end{aligned}$$

We can write the explicit algorithm that computes $[X_3,Y_3,Z_3]=2[X_1,Y_1,Z_1]$:

$$B=(X_1+Y_1)^2\,; \quad C=X_1^2; \quad D=Y_1^2;$$
$$E=C+D; \quad H=(c\cdot Z_1)^2; \quad J=E-2H;$$
$$X_3=c\cdot(B-E)\cdot J; \quad Y_3=c\cdot E\cdot(C-D); \quad Z_3=E\cdot J.$$

It uses only 3**M** + 4**S** + 3**c**.

Arithmetic on Twisted Edwards curves

Let $\mathcal{E}_{E,a,d}$ be a twisted Edwards curve of equation $ax^2+y^2=1+dx^2y^2$.

Addition in Twisted Edward curves. The following computes the sum $[X_3,Y_3,Z_3]=[X_1,Y_1,Z_1]\oplus[X_2,Y_2,Z_2]$:

$$A=Z_1\cdot Z_2; \quad B=A^2; \quad C=X_1\cdot X_2; \quad D=Y_1\cdot Y_2;$$
$$E=d\cdot C\cdot D; \quad F=B-E; \quad G=B+E;$$
$$X_3=A\cdot F\cdot((X_1+Y_1)\cdot(X_2+Y_2)-C-D)\,;$$
$$Y_3=A\cdot G\cdot(D-a\cdot C)\,; \quad Z_3=F\cdot G.$$

It uses 10**M** + **S** + **a** + **d**.

Doubling in Twisted Edward curves. The following computes the sum $[X_3,Y_3,Z_3]=2[X_1,Y_1,Z_1]$:

$$B=(X_1+Y_1)^2\,; \quad C=X_1^2; \quad D=Y_1^2;$$
$$E=a\cdot C; \quad F=E+D; \quad H=Z_1^2; \quad J=F-2H;$$
$$X_3=(B-C-D)\cdot J; \quad Y_3=F\cdot(E-D); \quad Z_3=F\cdot J.$$

It takes 3**M** + 4**S** + **a**.

Inverted coordinates

In inverted coordinates a point $[X_1, Y_1, Z_1]$ on the curve

$$(X^2 + aY_2)Z^2 = X^2Y^2 + dZ^4$$

corresponds to the affine point $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve $\mathscr{E}_{E,a,d}$.

Addition in Inverted Twisted Coordinates. The following computes $[X_3, Y_3, Z_3] = [X_1, Y_1, Z_1] \oplus [X_2, Y_2, Z_2]$:

$$A = Z_1 \cdot Z_2; \quad B = d \cdot A^2;$$

$$C = X_1 \cdot X_2; \quad D = Y_1 \cdot Y_2; \quad E = C \cdot D;$$

$$H = C - aD; \quad I = ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D)$$

$$X_3 = (E + B) \cdot H; \quad Y_3 = (E - B) \cdot I; \quad Z_3 = A \cdot H \cdot I.$$

It takes 9**M** + **S** + **a** + **d**.

Doubling in Inverted Twisted Coordinates. The following compute $[X_3, Y_3, Z_3] = 2[X_1, Y_1, Z_1]$:

$$A = X_1^2; \quad B = Y_1^2; \quad U = a \cdot B;$$

$$C = A + U; \quad D = A - U; \quad E = (X_1 + Y_1)^2 - A - B;$$

$$X_3 = C \cdot D; \quad Y_3 = E \cdot (C - 2d \cdot Z_1^2); \quad Z_3 = D \cdot E.$$

It need 3**M** + 4**S** + **a** + **d**.

Chapter 4

Arithmetic on Hyperelliptic curves of genus bigger than 1

The aim of this chapter is to explain how to compute the addition law on Jacobians of hyperelliptic curve of genus g. In the first section we give the notions of semi-reduced and reduced divisor, and in the second section we present the Cantor algorithm. This notions can be slightly modified in order to be adapted for superelliptic curves and also for algebraic curves in general, as we will see in chapter 5 and 6. In the third section we describe the Cantor Algorithm from a geometrical point of view and, in the last section, we describe a faster way to compute the addition law for hyperelliptic curves of genus 2.

We mainly refer to [Men+96] and [Lan05]

4.1 Reduced divisors

Let $\mathscr{C}$ be an hyperelliptic curve of genus g (with at least one $\mathbb{k}$-rational point) given by

$$y^2 + h(x)y = f(x),$$

with $\deg(f) = 2g + 1$. We denote by ι its canonical involution that send (a, b) to $(a, -b - h(a))$, and by P_∞ its unique point at infinity.
We say that a divisor $\mathcal{D}$ of $\mathscr{C}$ is *semi-reduced* if it is of the form

$$\mathcal{D} = \sum_{i=1}^{k} m_i P_i - (\sum_{i=1}^{k} m_i) P_\infty$$

where $m_i \geq 0$, and moreover $P_i \in supp(\mathcal{D})$ and $\iota(P_i) \in supp(\mathcal{D})$ implies $P_i = \iota(P_i)$ and $m_i = 1$.

We shall show that on hyperelliptic curves each divisor class can be represented by a unique semi-reduced divisor if $k \leq g$.

Lemma 4.1.1. *Every divisor in* $\mathrm{Pic}^0_{\mathscr{C}}$ *can be represented by a semi-reduced divisor*

Proof. Let $\mathcal{D} = \sum m_P P$ be a divisor of degree 0. Let (C_0, C_1, C_2) be a partition of the point in the curve where C_0 contains the Weierstrass points, i.e. the points Q

such that $\iota(Q) = Q$, $P \in C_1$ if and only if $\iota(P) \in C_1$, if $P \in C_1$ then $m_P \geq m_{\iota(P)}$. Then we can write

$$\mathcal{D} = \sum_{P \in C_0} m_P P + \sum_{P \in C_1} m_P P + \sum_{P \in C_2} m_P P + m_{P_\infty} P_\infty.$$

Consider now the following divisor

$$\mathcal{D}_1 = \mathcal{D} - \sum_{P \in C_2} m_P \mathrm{div}(x - a_P) - \sum_{P \in C_0} \left\lfloor \frac{m_P}{2} \right\rfloor \mathrm{div}(x - a_P)$$

then $\mathcal{D}_1 \sim \mathcal{D}$ and

$$\mathcal{D}_1 = \sum_{P \in C_1} (m_P - m_{\iota(P)})P + \sum_{P \in C_1} (m_P - \left\lfloor \frac{m_P}{2} \right\rfloor)P - kP_\infty.$$

The lemma is proved. □

Lemma 4.1.2. *Let $P = (a, b)$ be a point on $\mathscr{C}$ such that $\iota(P) \neq P$. Let $\phi \in \overline{\Bbbk}(\mathscr{C})$ be a rational function which doesn't have pole at P. Then for any $k \geq 0$, there exist unique constants $c_0, \cdots, c_k \in \overline{\Bbbk}$, and $\phi_k \in \overline{\Bbbk}(\mathscr{C})$ such that*

$$\phi = \sum_{i=0}^{k} c_i (x - a)^i + (x - a)^{k+1} \phi_k,$$

where ϕ_k doesn't have a pole at P.

Proof. Take $c_0 = \phi(a, b)$, since $(x - a)$ is a uniforming parameter for P, we can write $\phi = c_0 + (x - a)\phi_1$. The lemma follows by induction. □

Lemma 4.1.3. *Let $P = (a, b)$ be a point on $\mathscr{C}$ such that $\iota(P) \neq P$. Then for each $k \geq 1$ there exists a unique polynomial $\psi_k(x) \in \overline{\Bbbk}[x]$ such that*
(a) $\deg \psi_k < k$;
(b) $\psi_k(a) = b$;
(c) $\psi_k^2(x) + \psi_k(x)h(x) \equiv f(x) \mod (x - a)^k$.

Proof. By the previous lemma write $y = \sum_{i=0}^{k-1} c_i (x - a)^i + (x - a)^k \phi_{k-1}$. Define $\psi_k(x) = \sum_{i=0}^{k} c_i (x - a)^i$. We know that $c_0 = b$, hence $\psi_k(a) = b$ holds. Since $b^2 + h(a)b = f(a)$, we can reduce both sides modulo $(x - a)^k$ and obtain $\psi_k^2(x) + \psi_k(x)h(x) \equiv f(x) \mod (x - a)^k$. The uniqueness can be proved easily by induction. □

Theorem 4.1.4. *Let $\mathcal{D} = \sum_{i=1}^{k} m_i P_i - (\sum_{i=1}^{k} m_i)P_\infty$ be a semi-reduced divisor, with $P_i = (a_i, b_i)$. Let $u(x) = \prod (x - a_i)^{m_i}$. There exists a unique polynomial $v(x)$ satisfying:*
(a) $\deg v < \deg u$*;*
(b) $v(a_i) = b_i$ for all i such that $m_i \neq 0$;
(c) $u(x) | (v(x)^2 + v(x)h(x) - f(x))$.
Moreover

$$\mathcal{D} = \gcd(\mathrm{div}(u(x)), \mathrm{div}(v(x) - y)),$$

where $\gcd(\sum s_P P, \sum r_P P) = \sum \min(s_P, r_P)P$ *(we will denote* $\gcd(\mathrm{div}(f), \mathrm{div}(g))$ *by* $\mathrm{div}(f, g)$*).*

Proof. Let (C_0, C_1) be the partition of *supp*$(\mathcal{D})$ such that C_0 contains the points with $\iota(P) = P$ and C_1 the other ones. Let $C_2 = \{\iota(P) \mid P \in C_1\}$. We can write

$$\mathcal{D} = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - m_\infty P_\infty.$$

For every $P_i \in C_1$ there exist polynomials $\psi_i(x) \in \overline{\mathbb{k}}[x]$ satisfying the condition of the previous lemma. For each $P_i \in C_0$ set $\psi_i(x) = b_i$. By the Chinese Remainder Theorem, there is a unique polynomial $v(x) \in \overline{\mathbb{k}}[x]$, with $\deg(v) < \sum m_i$, such that

$$v(x) \equiv \psi_i(x) \mod (x - a_i)^{m_i}, \quad \text{for all } i.$$

Moreover,

$$\operatorname{div}(u(x)) = 2 \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \iota(P_i) - \left(2 \sum m_i\right) P_\infty$$

and

$$\operatorname{div}(v(x) - y) = \sum_{P_i \in C_0} t_i P_i + \sum_{P_i \in C_1} s_i P_i + \sum_{P_i \in C} r_i \iota(P_i) - \left(\sum (t_i + s_i + r_i)\right) P_\infty,$$

where $C = \mathscr{C} \setminus (C_0 \cup C_1 \cup C_2 \cup \{P_\infty\})$. We have that each $s_i \geq m_i$, because $(x - a_i)^{m_i}$ divides $v^2 + hv - f = (v(x) - y)(v(x) + h(x) + y)$. For each $P_i \in C_0$ we have that the element a_i is a single root of $v(x)^2 + v(x)h(x) - f(x)$, therefore $t_i = 1$ for all i. Hence

$$\gcd\left(\operatorname{div}(u(x)), \operatorname{div}(v(x) - y)\right) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \iota(P_i) - m P_\infty.$$

So $\operatorname{div}(u, v - y) = \mathcal{D}$ and this proves the theorem. □

The converse is also true

Corollary 4.1.5. *Let* $\mu(x), \nu(x) \in \overline{\mathbb{k}}[x]$ *be two polynomials such that* $\deg \nu < \deg \mu$ *and* $\mu \mid (\nu^2 + \nu h - f)$ *then div*$(\mu, \nu - y)$ *is semi-reduced.*

Let $\mathcal{D} = \sum_{i=1}^k m_i P_i - \left(\sum_{i=1}^k m_i\right) P_\infty$ be a semi-reduced divisor. We say that it is a *reduced* divisor if $\sum_{i=1}^k m_i < g$.

Theorem 4.1.6. *Each divisor* $\mathcal{D} \in \operatorname{Pic}^0_{\mathscr{C}}$ *can be represented by a reduced divisor in a unique way.*

Proof. Note that if we use the construction of the semi-reduced divisor given by the lemma 4.1.1 we obtain a divisor $\mathcal{D}_1$ with $N(\mathcal{D}_1) \leq N(\mathcal{D})$, where N is the norm $N(\mathcal{D}) = \sum_{P \in \mathscr{C} \setminus \{P_\infty\}} |m_P|$. Now, if $N(\mathcal{D}_1) \leq g$ then we are done, otherwise pick $g + 1$ points in *supp*$(\mathcal{D}_1)$, say $P_1, \cdots, P_{g+1}$ (the point P cannot occur in this list more than $\operatorname{ord}_P(\mathcal{D}_1)$ times). Let $\operatorname{div}(u, v - y)$ be a representation of the divisor $\mathcal{D}_1' = P_1 + \cdots + P_{g+1} - (g+1)P_\infty$, since $\deg(v) \leq g$ we have $\deg(v(x) - y) = 2g + 1$, hence

$$\operatorname{div}(v(x) - y) = P_1 + \cdots + P_{g+1} + Q_1 + \cdots + Q_g - (2g + 1)P_\infty$$

for some points $Q_1, \cdots, Q_g$. Subtracting this divisor from D_1, it gives a divisor $\mathcal{D}_2 \sim \mathcal{D}_1 \sim \mathcal{D}$ with $N(D_2) < N(D_1)$. We can repeat this operation obtaining divisors $\mathcal{D}_3, \cdots, \mathcal{D}_k$ unless $N(\mathcal{D}_k) \leq g$.

For the uniqueness, suppose that $\mathcal{D}_1$ and $\mathcal{D}_2$ are two reduced divisor such that $\mathcal{D}_1 \sim \mathcal{D}_2$ and $\mathcal{D}_1 \neq \mathcal{D}_2$. Let D_3 be the semi-reduced divisor $\mathcal{D}_3 \sim \mathcal{D}_1 - \mathcal{D}_2$ obtained using Lemma 4.1.1. The divisor $\mathcal{D}_3$ is principal (since $\mathcal{D}_1 \sim \mathcal{D}_2$) and non zero (since $\mathcal{D}_1 \neq \mathcal{D}_2$). Since it is semi-reduced the corresponding function ϕ has no affine poles, then $\mathcal{D}_3 = \mathrm{div}(\phi)$ with ϕ polynomial function, i.e. $\phi = f(x) - g(x)y$ for some $f, g \in \overline{\mathbb{k}}[x]$. Since $\deg(\phi) = N(\mathcal{D}_3) \leq N(\mathcal{D}_1 - \mathcal{D}_2) \leq N(\mathcal{D}_1) + N(\mathcal{D}_2) \leq 2g$ and $\deg(y) = 2g+1$ we must have $g(x) = 0$. Hence $\phi = f(x)$, then $\mathcal{D}_3$ is of the form $\sum m_P(P + \iota(P)) - (2\sum m_P)P_\infty$, contradicting the fact that $\mathcal{D}_3$ is semi-reduced. □

We proved also that the Jacobian $\mathscr{J}_{\mathscr{C}}(\overline{K})$ is in bijection with the set of reduced divisor of the hyperelliptic curve $\mathscr{C}$. This is also true for any hyperelliptic curves over a perfect field $\mathbb{k}$.

4.2 Mumford representation and Cantor algorithm

Summing up we have the so called *Mumford representation*:

Proposition-Definition 4.2.1. *Each nontrivial ideal class over $\mathbb{k}$ can be represented via a unique ideal generated by $u(x)$ and $y - v(x)$, $u, v \in \mathbb{k}[x]$, where*
(a) u is monic,
(b) $\deg v < \deg u \leq g$,
(c) $u \mid v^2 + vh - f$.
Let $\mathcal{D} = \sum_{i=1}^r P_i - rP_\infty$ be a reduced divisor. Put $P_i = (a_i, b_i)$, then the corresponding ideal class is represented by $u = \prod_{i=1}^r (x - a_i)$ and if $\mathrm{ord}_{P_i}(\mathcal{D}) = m_i$ then $\left(\frac{d}{dx}\right)^j [v(x)^2 + v(x)h(x) - f(x)]_{|x=a_i} = 0$ for $0 \leq j < m_i$.

For brevity we denote the points in $\mathscr{J}_{\mathscr{C}}$ by $[u, v]$. The inverse is represented by $[u, -h - v]$, (where the second polynomial is understood modulo u if necessary). The zero element $\mathscr{J}_{\mathscr{C}}$ is represented by $[1, 0]$.

Fix two reduced divisors $\mathcal{D}_1$ and $\mathcal{D}_2$. Now we present two algorithms:
the first one finds a semi-reduced divisor $\mathcal{D} \sim \mathcal{D}_1 + \mathcal{D}_2$;
the second one finds the reduced divisor $\mathcal{D}' \sim \mathcal{D}$.

Algorithm 1.

INPUT: *Reduced divisors $\mathcal{D}_1 = [u_1, v_1]$ and $\mathcal{D}_2 = [u_2, v_2]$ of $\mathscr{C}_{\mathbb{k}}$.*

OUTPUT: *A semi-reduced divisor $\mathcal{D} = [u, v]$ such that $\mathcal{D} \sim \mathcal{D}_1 + \mathcal{D}_2$.*

1. *Use the extended Euclidean algorithm to find three polynomials d_1, e_1, $e_2 \in \mathbb{k}[x]$ such that $d_1 = e_1u_1 + e_2u_2$.*

2. *Use the extended Euclidean algorithm to find three polynomials d, c_1, $c_2 \in \Bbbk[x]$ such that $d = c_1 d_1 + c_2(v_1 + v_2 + h)$.*

3. *Let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$, so that*

$$d = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h).$$

4. *Set*

$$u = \frac{u_1 u_2}{d^2}$$

and

$$v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \mod u.$$

Algorithm 2.

INPUT: *A semi-reduced divisor $\mathcal{D} = [u, v]$;*

OUTPUT: *The reduced divisor $\mathcal{D}' = [u', v']$ such that $\mathcal{D}' \sim \mathcal{D}$.*

1. *Set*

$$u' = (f - vh - v^2)/u$$

and

$$v' = (-h - v) \mod u'$$

2. *If $\deg u' > g$ then set $u \leftarrow u'$ and $v \leftarrow v'$and go to step 1.*

3. *Otherwise make u' monic, i.e. put $u' \leftarrow a^{-1}u'$, where a is the leading coefficient of u'. Return $[u', v']$.*

Theorem 4.2.2. *The Algorithm 1 works.*

Proof. First prove that v is indeed a polynomial. We have

$$\begin{aligned} v &= \frac{v_2(d - s_2 u_2 - s_3(v_1 + v_2 + h)) + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \\ &= v_2 + \frac{s_2 u_2(v_1 - v_2) - s_3(v_2^2 + v_2 h - f)}{d}. \end{aligned}$$

Since $d|u_2$ and $u_2|(v_2^2 + b_2 h - f)$, v is a polynomial.

We can write

$$\begin{aligned} v - y &= \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f) - dy}{d} \mod a \\ &= \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} + \\ &\qquad \frac{-s_1 u_1 y + s_2 u_2 y + s_3(v_1 + v_2 + h)y}{d} \mod a \\ &= \frac{s_1 u_1(v_2 - y) + s_2 u_2(v_1 - y) + s_3(v_1 - y)(v_2 - y)}{d} \mod a. \quad (4.1) \end{aligned}$$

To prove that $u|(v^2 + vh - f)$ it suffices to show that $u_1 u_2$ divides the product of $s_1 u_1(v_2 - y) + s_2 u_2(v_1 - y) + s_3(v_1 - y)(v_2 - y)$ by its conjugate. This follows because

$u_1|(v_1^2+v_1h-f) = (v_1-y)(v_1+y+h)$ and $u_2|(v_2^2+v_2h-f) = (v_2-y)(v_2+y+h)$. Then, by Corollary 4.1.5, $[u, v]$ is a semi-reduced divisor.

We need to prove now that $\mathcal{D} \sim \mathcal{D}_1 + \mathcal{D}_2$. First we remark that

$$m(P) + n(\iota P) \sim (m-n)P + 2nP_\infty$$

using the polynomial function $x - x_P$.
Now we consider two different cases:

1. Let $P = (x_P, y_P)$ an ordinary point. And consider the two subcases:

   (a) Suppose that

   $$\mathrm{ord}_P(\mathcal{D}_1) = m_1, \qquad \mathrm{ord}_{\iota(P)}(\mathcal{D}_1) = 0$$
   $$\mathrm{ord}_P(\mathcal{D}_2) = m_2, \qquad \mathrm{ord}_{\iota(P)}(\mathcal{D}_2) = 0.$$

   Then

   $$\mathrm{ord}_P(u_1) = m_1, \qquad \mathrm{ord}_P(u_2) = m_2,$$
   $$\mathrm{ord}_P(v_1 - y) \geq m_1, \qquad \mathrm{ord}_P(v_2 - y) \geq m_2.$$

   If $m_1 = 0$ or $m_2 = 0$ then $\mathrm{ord}_P(d_1) = 0$, hence $\mathrm{ord}_P(d) = 0$ and $\mathrm{ord}_P(u) = m_1 + m_2$.
   If $m_1 \geq 1$ and $m_2 \geq 1$, then $\mathrm{ord}_P(d) = 0$ and $\mathrm{ord}_P(u) = m_1 + m_2$, because $(v_1 + v_2 + h)(x_P) = 2y_P + h(x_P) \geq 0$.
   From 4.1 it follows that $\mathrm{ord}_P(v - y) \geq m_1 + m_2$, hence we have $\mathrm{ord}_P(\mathcal{D}) = m_1 + m_2$.

   (b) Suppose now that

   $$\mathrm{ord}_P(\mathcal{D}_1) = m_1, \quad \mathrm{ord}_\iota(P)(\mathcal{D}_2) = m_2,$$

   with $m_1, m_2 > 0$. Then

   $$\mathrm{ord}_P(u_1) = m_1, \quad \mathrm{ord}_P(u_2) = m_2, \quad \mathrm{ord}_P(d_1) = m_2,$$
   $$\mathrm{ord}_P(v_1 - y) \geq m_1, \quad \mathrm{ord}_P(v_2 - y) = 0, \quad \mathrm{ord}_{\iota(P)}(v_2 - y) \geq m_2.$$

   This implies that $\mathrm{ord}_P(v_2 + h + y) \geq m_2$, hence $\mathrm{ord}_P(v_1 + v_2 + h) \geq m_2$ or $(v_1 + v_2 + h) = 0$. Then $\mathrm{ord}_P(d) = 0$ and $\mathrm{ord}_P(u) = m_1 - m_2$.
   From 4.1 it follows that $\mathrm{ord}_P(v - y) \geq m_1 - m_2$, hence we have $\mathrm{ord}_P(\mathcal{D}) = m_1 - m_2$.

2. Let now P be a Weierstrass point. There are two other subcases:

   (a) Suppose that

   $$\mathrm{ord}_P(\mathcal{D}_1) = \mathrm{ord}_P(\mathcal{D}_2) = 1.$$

   Then

   $$\mathrm{ord}_P(u_1) = 2, \quad \mathrm{ord}_P(u_2) = 2, \quad \mathrm{ord}_P(d_1) = 2.$$

   Now we have $(v_1 + v_2 + h)(x_P) = 2y_P + h(x_P) = 0$, hence either $\mathrm{ord}_P(v_1 + v_2 + h) \geq 2$ or $(v_1 + v_2 + h) = 0$. It follows that $\mathrm{ord}_P(d) = 2$ and $\mathrm{ord}_P(u) = 0$, hence $\mathrm{ord}_P(\mathcal{D}) = 0$.

(b) Suppose that

$$\mathrm{ord}_P(\mathcal{D}_1) = 1, \qquad \mathrm{ord}_P(\mathcal{D}_2) = 0.$$

Then

$$\mathrm{ord}_P(u_1) = 2, \quad \mathrm{ord}_P(u_2) = 0,$$

$$\mathrm{ord}_P(d_1) = 0, \quad \mathrm{ord}_P(d) = 0, \quad \mathrm{ord}_P(u) = 2.$$

Since $\mathrm{ord}_P(v_1 - y) = 1$, then by 4.1 we get $\mathrm{ord}_P(v - y) \geq 1$. Since the divisor $\mathcal{D}$ is semi-reduced we have $\mathrm{ord}_P(v - y) = 1$ and $\mathrm{ord}_P(\mathcal{D}) = 1$.

Using the first remark we proved the correctness of the first algorithm. □

Theorem 4.2.3. *The Algorithm 2 works.*

Proof. We shall show that after the step 1 we have:

1. $\deg(u') < \deg(u)$;
2. $\mathcal{D}' = [u', v']$ is semi-reduced;
3. $\mathcal{D}' \sim \mathcal{D}$.

We shall prove it step by step:

1. Let $m = \deg u$, and $n = \deg v$, where $m > n$ and $m \geq g + 1$. Then $\deg u' = \max(2g + 1, 2n) - m$.
   If $m > g+1$, then $\max(2g+1, 2n) \leq 2(m-1)$, hence $\deg u' \leq m-2 < \deg u$.
   If $m = g + 1$, then $\max(2g + 1, 2n) = 2g + 1$, hence $\deg u' = g < \deg u$.

2. We have that $f - vh - v^2 = uu'$. Then

   $$f + (v' + h)h - (v' + h)^2 = 0 \mod u'$$

   hence

   $$f - v'h - v'^2 = 0 \mod u'.$$

   This implies that $u'|(f - v'h - v'^2)$. Then, by Corollary 4.1.5, $[u', v']$ is semi-reduced.

3. As we use in the previous proofs, let C_0 be the set of the Weierstrass points in *supp*$(\mathcal{D})$, let C_1 be the set of ordinary points in *supp*$(\mathcal{D})$, and finally let $C_2 = \{\iota(P) : P \in C_1\}$. Then we can write

   $$\mathcal{D} = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - m_\infty P_\infty.$$

   We have

   $$\mathrm{div}(u) = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} m_i(P_i + \iota(P_i)) - 2m_\infty P_\infty$$

and

$$\operatorname{div}(v-y)=\sum_{P_i\in C_0}P_i+\sum_{P_i\in C_1}n_iP_i+\sum_{P_i\in C}0\iota(P_i)+\sum_{P_i\in C}s_iP_i-(*)P_\infty,$$

where $C=\mathscr{C}\setminus(C_0\cup C_1\cup C_2\cup\{P_\infty\}$, $n_i\geq m_i$, $s_i\geq 1$, and $s_i=1$ if P_i is a Weierstrass point. Since $(v^2+vh-f)=(v-y)(v+y+h)$ it follows that

$$\operatorname{div}(v^2+vh-f)=\sum_{P_i\in C_0}2P_i+\sum_{P_i\in C_1}n_i(P_i+\iota(P_i))+\sum_{P_i\in C}s_i(P_i+\iota(P_i))-(*)P_\infty,$$

hence

$$\begin{array}{rcl}\operatorname{div}(u') & = & \operatorname{div}(v^2+vh-f)-\operatorname{div}(u)\\ & = & \displaystyle\sum_{P_i\in C_1'}t_i(P_i+\iota(P_i))+\sum_{P_i\in C}s_i(P_i+\iota(P_i))-(*)P_\infty,\end{array}$$

where $t_i=n_i-m_i$ and $C_1'=\{P\in C_1\mid t_i>0\}$.
If $P_i=(a_i,b_i)\in C_1'\cup C$, then

$$v'(a_i)=-h(a_i)-v(a_i)=-h(a_i)-y_i\mod u'.$$

We have

$$\operatorname{div}(v'-y)=\sum_{P_i\in C_1'}r_i\iota(P_i)+\sum_{P_i\in C}w_i\iota(P_i)+\sum_{P_i\in C_3}z_iP_i-(*)P_\infty,$$

where $r_i\geq t_i$, $w_i\geq s_i$, $w_i=1$ if P_i is a Weierstrass point, and C_3 is the set $\mathscr{C}\setminus C_1'\cup C\cup\{P_\infty\}$. Finally

$$\begin{array}{rcl}\operatorname{div}(u',v'-y) & = & \displaystyle\sum_{P_i\in C_1'}t_i\iota(P_i)+\sum_{P_i\in C}s_i\iota(P_i)-(*)P_\infty\\ & \sim & \displaystyle-\sum_{P_i\in C_1'}t_iP_i-\sum_{P_i\in C}s_iP_i+(*)P_\infty\\ & = & \mathcal{D}-\operatorname{div}(v-y),\end{array}$$

therefore $\mathcal{D}\sim\mathcal{D}'$.

□

4.3 Geometric interpretation

Starting from a hyperelliptic curve $\mathscr{E}:y^2+h(x)y=f(x)$ of genus $g\geq 2$, over an algebraic closed field, we can describe the geometric interpretation of the two algorithms. Suppose now that we want to add two reduced divisors of the form $\mathcal{D}_1=\sum_{i=1}^k m_iP_i-(\sum_{i=1}^k m_i)P_\infty$ and $\mathcal{D}_2=\sum_{j=1}^k n_jP_j-(\sum_{j=1}^k n_j)P_\infty$. Suppose that $P_i\neq\iota(P_j)$ for each i and j (if not we can eliminate the couples from $\mathcal{D}_1+\mathcal{D}_2$, indeed the complete system do not change). We can interpreter the algorithm in such a way: find the function t that interpolates the points P_i and P_j with the

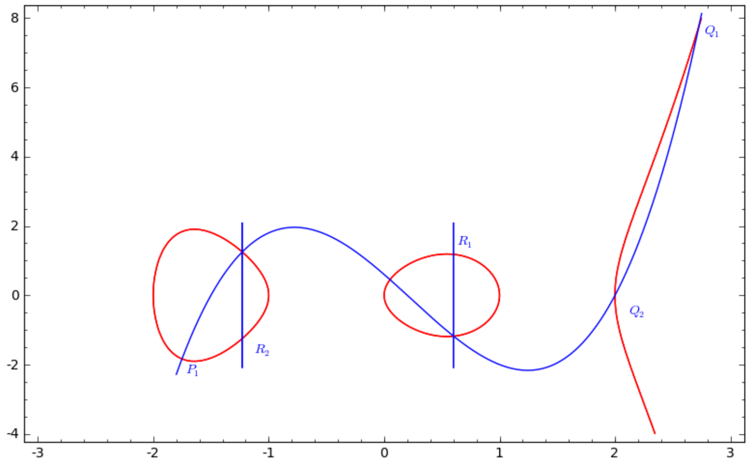

Figure 4.1: Addition law on hyperelliptic curves of genus 2

respective multiplicities, i.e if the multiplicity is bigger that 1 on a point Q then the derivative of t and $\mathscr{E}$ evaluated in Q are the same. In general t is a polynomial of degree $2g-1$ (or less). Now the divisor $\operatorname{div}(t) = \mathcal{D}_1+\mathcal{D}_2+\mathcal{E}$, then $\mathcal{D}_1+\mathcal{D}_2 \sim -\mathcal{E}$. The figure 4.3 represent the addition on an hyperelliptic curve of genus 2. Note that in the figure the divisor $-\mathcal{E} = R_1 + R_2$ is already reduced. But this is not the case for higher genus. In fact, the Bézout Theorem says that the number of (projective) points of intersection (with multiplicities) of two plane curve is the product of their degrees, then, computing the multiplicity of the intersection of t and $\mathscr{E}$ in P_∞, we can find the number of points of intersection in the affine plane. In order to do this we only care on terms of higher degree in t and $\mathscr{E}$, then we can suppose that the functions are $t' : y = x^k$ and $\mathscr{E}' : y^2 = x^{2g+1}$. Passing to the projective coordinate and using the affinization respect the variable y, we can look at the function $t'' : z^{k-1} = x^k$ and $\mathscr{E}'' : z^{2g-1} = x^{2g+1}$. Using the definition of multiplicity of intersection we can compute

$$m_{P_\infty}(t, \mathscr{E}) = \min\{(2g+1)(k-1), (2g-1)k\}.$$

Remark. Computing the multiplicity with the definition could take more than a while. Note that in this case we can avoid it using the idea of Algorithm 2. Indeed the number of affine point is $\deg(f - th - t^2) = \max\{2g+1, 2k\}$, then the multiplicity at infinity is $(2g+1)k - \deg(f - th - t^2) = \min\{(2g+1)(k-1), (2g-1)k\}$.

Now, assuming that we are in the most common case in which $k = 2g-1$, then $m_{P_\infty}(t, \mathscr{E}) = (2g-1)^2$ and the total points of intersection in the affine plane are $(2g-1)(2g+1) - (2g-1)^2 = 4g-2$. The divisor $\mathcal{D}_1 + \mathcal{D}_2$ has already $2g$ points in the affine plane, hence the divisor $\mathcal{E}$ has $2g-2$ finite points. So only for $g = 2$ it is already reduced.

If the divisor $\mathcal{E}$ is not reduced than we can do it again using the affine point of $\mathcal{E}$ instead of the affine points of $\mathcal{D}_1 + \mathcal{D}_2$, and find others divisors $\mathcal{E}_2, \mathcal{E}_3, \cdots$ until the affine points of $\mathcal{E}_k$ are less than g.

Here are some examples:

- genus 2. After the first iteration $\mathcal{E}$ has 2 affine points. So the divisor $\mathcal{E}$ is reduced
- genus 3. After the first iteration $\mathcal{E}$ has 4 affine points, hence another iteration is necessary. Now let t_2 the polynomial that interpolates these 4 points, it has degree 3. Then

  $$\deg(t_2)\deg(\mathscr{E}) - 4 - m_{P_\infty}(t_2, \mathscr{E}) = 3 \cdot 7 - 4 - 14 = 3 = g.$$

  Hence the divisor $\mathscr{E}_2$ is reduced.
- genus 4. After the first iteration $\mathcal{E}$ has $6 > g$ affine points. Now let t_2 the polynomial that interpolates these 6 points, it has degree 5. Then

  $$\deg(t_2)\deg(\mathscr{E}) - 6 - m_{P_\infty}(t_2, \mathscr{E}) = 5 \cdot 9 - 6 - 35 = 4 = g.$$

  Hence the divisor $\mathscr{E}_2$ is reduced.
- genus 5. After the first iteration $\mathcal{E}$ has $8 > g$ affine points. Now let t_2 the polynomial that interpolates these 8 points, it has degree 7. Then

  $$\deg(t_2)\deg(\mathscr{E}) - 8 - m_{P_\infty}(t_2, \mathscr{E}) = 7 \cdot 11 - 8 - 63 = 6 > g.$$

  Hence the divisor $\mathscr{E}_2$ is not reduced yet. Let t_3 the polynomial that interpolates these last 6 points, it has degree 5. Then

  $$\deg(t_3)\deg(\mathscr{E}) - 6 - m_{P_\infty}(t_3, \mathscr{E}) = 5 \cdot 11 - 6 - 44 = 5 = g.$$

  Hence the divisor $\mathscr{E}_3$ is reduced.

We can also prove that the number of iteration required are $\lceil \frac{g}{2} \rceil$.

4.4 Explicit formulæ on genus 2

Here we present how to compute explicitly the addition and the doubling on hyperelliptic curves of genus 2. As we already said in this case it suffices to only do one iteration of the reduction step, moreover we can describe quickly all the types of the possible couples of divisors that can occur in the addition. Suppose that we want to add $\mathcal{D}_1 = [u_1, v_1]$ and $\mathcal{D}_2 = [u_2, v_2]$, then we can distinguish the possible cases according to the degree of u_1 and u_2.

1. If $\deg u_1 = 0$, then $\mathcal{D}_1 = [1, 0]$ is the neutral element. Hence $\mathcal{D}_1 + \mathcal{D}_2 = \mathcal{D}_2$.
2. If $\deg u_1 = \deg u_2 = 1$, then we can write $\mathcal{D}_1 = P_1 - P_\infty$ and $\mathcal{D}_1 = P_2 - P_\infty$.
   If $P_1 = \iota P_2$ then $\mathcal{D}_1 + \mathcal{D}_2 = [1, 0]$, the neutral element.
   If $P_1 \neq \iota P_2$ then $\mathcal{D}_1 + \mathcal{D}_2 = P_1 + P_2 - 2P_\infty$, in particular we can compute the function u and v as follow

a) If $P_1 = P_2$, hence $[u_1, v_1] = [u_2, v_2]$, then we put

$$u = u_1^2, \quad v = ((f'(x_P) - v_1 h'(x_P))x + \frac{f'(x_P) + v_1 h'(x_P) x_P}{2v_1 + h(x_P)} + v_1.$$

b) If $P_1 \neq P_2$ we can put

$$u = u_1 u_2, \quad v = \frac{(v_2 - v_1)x + v_2 x_{P_1} - v_1 x_{P_2}}{x_{P_1} - x_{P_2}}.$$

In both cases the divisors are already reduced.

3. If $\deg u_1 = 1$ and $\deg u_2 = 2$, say $u_1 = x + x_{10}$ and $u_2 = x^2 + u_{21}x + u_{20}$ then we can write $\mathcal{D}_1 = P_1 - P_\infty$ and $\mathcal{D}_1 = P_2 + P_3 - 2P_\infty$.

   a) If ιP_1 occurs in $\mathcal{D}_2$, say $\iota P_1 = P_2$ then $\mathcal{D}_1 + \mathcal{D}_2 = P_3 - P_\infty$. In particular

   $$u = x + u_{21} - u_{10}, \quad v = v_2(-u_{21} + u_{10}).$$

   b) If P_1 occurs in $\mathcal{D}_2$ then we can apply the doubling in (2.a) and add $[x + u_{21} - u_{10}, v_2(-u21 + u_{10})]$ using the following (3.c) if $P_2 \neq P_3$. Otherwise one can double $\mathcal{D}_2$ and then subtracts $\mathcal{D}_1$ using (3.c).

   c) If ιP_1 and P_1 do not occur in $\mathcal{D}_2$ we can use the general algorithms. Faster implementations will be discussed later in section 4.4

4. If $\deg u_1 = \deg u_2 = 2$, then we can assume that $\mathcal{D}_1 = P_1 + P_2 - 2P_\infty$ and $\mathcal{D}_1 = P_3 + P_4 - 2P_\infty$.

   a) If $u_1 = u_2$, then we can assume that the x-coordinate of P_i and P_{i+2} are equal.

      i) If $v_1 = -v_2 - h \mod u_1$, then the two divisors are opposite and $\mathcal{D}_1 + \mathcal{D}_2 = [1, 0]$.

      ii) If $v_1 = v_2$ we can distinguish two cases:

         - If P_1 is a Weierstrass point, then $\mathcal{D}_1 + \mathcal{D}_2 = 2P_2 - 2P_\infty$ and we can apply (2.a) to $[x + u_{11} + x_{P_1}, v_1(-u_{11} - x_{P_1}]$, where x_{P_1} is compute using $(x - x_{P_1}) = \gcd(h + 2v_1, u_1)$. Indeed P_1 is a Weierstrass point iff $h(x_{P_1}) = -2y_{P_1}$.
         - If P_1 is not a Weierstrass point we can apply the general algorithms. A faster implementation will be discuss later in section 4.4

      iii) The last of these cases is $P_1 = P_3$ and $P_2 = \iota P_4$. Then $\mathcal{D}_1 + \mathcal{D}_2 = 2P_1$ and we can compute it using (2.a) on $[x - \frac{v_{10} - v_{20}}{v_{21} - v_{11}}, v_1(\frac{v_{10} - v_{20}}{v_{21} - v_{11}})]$.

   b) If $\deg(\gcd(u_1, u_2)) = 1$, then we can suppose that P_2 and P_4 are distinct and non-conjugate.

      i) If $P_1 = \iota P_3$, then the sum $\mathcal{D}_1 = \mathcal{D}_2 = P_2 + P_4 - 2P_\infty$ and we are done.

ii) If $P_1 = P_3$ then we can use (2.a) and (3.c) and compute $\mathcal{D}_1 + \mathcal{D}_2$ as

$$\Big(\Big(\big(2\,(P_1 - P_\infty)\big) + P_2 - P_\infty\Big) + P_3 - P_\infty\Big)$$

c) If $\gcd(u_1, u_2) = 1$ then all the P_j are distinct and non-conjugate each other. This is the most common case and we will give the explicit algorithm.

Addition

Now we give the explicit formulæ for the most common case, $\deg u_1 = \deg u_2 = 2$ and $\gcd(u_1, u_2) = 1$. The addition algorithm simply return the function $u = u_1u_2$ and the function v which satisfies

$$\begin{aligned} v &\equiv v_1 \mod u_1 \\ v &\equiv v_2 \mod u_2 \end{aligned}$$

The reduction algorithm must be iterated one time. And it returns the polynomials $u' = (f - vh - v^2)/u$ (if necessary make it monic) and $v' = -h - v \mod u$. In order to optimize the computation we give a different algorithm that does not compute explicitly the semi-reduced divisor.

$$\begin{aligned} k &= (f - v_2h - v_2^2)/u_2 \\ s &\equiv (v_1 - v_2)/u_2 \mod u_1 \\ l &= su_2 \\ u &= (k - s(l + h + 2v_2))/u_1 \\ u' &= u^* \\ v' &\equiv -h(l + v_2) \mod u' \end{aligned}$$

where u^* means that we make u monic.

For further details on the computation time and for the proof that this algorithm works see [Lan05]; it takes 3**S** + 22**M** + **I**, and if s is constant it takes only 2**S** + 11**M** + **I**.

In [Lan05] we can also find a way to compute the addition much faster in the case (3.c), when $\deg u_1 = 1, \deg u_2 = 2$ and $\gcd(u_1, u_2) = 1$. It is proved that it needs only **S** + 10**M** + **I**.

The same argument leads to a faster doubling algorithm:

$$\begin{aligned} k &= (f - hv - v^2)/u \\ s &\equiv k/(h + 2v) \mod u \\ l &= su \\ \tilde{u} &= s^2 - ((h + 2v)s - k)/u \\ u' &= \tilde{u}^* \\ v' &\equiv -h - (l + v) \mod u'. \end{aligned}$$

In [Lan05] it is proved that it needs $5\mathbf{S} + 22\mathbf{M} + \mathbf{I}$, and if s is constant it takes only $3\mathbf{S} + 13\mathbf{M} + \mathbf{I}$ in odd characteristic. Another multiplication is required in even characteristic.

Chapter 5

Arithmetic on non-hyperelliptic curves

The present chapter will focus on the study of superelliptic curves and general non-hyperelliptic curves of genus 3, i.e. smooth quartics in the plane. These curves are the first and simplest examples of non-hyperelliptic curves. The construction of the reduction algorithm in the superelliptic case will be very similar to the hyperelliptic case, indeed they both have a single point at infinity. The case of quartics will be slightly different, indeed they have in general more than one point at infinity. For this chapter we mainly refer to [Bas+05] and [FOR07].

5.1 Superelliptic curves

A *superelliptic* curve is a plane curve of the form

$$\mathscr{C} : y^3 = f(x),$$

where f is a polynomial of degree at least 3, not divisible by 3 and without multiple roots in $\overline{\mathbb{k}}$. Since $\deg f \geq 4$ the curve has a unique point at infinity, namely $[0, 1, 0]$, and it is a singulas point if $\deg f > 4$. It is clear that $\mathscr{C}$ is a cover of degree 3 of the projective line, and that $\mathrm{Gal}(\overline{\mathbb{k}}(\mathscr{C})/\overline{\mathbb{k}}(x)) = \{1, \sigma, \sigma^2\}$ where $\sigma : Y \mapsto \xi Y$ and ξ is a primitive third root of unity. By Hurwitz formula we have

$$2g - 2 = (-2)\deg(\pi) + ram(\pi)$$

where $\pi : (x, y) \mapsto (y)$. Since the points of ramification for π are the points $(x_i, 0)$ with $f(x_i) = 0$ and the point at infinity, we have $2g - 2 = -2 \cdot 3 + 2\deg(f) + 2$ because they are of ramification 2, then

$$g = \deg(f) - 1.$$

As in Theorem 1.12.1 we represent every divisor $\mathcal{D}$ of degree 0 with its *reduced representation*, i.e. a divisor $\mathcal{E} - mP_\infty \sim \mathcal{D}$ that is minimal (respect to m).

As in the case of the hyperelliptic curve we can write it with its Mumford representation (u, w). If $\mathcal{E} = \sum P_i$, with $P_i = (x_i, y_i)$, then $u = \prod(x - x_i)$.

We remark that w is of the form $ry^2 + sy + t$ where $r, s, t \in \Bbbk[x]$, $\deg r$, $\deg s$, $\deg t < \deg u \leq g$, and $\gcd(u, r, s, t) = 1$.
Indeed, if $\mathcal{D}$ contains in its support the point $P_i, \sigma P_i, \sigma^2 P_i$ then we can remove these points using the rational function ℓ/ℓ_∞ where $\ell : x - x_i$ and ℓ_∞ is the line at infinity, hence $\mathcal{D}$ is not reduced. Therefore a reduced divisor cannot contain all the cycle $P_i + \sigma P_i + \sigma^2 P_i$ and the points $(x_i, 0)$ must have multiplicity at most 2, hence the degree (respect to y) of w is at most 2.

The sum $\mathcal{D} + \sigma\mathcal{D} + \sigma^2\mathcal{D}$ is the divisor of a polynomial in x, so that the divisor $\sigma\mathcal{D} + \sigma^2\mathcal{D}$ is the inverse of the divisor $\mathcal{D}$.

Even if the representation $(u(x), y - v(x))$ cannot be always obtained (unlike the hyperelliptic curves), it correspond to the most common case, so that we define the *typical divisor* to be a divisor of the form $(u, y - v)$, with $\deg v < \deg u \leq g$ and $u | v^3 - f$.

Now we give a results that shows the probability to have a typical divisor.

Theorem 5.1.1. *If $\Bbbk = \mathbb{F}_q$, then the ratio of the reduced typical divisors over the reduced divisors is $1 - \frac{1}{q}O(1)$. Moreover the probability to have a typical divisor after adding a distinct typical divisor or doubling a typical divisor is again $1 - \frac{1}{q}O(1)$.*

Proof. See [Bas+05]. □

The following theorem explain if a divisor $\sum_{i=1}^{k} P_i - kP_\infty$, with $k \leq g$, on a superellitic curve of genus 3 or 4 is already reduced or not.

Theorem 5.1.2. *On a superellipctic curve of genus 3 a divisor of the form $\sum_{i=1}^{k} P_i - kP_\infty$, with k at most 3, is not reduced if and only if it consist of three collinear points.*
On a superellipctic curve of genus 4 a divisor of the form $\sum_{i=1}^{k} P_i - kP_\infty$, with k at most 4, is not reduced if and only if it satisfies one of the following conditions:
⋆ *it contains a triplet of conjugate points,*
⋆ *it consists in two pairs of conjugate points,*
⋆ *it consists of four collinear points,*
⋆ *it consists of four points lying on a parabola $y - v$ and on an elliptic curve $y^2 + sy + t$ with $\deg s \leq 1$ and $\deg t = 2$.*
Moreover the elliptic curve intersect the superelliptic curve is these four points, three collinear points and their conjugate.

Proof. First assume that $\mathcal{D}$ is not reduced, and call $\mathcal{D}'$ its reduction. Write

$$\mathcal{D}' = \sum m_i P_i + \sum n_j (\sigma Q_j + \sigma^2 Q_j) - (*)P_\infty,$$

where the P_i and the Q_j have different x-coordinates, and denote by μ and ν respectively $\sum m_i$ and $\sum n_j$.

Let $\beta \in \Bbbk[x]$ be the monic polynomial such that

$$\text{div}\beta = \sum m_i (P_i + \sigma P_i + \sigma^2 P_i) + \sum n_j (Q_j + \sigma Q_j + \sigma^2 Q_j) - (*)P_\infty,$$

then the divisor $\mathcal{D} - \mathcal{D}' + \mathrm{div}\beta$ is principal and we call α its function. We have

$$\mathrm{div}\alpha = \mathcal{D} + \sum m_i(\sigma P_i + \sigma^2 P_i) + \sum n_j Q_j - (*)P_\infty.$$

Write $\alpha = ry^2 + sy + t$, we have

$$\begin{aligned}
\deg \mathcal{D}^+ + 2\deg \mathcal{D}'^+ &\geq \deg \mathcal{D}^+ + 2\deg \mathcal{D}'^+ - 3\nu \\
&= \deg \alpha \\
&= \deg_x N_{\Bbbk(\mathscr{C})/\Bbbk(x)}(\alpha) \\
&= \deg_x(\alpha \cdot \sigma\alpha \cdot \sigma^2\alpha) \\
&= \deg_x(r^3 f^2 + (s^3 - 3srt)f + t^3) \\
&= \max\{3\deg r + 2(g+1), 3\deg s + g + 1, 3\deg t\}
\end{aligned}$$

Now we distinguish different cases:

1) If $\deg \mathcal{D}^+ \neq g$ then $\deg \mathcal{D}'^+ \leq g - 2$ and $\deg \alpha \leq 3g - 5$. Since $g \in \{3, 4\}$ we have $r = 0$ and $\deg s \leq 0$, i.e. $s \in \{0, 1\}$.

   If $s = 1$, then $\mathrm{div}(\alpha)$ cannot contain a pair of conjugate points, hence $\mu = 0$, $\nu = \lfloor \frac{\deg \mathcal{D}'^+}{2} \rfloor \leq \lfloor \frac{g-2}{2} \rfloor \leq 1$ and $\deg \alpha \leq g - 1 + 1 < \deg f$, contradiction.

   If $s = 0$, then $\alpha = t \in \Bbbk[x]$, so that $\mathrm{div}(\alpha) \geq \mathrm{div}(\beta)$, hence $\beta | \alpha$. Since $\mathcal{D} = \mathcal{D}' + \mathrm{div}(\alpha/\beta)$ and $\deg \mathcal{D}^+ > \deg \mathcal{D}'^+$ we have $\deg(\alpha/\beta) \geq 1$, whence $\mathcal{D}$ contains to divisor of a vertical line.

2) If $\deg \mathcal{D}^+ = g$ and $r = 0$ then, since $\deg \alpha \leq 3g - 2$, $\deg s \leq 1$.

   If $s = 0$, then $\mathcal{D}$ contains to divisor of a vertical line.

   If $s = 1$, then as above $\mathrm{div}\alpha$ doesn't contains a pair of conjugate points, $\mu = 0$, $\nu \leq 1$, $\deg \alpha \leq g + 1$, and $\deg t \leq 1$. If $\nu = 0$, then $\beta = 0$, contradiction. If $\nu = 1$, then $\mathcal{D}' = \sigma Q + \sigma^2 Q$ and $\mathrm{div}\alpha = \mathcal{D} + Q$ and $\mathcal{D}$ contains g collinear points.

   If $\deg s = 1$, we can assume $\mu \geq 1$. Indeed if $\mu = 0$ then $\deg \alpha \leq g + 1$ and it contradicts $\deg(s^3 f + t^3) \geq g + 4$. Fix a point P_i in $\mathcal{D}'$,
   if P_i is unramified, then $y_i \neq 0$ and $\begin{cases} s(x_i)\sigma(y_i) + t(x_i) = 0 \\ s(x_i)\sigma^2(y_i) + t(x_i) = 0 \end{cases}$;
   if it is ramified, then $\mathrm{ord}_P\alpha = \mathrm{ord}_P Y + 1 = 2$ and $s(x_i)y_i + t(x_i) = 0$, hence, in every case $s(x_i) = t(x_i) = 0$. We have $x - x_i | \alpha$ and $P_i \leq \mathcal{D}$, hence $\mathcal{D} - P_i$ reduced to $\mathcal{D}' - P_i$ and, since $\deg(\mathcal{D}^+ - P_i) = g - 1$, $\mathcal{D} - P_i$ contains a triplet of conjugate point $Q, \sigma Q, \sigma^2 Q$, so that $g = 4$, $\mathcal{D}' = P$, $\beta = x - x_i$, and $\alpha = (x - x_i)(x - x_Q)$, contradiction.

3) If $\deg \mathcal{D}^+ = g$ and $r \neq 0$, then

$$\begin{aligned}
2g + 2 &\leq 3\deg r + 2g + 2 \\
&\leq \deg \alpha \\
&= \deg \mathcal{D}^+ + 2\deg \mathcal{D}'^+ - 3\nu \\
&\leq \deg \mathcal{D}^+ + 2\deg \mathcal{D}'^+ \\
&\leq 3g - 2.
\end{aligned}$$

This implies $g \geq 4$ (hence $g = 4$), and then all the inequalities are equalities. We have $\nu = 0$, $\mu = 3$, $r = 1$, $\mathcal{D}' = P_1+P_2+P_3$ with $P_i = (x_i, y_i)$, $\alpha = y^2+sy+t$, $\beta = (x-x_1)(x-x_2)(x-x_3)$, $\deg t \leq 3$, and $\deg s \leq 1$.

Now we prove that in this case $\beta | t - s^2$. Let $1 \leq m \leq 3$ such that the sum $m(\sigma P) + m(\sigma^2 P)$ is in $\mathrm{div}(\alpha)$.

a) If P is a ramification point, then the $\mathrm{ord}_P(y) = 1$, $\mathrm{ord}_P(\alpha) \geq 2m \geq 2$, $t(x_P) = 0$, $\mathrm{ord}_P(t) \geq 3$, $\mathrm{ord}_P(y^2+t) = 2$, $s(x_P) = 0$, $\mathrm{ord}_P(s) \geq 3$, $\mathrm{ord}_P(\alpha) = 2$, $m = 1$. In particular $(x - x_P) | t - s^2$.

b) If P is unramified, then $\mathrm{ord}_P(y) = 0$, $\mathrm{ord}_P(\sigma\alpha) \geq m$, $\mathrm{ord}_P(\sigma^2\alpha) \geq m$. This implies $m \leq \mathrm{ord}_P(\sigma\alpha - \sigma^2\alpha) = \mathrm{ord}_P(y(y-s)) = \mathrm{ord}_P(y-s)$. Therefore, $m(\sigma P) + m(\sigma^2 P) \leq \mathrm{div}(\tilde{\alpha})$, where the function $\tilde{\alpha}$ is given by

$$\tilde{\alpha} = \sigma(y-s) \cdot \sigma^2(y-s) = y^2 + sy + s^2.$$

So that $m\sigma P + m\sigma^2 P$ is in $\mathrm{div}(\alpha - \tilde{\alpha}) = \mathrm{div}(t - s^2)$. In particular we have $(x - x_P)^m | t - s^2$.

c) Since $\sigma\mathcal{D}' + \sigma^2\mathcal{D}' \leq \mathrm{div}(\alpha)$, we have $\beta | t - s^2$. Moreover we proved that $\mathcal{D}' \leq \mathrm{div}(y - s)$.

By the Bézout theorem we have $\mathrm{div}(y-s) = \mathcal{D}' + Q + S$, where Q and S are two points. Consider now the following two cases:

a) $\deg t \leq 2$. Since β has degree 3, we have $t = s^2$ and $\alpha = \tilde{\alpha}$. Then

$$\begin{aligned}
\mathcal{D} &= \mathrm{div}\alpha - \mathrm{div}\beta + \mathcal{D}' \\
&= \left(\sum_{i=1}^{3}(\sigma P_i + \sigma^2 P_i) + \sigma S + \sigma^2 S + \sigma Q + \sigma^2 Q\right) \\
&\quad - \left(\sum_{i=1}^{3}(P_i + \sigma P_i + \sigma^2 P_i\right) + \left(\sum_{i=1}^{3} P_i\right) \\
&= \sigma S + \sigma^2 S + \sigma Q + \sigma^2 Q.
\end{aligned}$$

b) $\deg t = 3$. We have $\alpha = y^2 + sy + s^2 + c\beta$, that is an elliptic curve. Then

$$\begin{aligned}
\mathcal{D} &= \mathrm{div}\alpha - \mathrm{div}\beta + \mathcal{D}' \\
&= \mathrm{div}\left(\frac{\alpha(y-s)}{c\beta}\right) - Q - S \\
&= \mathrm{div}\left(y - s + \frac{(y^2+sy+s^2)(y-s)}{c\beta}\right) - Q - S \\
&= \mathrm{div}\left(y - s + \frac{(f - s^3)}{c\beta}\right) - Q - S.
\end{aligned}$$

Since $\mathrm{div}\beta \leq \mathrm{div}N_{\Bbbk(\mathscr{C})/\Bbbk(x)}(y-s)$, we have $\beta | f - s^3 = N_{\Bbbk(\mathscr{C})/\Bbbk(x)}(y-s)$. Furthermore $\deg\left(s - \frac{(f-s^3)}{c\beta}\right) = 2$, hence $y - \left(s - \frac{(f-s^3)}{c\beta}\right)$ define a parabola containing the points of $\mathcal{D}$.
Moreover we have $\mathrm{div}\alpha = \sum_{i=1}^{3}(\sigma P_i + \sigma^2 P_i) + \mathcal{D}$ and the P_i's lie on $y - s$, hence they are collinear.

This proves the necessity of the conditions.

To prove that the conditions are sufficient we can easily construct the reducing functions. □

Corollary 5.1.3. *On a superelliptic curve of genus 3 or 4, a typical divisor represented by* $(u, y-v)$ *is reduced whenever* $\deg u < g$, *or* $\deg u = g$ *and* $\deg v = g-1$.

Proof. The previous theorem shows that, for $g \in \{3, 4\}$, a divisor is not reduced either if $\deg u < g$ and it contains a pair of conjugate points, or $\deg u = g$ and its points can be interpolated by a polynomial $y - v$ with $\deg v \leq g - 2$. □

Addition

As for hyperelliptic curves, we give two algorithms for computing the addition or the doubling of two divisors, one for the composition and one for the reduction. We consider only typical divisors $\mathcal{D}_i = (u_i, y - v_i)$. As we had already seen in Theorem 5.1.1, the probability to have a typical divisor after an addition of two typical divisor is extremely high. To be accurate, it does not occur when $\gcd(u_1, u_2, v_1^2 + v_1v_2 + v_2^2) \neq 1$. Indeed suppose that u_1 and u_2 have a common root on a point P, now if P is a ramification point, then $v_1(x_P) = v_2(x_P) = 0$ and $(v_1^2 + v_1v_2 + v_2^2)(x_P) = 0$; if P is not a ramification point, then $v_1(x_P) = v_2(x_P)$ if and only if $(v_1^2 + v_1v_2 + v_2^2)(x_P) \neq 0$.

So we give an algorithm that works only in this case.

Algorithm 3.

INPUT: $\mathcal{D}_1 = (u_1, y - v_1)$, $\mathcal{D}_2 = (u_2, y - v_2)$ *two typical divisors on the superelliptic curve* $\mathscr{C}$ *such that* $\gcd(u_1, u_2, v_1^2 + v_1v_2 + v_2^2) = 1$.

OUTPUT: $\mathcal{D}_3 = \mathcal{D}_1 + \mathcal{D}_2 = (u, y - v)$.

1. *Find* $s_1, s_2, s_3 \in \Bbbk[x]$ *such that*

$$s_1u_1 + s_2u_2 + s_3(v_1^2 + v_1v_2 + v_2^2) = 1;$$

2. *Set*

$$\begin{aligned} u &= u_1u_2 \\ v &= v_1 + s_1u_1(v_2 - v_1) - s_3(v_1^3 - f) \mod u \end{aligned}$$

Theorem 5.1.4. *The previous Algorithm is correct.*

Proof. First note that the definition of v is symmetric in v_1 and v_2. Indeed

$$\begin{aligned} v &= v_1 + s_1u_1(v_2 - v_1) - s_3(v_1^3 - f) \mod u \\ &= (1 - s_1u_1)v_1 + s_1u_1v_2 - s_3(v_1^3 - f) \mod u \\ &= (s_2u_2 + s_3(v_1^2 + v_1v_2 + v_2^2))v_1 + s_1u_1v_2 - s_3(v_1^3 - f) \mod u \\ &= s_1u_1v_2 + s_2u_2v_1 + s_3(v_1^2v_2 + v_1v_2^2 + f) \mod u. \end{aligned}$$

Now the only thing to prove is that $u|v^3-f$. Let p be an irreducible polynomial and e_1, e_2 such that $p^{e_i}||u_i$, hence $p^e||u$, with $e=e_1+e_2$. Suppose that $e_1=0$ then $p^{e_2}|v_2^3-f$ and $v \equiv v_2 \pmod{u_2}$; this implies that $p^e|v^3-f$. The same for $e_2=0$. Assume now that $e_1, e_2 \geq 1$, and assume also $e_2 \leq e_1$, so that p^{e_2} divides u_1, u_2; since $v_1 \equiv v_2 \equiv f \pmod{p^{e_2}}$, p^{e_2} divides also $v_1^3-v_2^3$. From $\gcd(u_1, u_2, \frac{v_1^3-v_2^3}{v_1-v_2})=1$ we deduce that $p^{e_2}|v_1-v_2$. We have also that $1 \equiv s_3\frac{v_1^3-v_2^3}{v_1-v_2} \equiv 3s_3v_1^2 \pmod{p^{e_2}}$, and then $p^e|u_1(v_1-v_2)$. By definition we get

$$v \equiv v_1 - s_3(v_1^3-f) \mod p^e.$$

Hence

$$v^3-f \equiv v_1^3 - 3v_1^2s_3(v_1^3-f) + (v_1^3-f)^2(\cdots) - f \mod p^e,$$

but, since $p^e|u_1^2$ and $u_1|(v_1^3-f)$, we have

$$v^3-f \equiv (v_1^3-f)(1-3v_1^2s_3) \equiv 0 \mod p^e.$$

□

We can apply the previous algorithm to the case of doubling only if the divisor does not contain a ramification point in its support, i.e. if $\gcd(u_1, v_1)=1$. Then the algorithm becomes

Algorithm 4.

INPUT: $\mathcal{D}_1 = (u_1, y-v_1)$, *a typical divisor such that* $\gcd(u_1, v_1)=1$.

OUTPUT: $\mathcal{D}_3 = 2\mathcal{D}_1 = (u, y-v)$.

1. *Find* $s_1, s_3 \in \Bbbk[x]$ *such that*

$$s_1u_1 + 3s_3v_1^2 = 1.$$

2. *Set*

$$\begin{aligned} u &= u_1^2, \\ t &= -s_3 \cdot (v_1^3-f)/(u_1) \mod u_1, \\ v &= v_1 + tu_1. \end{aligned}$$

The addition of two divisor $\mathcal{D}_1$ and $\mathcal{D}_2$ in case their support are disjoint becomes easier. Indeed we can use the following

Algorithm 5.

INPUT: $\mathcal{D}_1 = (u_1, y-v_1)$, $\mathcal{D}_2 = (u_2, y-v_2)$ *such that* $\gcd(u_1, u_2)=1$.

OUTPUT: $\mathcal{D}_3 = \mathcal{D}_1 + \mathcal{D}_2 = (u, y-v)$.

1. *Find* $s_1, s_2 \in \Bbbk[x]$ *such that*

$$s_1u_1 + s_2u_2 = 1.$$

2. *Set*

$$\begin{aligned} u &= u_1^2, \\ t &= s_1(v_2 - v_1) \mod u_2, \\ v &= v_1 + tu_1. \end{aligned}$$

Reduction

Now we give an algorithm that reduces a typical divisor $\mathcal{D} = (u, y-v)$ to a reduced typical divisor $\mathcal{D}_R = (u_R, y - v_R)$. The main idea is to:

1. invert the divisor $\mathcal{D}$ using
$$-\mathcal{D} + \mathrm{div}(u) = (u, y^2 + vy + v^2);$$
2. choose a typical ideal $\mathcal{D}'$ in the class of $-\mathcal{D}$, say $\mathcal{D}' = -\mathcal{D} + \mathrm{div}(\beta)$;
3. let $\alpha \in \mathscr{L}(\mathcal{D}'^+)$ such that
$$-\mathrm{ord}_{P_\infty}(\alpha) = \min_{\psi \in \mathscr{L}(\mathcal{D}'^+)} \{-\mathrm{ord}_{P_\infty}(\psi)\};$$
4. put $\mathcal{D}_R = \mathcal{D} + \mathrm{div}(\alpha) - \beta$.

The following algorithm tells us how to compute the typical form of a divisor in the opposite class of the divisor $\mathcal{D}$. Moreover, for an appropriate index i_0, the algorithm returns a divisor with lower degree of the given divisor $\mathcal{D}$. Then we can iterate an even number of times the algorithm to compute the reduced typical divisor of $\mathcal{D}$.

Algorithm 6.

INPUT: *a typical divisor* $\mathcal{D} = (u, y - v)$.

OUTPUT: *a typical divisor* $\mathcal{D}' \sim -\mathcal{D}$ *in the form* $(u', y - v')$

1. *Use the extended Euclidean algorithm and find the sequence of polynomial* r_i, s_i, *and* t_i *such that*
$$r_i = s_i u + t_i v.$$
Assume that $\gcd(r_i, t_i) = 1$.

2. *Set*
$$\begin{aligned} u' &= \frac{t_i^3 f - r_i^3}{u} \\ v' &= r_i \cdot (t_i^{-1} \mod u') \end{aligned}$$

Remark. The assumption $\gcd(r_i, t_i) = 1$ happens with probability $1 - \frac{1}{q}O(1)$ and we have
$$\gcd(t_i, u') | \gcd(t_i, t_i^3 f - r_i^3) | \gcd(t_i, r_i)^3 = 1,$$
then the inverse of t_i modulo u' does exist.

Theorem 5.1.5. *The previous algorithm is correct. Moreover if* $\deg u \geq g$ *and* $\deg v = \deg u - 1$*, and suppose also that* $\deg r_i = \deg_u -1 - i$ *and* $\deg t_i = i$*, then using the algorithm with the index* $i_0 = \left\lfloor \frac{3\deg u - g - 4}{6} \right\rceil$*, we have:*

⋆ *if* $\deg u \geq g + 2$*, then* $\deg u' < \deg u$*;*

⋆ *if* $\deg u \in \{g, g+1\}$*, then* $\deg u' = g$*.*

Proof. First we prove that the algorithm gives the correct result.

$$\begin{aligned} \operatorname{div}((u, y - v)) &= \operatorname{div}((u, t_i y - t_i v)) && (5.1)\\ &= \operatorname{div}((u, t_i y - r_i)) && (5.2)\\ &\sim -(\operatorname{div}(t_i y - r_i) - \operatorname{div}((u, t_i y - r_i))) && (5.3)\\ &= -\operatorname{div}((u', t_i y - r_i)) && (5.4)\\ &= -\operatorname{div}((u', y - r_i(t_i \mod u'))) && (5.5)\end{aligned}$$

In the step 5.1 we used $\gcd(t_i, u) | \gcd(t_i, r_i) = 1$; in 5.2 we used $t_i v \equiv r_i \mod u$; the step 5.3 is true because the divisor $\operatorname{div}(t_i y - r_i)$ is principal; and in 5.5 we used $\gcd(u', t_i) = 1$. For the step 5.4 note that $N_{\bar{\mathbb{k}}(\mathscr{C})/\bar{\mathbb{k}}(x)}(t_i y - r_i) = t_i^3 f - r_i^3 = uu'$, so that $\operatorname{div}(t_i y - r_i) = \operatorname{div}(uu', t_i y - r_i)$. Moreover if a point $P = (x_P, y_P)$ is in $\operatorname{div}(t_i y - r_i)$, then $t_i(x_P) \neq 0$ since $\gcd(t_i, r_i) = 1$, and if $y_P \neq 0$, then the points $\sigma P, \sigma^2 P$ are not contained in $\operatorname{div}(t_i y - r_i)$; if $y_P = 0$, then we have $\operatorname{ord}_P(t_i y - r_i) = 1$, because $\operatorname{ord}_P(y) = 1$, this shows that exactly one of the two divisors $\operatorname{div}((u, t_i y - r_i))$ or $\operatorname{div}((u', t_i y - r_i))$ contains P. This shows that 5.4 holds, and the algorithm is correct.

For the second part of the theorem define the function

$$d(i) = \max\{3i + g + 1 - \deg u, 2\deg u - 3 - 3i\} = \max\{\delta, \gamma\}$$

that is the degree of the divisor $\operatorname{div}((u', y - r_i(t_i \mod u')))$ after one iteration of the algorithm using the function r_i, t_i. Since δ is strictly increasing and γ is strictly decreasing, $d(i)$ assume the (real) minimum for $i = i_{min} = \frac{3\deg u - g - 4}{6}$. Then we have $d(i_{min}) = \frac{\deg u + g - 2}{2}$. Note that the slopes of the linear functions δ and γ are $+3, -3$ then for $i \in \mathbb{N}$, $d(i) = d(i_{min}) + 3 \cdot |i - i_{min}|$ and the minimum of the function d is attained for the closed integer i_0 to i_{min}. Since $|i - i_{min}| \leq \frac{1}{2}$, we have $d(i_0) \leq \lfloor g - 1 + \frac{3}{2} \rfloor$ for $\deg u = g$ and $d(i_0) \leq \lfloor \deg u - 2 + \frac{3}{2} \rfloor = \deg u - 1$ for $\deg u \geq g + 2$. In case $\deg u = g + 1$ we use the fact that $g \not\equiv -1 \mod 3$, then $d(i_0) < \lfloor g - \frac{1}{2} + \frac{3}{2} \rfloor$, hence $d(i_0) = g$. □

Corollary 5.1.6. *Let* $\mathcal{D} = (u, y - v)$ *with* $\deg u = 2g$ *and* $\deg v = 2g - 1$*. In the assumptions of Theorem 5.1.5 we can apply the algorithm two times for* $g = 3$*, or four times for* $g = 4$ *and it is enough to obtain a reduced typical divisor* $\mathcal{D}' \sim \mathcal{D}$*.*

5.2 Non-hyperelliptic curves of genus 3

As we already proved, a non-hyperelliptic curve of genus 3 is birationally equivalent to a smooth plane curve of degree 4. So we are allowed to consider a quartics, call it $\mathscr{Q}$.

Suppose that there exists a line that intersects the curve $\mathscr{Q}$ in four $\Bbbk$ rational points, possibly with multiplicity. Up to linear transformation of the projective space, we can consider the line at infinity, $\ell_\infty : Z = 0$, and we can call the four point $P_1^\infty, P_2^\infty, P_3^\infty, P_4^\infty$. We state without proof the sufficient conditions in which this assumption is fulfilled for a base field $\Bbbk = \mathbb{F}_q$, where $q = p^r$.

Proposition 5.2.1. *There exists a line intersecting the smooth quartic $\mathscr{Q}$ in four $\Bbbk$-rational points, with multiplicity, if*

- *$p = 2$, $q > 8$ and $\#\mathscr{Q}(\mathbb{F}_q) \geq q + 3$,*
- *$p > 2$ and $q > 10^6$,*
- *$p > 2$, $q > 8$ and $\#\mathscr{Q}(\mathbb{F}_q) \geq p - \frac{\sqrt{q}}{4} + \frac{7}{4}$.*

Proof. See [FOR07]. □

Now, fix the divisor $\mathcal{D}^\infty = P_1^\infty + P_2^\infty + P_3^\infty$. Rearranging the proof of 1.12.1 we know that for every divisor $\mathcal{D}$ of degree 0 there exists an effective divisor $\mathcal{D}^+$ such that $\mathcal{D}^+ - \mathcal{D}^\infty \sim \mathcal{D}$.

Theorem 5.2.2. *Let $\mathcal{D}_1$ and $\mathcal{D}_2$ two divisor of degree 0. Then $\mathcal{D}_1 + \mathcal{D}_2$ is equivalent to $\mathcal{D}^+ - \mathcal{D}^\infty$ given by the following algorithm:*

- *Take the cubic $\mathscr{E}$ passing through $\mathcal{D}_1^+, \mathcal{D}_2^+, P_1^\infty, P_2^\infty, P_4^\infty$. It is unique since it is determined by nine points on the plane (if some point are equal consider the relative multiplicity of intersection with $\mathscr{Q}$). The cubic intersect the quadric also in the residual effective divisor $\mathcal{E}$.*
- *Take the unique conic $\mathscr{C}$ passing through $\mathcal{E}, P_1^\infty, P_2^\infty$. This conic in unique and it also intersect the quadric in the residual divisor $\mathcal{D}^+$.*

Proof. Consider the differential $\omega = dx/f_y$, where f_y is the derivatives respect to y of the affine equation for $\mathscr{Q}$. It is easy to see that $\operatorname{div}(\omega)$ has support only on l_∞ because $\mathscr{Q}$ is smooth. Changing coordinates $\xi = X_1/X_2, \zeta = X_0/X_2$ we have $\frac{dx}{f_y} = -\frac{dy}{f_x} = \frac{\zeta^{\deg(\mathscr{Q})-3}}{\tilde{f}(\xi,\zeta)} d\zeta$, where $f_X(\xi/\zeta, 1/\zeta) = \frac{\tilde{f}(\xi,\zeta)}{\zeta^{\deg(\mathscr{Q})-1}}$, hence every point at infinity has order $\deg(\mathscr{Q}) - 3 = 1$, hence $(\mathscr{Q} \cdot l_\infty)$ is canonical. Now it is clear that $(\mathscr{E} \cdot \mathscr{Q}) \sim 3K$ and $(\mathscr{C} \cdot \mathscr{Q}) \sim 2K$. Therefore we have

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + \mathcal{E} \sim 3K,$$

$$\mathcal{E} + P_1^\infty + P_2^\infty + \mathcal{E}' \sim 2K$$

and

$$P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty \sim K.$$

Then

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + \mathcal{E} \sim 3K \sim \mathcal{E} + P_1^\infty + P_2^\infty + \mathcal{E}' + P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty$$

so that

$$D_1^+ + D_2^+ \sim \mathcal{E}' + \mathcal{D}^\infty.$$

Finally

$$\mathcal{D}_1 + \mathcal{D}_2 \sim \mathcal{E}' - \mathcal{D}^\infty,$$

hence $\mathcal{E}' = D^+$. □

A divisor $\mathcal{D}$ is in the typical form if

- the three points in $\mathcal{D}^+$ are not collinear;
- there is no point at infinity in the support of $\mathcal{D}^+$;
- the three x-coordinate x_i of the points in the support of $\mathcal{D}^+$ are distinct.

In this case we can associate to it the Mumford representation $\mathcal{D} = (u, v)$ as follow:

⋆ $u, v \in \Bbbk[x]$
⋆ $u = \prod(x - x_i)$ is monic of degree 3
⋆ $\deg(v) = 2$
⋆ $u|f(x, v(x))$

Now we distinguish different cases:

- the line ℓ_∞ intersect the quartic in four distinct points.
- the line ℓ_∞ intersect the quartic in three points, assume that $P_1^\infty = P_2^\infty$. Hence the line is a tangent line
- the line ℓ_∞ intersect the quartic in two points.
  If $P_1^\infty = P_2^\infty$ and $P_3^\infty = P_4^\infty$, then the line is a bitangent.
  If $P_1^\infty = P_2^\infty = P_3^\infty$ the the point P_1^∞ is a flex.
- the line ℓ_∞ intersect the quartic in one point. That point is called hyperflex.

Tangent case

Assume now that the line ℓ_∞ is tangent at P_1^∞ then in this situation the quadric has the form

$$y^3 + h_1 y^2 + h_2 y = f_4,$$

where $\deg(h_1) \leq 2, \deg(h_2) \leq 3, \deg(f_4) \leq 4$. It follows that the cubic $\mathscr{E}$ has the form

$$y^2 + sy + t = 0,$$

where s and t are polynomials in x of degrees $\deg(s) \leq 2$ and $\deg(t) \leq 2$. The conic $\mathscr{C}$ has the form

$$y - v,$$

with v of degree 2.

Algorithm 7.

INPUT: $\mathcal{D}_1 = (u_1, v_1)$ *and* $\mathcal{D}_2 = (u_2, v_2)$*, two typical divisor*

OUTPUT: $\mathcal{D}_3 = \mathcal{D}_1 + \mathcal{D}_2 = (u_3, v_3)$

1. *Computation of the cubic* $\mathscr{E}$ *in case of addition*

   a. *Compute* $t_1 = (v_1 - v_2)^{-1} \mod u_2$

   b. *Compute the remainder* r *of* $(u_1 - u_2)t_1$ *by* u_2

   c. *Find the couple* (s, δ_1) *such that*

   $$\begin{cases} \deg_x(-v_1(v_1 + s) + u_1\delta_1) = 2 & \\ v_1 + v_2 + s \equiv r\delta_1 & \mod u_2 \end{cases}$$

   where $s, \delta_1 \in \Bbbk[x]$ *with* $\deg(s) = 2$ *and* $\deg(\delta_1) = 1$.
   Then $\mathscr{E} = (y - v_1)(y + v_1 + s) + u_1\delta_1$.

2. *Computation of the cubic* $\mathscr{E}$ *in case of doubling*

   a. *Compute* $t_1 = \big((v_1^3 + v_1^2h_1 + v_1h_2 - f_4)/u_1\big)^{-1} \mod u_1$

   b. *Compute the remainder* r *of* $3v_1^2 + 2v_1h_1 + h_2)t_1$ *by* u_1

   c. *Find a couple* (s, δ_1) *such that*

   $$\begin{cases} \deg_x(-v_1(v_1 + s) + u_1\delta_1) = 2 & \\ 2v_1 + s \equiv r\delta_1 & \mod u_1 \end{cases}$$

   where $s, \delta_1 \in \Bbbk[x]$ *with* $\deg(s) = 2$ *and* $\deg(\delta_1) = 1$.
   Then $\mathscr{E} = (y - v_1)(y + v_1 + s) + u_1\delta_1$.

3. *Computation of the conic* $\mathscr{C}$

   a. *Compute* $u' = Res_y^*(\mathscr{E}, \mathscr{Q})/(u_1u_2)$

   b. *Compute* $\alpha_1 = (t - s^2 - h_2 + sh_1)^{-1} \mod u'$

   c. *Compute the remainder* v' *of* $\alpha_1(st - th_1 - f_4)$ *by* u'.
   Then the conic $\mathscr{C}$ *is* $y - v'$.

4. *Computation of* $\mathcal{D}_1 + \mathcal{D}_2$

   a. $v_3 = v'$

   b. $u_3 = ((v_3^3 + v_3^2h_1 + v_3h_2 - f_4)/(u'))^*$

   c. $\mathcal{D}_1 + \mathcal{D}_2 = (u_3, v_3)$.

Here the * *means that we divide a function by its leading coefficient.*

Theorem 5.2.3. *The algorithm works*

Proof. We have to prove that the points in the support of $\mathcal{D}_1$ and $\mathcal{D}_2$ are in the cubic $\mathscr{E}$. Pick a point $P = (x_i, y_i)$ in $\mathcal{D}_1$, then $u_1(x_i) = 0$ and $y_i = v_1(x_i)$. Evaluating in the cubic we have $(v_1(x_i) - v_1(x_i))(*) + u_1(x_i)\delta_1(x_i) = 0$. Pick now a point in $\mathcal{D}_2$, evaluating in $\mathscr{E}$ we get

$$(v_2(x_i) - (v_1(x_i))((v_2(x_i) + (v_1(x_i) + s(x_i)) + u_1(x_i)\delta_1(x_i)$$

and then

$$(-t_1(x_i))(r(x_i)\delta_1(x_i)) + u_1(x_i)\delta_1(x_i) = -u_1(x_i)\delta_1(x_i) + u_1(x_i)\delta_1(x_i) = 0.$$

Then the cubic $\mathscr{E}$ is the right one.
For the doubling we can do the same check.
For the equation of the conic, assume that $Q = (x', y')$ is a point in the intersection of the cubic with quartic such that $u'(x') = 0$, i.e. Q is in $\mathcal{E}$ (see Theorem 5.2.2). Then

$$\begin{aligned} v'(x') &= \frac{s(x')t(x') - t(x')h_1(x') - f_4(x')}{t(x') - s^2(x') - h_2(x') - s(x')h_1(x')} \\ &= \frac{y'\big(-s^2(x') - s(x')y' + s(x')h_1(x') + y'h_1(x') - y'^2 - y'h_1(x') - h_2(x')\big)}{-y'^2 - s(x')y - s^2(x') - h_2(x') + s(x')h_1(x')} \\ &= y'. \end{aligned}$$

Hence the conic passes through the divisor $\mathcal{E}$ (with the appropriate multiplicities).

Step 4. is clear. The algorithm is correct. □

Flex case

Conjecture 5.2.1. *The probability that a smooth curve has at least one rational flex is asymptotic to $1 - e^{-1} + \alpha$ when q tends to infinity, where $|\alpha| \leq 10^{-25}$.*

If the quadric $\mathscr{Q}$ as a flex, we can assume that ℓ_∞ is the tangent at the flex $P_1^\infty = (0, 1, 0)$ and then the curve is of the form

$$y^3 + h_1y^2 + h_2y = f_4,$$

where $\deg(h_1) \leq 1, \deg(h_2) \leq 3, \deg(f_4) \leq 4$. It follows that the cubic $\mathscr{E}$ has the form

$$y^2 + sy + t = 0,$$

where s and t are polynomial in x of degrees $\deg(s) \leq 1$ and $\deg(t) \leq 3$. The conic $\mathscr{C}$ has the form

$$y - v,$$

with v of degree 2.

The algorithm is the same as Algorithm 7, but in this case the polynomial s and δ_1 are of degree 1. All become easier to compute.
If the characteristic of the field $\Bbbk$ is greater than 3, then we can also assume that the curve has the form $y^3 + h_2y = f_4$, and f_4 had no x^3 term. In this case the addition require 148**M** + 15**S** + 2**I** and the doubling require 165**M** + 20**S** + 2**I**.

Hyperflex case

This is a sub case of the Flex case. Here the curve is birationally equivalent to a curve of the form $y^3 + h_1y^2 + h_2y = f_4$, where $\deg(h_1) \leq 1$, $\deg(h_2) \leq 2$, $\deg(f_4) \leq 4$. We can take the same assumption for high characteristic. In this case the addition require 131**M** + 14**S** + 2**I** and the doubling require 148**M** + 19**S** + 2**I**.

Chapter 6

Reduction for general curve

In this chapter we explain how to reduce divisors in general. We have already seen in Theorem 1.12.1 that every divisor class in $\mathrm{Pic}^0_{\mathscr{C}}$ admits a reduced representative of the form $\mathcal{E} - gP_\infty$, where $\mathcal{E}$ is an effective divisor of degree g. We have seen also, in Theorem 4.1.6, that for hyperelliptic curves this representative is unique if we consider only semi-reduced divisor, but this is not true for general curves.

For this chapter we mainly refer to [Heß02].

General strategy

Denote by $\mathcal{A}$ a divisor of degree bigger than 1, and assume for simplicity that its support is a subset of the points at infinity. A divisor $\widetilde{\mathcal{D}}$ is *maximal reduced along* $\mathcal{A}$ if $\widetilde{\mathcal{D}} \geq 0$ and $\dim_{\Bbbk}(\widetilde{\mathcal{D}} - r\mathcal{A}) = 0$ for each $r \geq 1$. The representation $\mathcal{D} = \widetilde{\mathcal{D}} + s\mathcal{A} - \mathrm{div}(a)$ is called maximal reduction for $\mathcal{D}$ along $\mathcal{A}$.

The maximal reduction is still not unique in general, but

Proposition 6.0.4. *For a maximal reduction* $\mathcal{D} = \widetilde{\mathcal{D}} + s\mathcal{A} - \mathrm{div}(a)$ *we have* $\dim \widetilde{\mathcal{D}} \leq \deg \mathcal{A}$*,* $\deg \widetilde{\mathcal{D}} < g + \deg \mathcal{A}$*, and an other maximal reduction has the same degree. Moreover the maximal reduction are in a bijection with* $\mathbb{P}^{\dim(\widetilde{\mathcal{D}})}$*. If furthermore* $\deg \mathcal{A} = 1$*, then the maximal reduction is unique.*

Proof. The first proprieties are easy to prove. Let now $\deg \mathcal{A} = 1$, and let s be the greatest integer such that $\dim(\mathcal{D} - r\mathcal{A}) = 1$. Then let $\widetilde{\mathcal{D}}$ be the only effective divisor in $|\mathcal{D} - r\mathcal{A}|$, it is maximal reduced and $\widetilde{\mathcal{D}} + r\mathcal{A}$ is the unique maximal reduction of $\mathcal{D}$ along $\mathcal{A}$. □

Remark.

i) On hyperelliptic curves we can consider $\mathcal{A} = P_\infty$ and then the notions of maximal reduced and reduced are equal.

ii) On superelliptic curves we can consider $\mathcal{A} = P_\infty$, and also in this case the maximal reduction is unique.

iii) On smooth plane quartics we set $\mathcal{A} = \mathcal{D}^\infty = P_1^\infty + P_2^\infty + P_3^\infty$, and this case is slightly different from the previous.

The main idea for computing the maximal reduction of a divisor $\mathcal{D}$ is to search the largest r such that $\mathcal{D}-r\mathcal{A}$ still has positive dimension, then $\widetilde{\mathcal{D}} = \mathcal{D}-r\mathcal{A}+\text{div}(a)$ is either maximal reduced along $\mathcal{A}$ or an effective divisor with degree less than $g + \deg \mathcal{A}$; it is called *elementary reduction along* $\mathcal{A}$. In order to construct an algorithm that follows this idea we need a way to compute r, $\widetilde{\mathcal{D}}$, and a, hence we need to compute a basis for the space $\mathscr{L}(\mathcal{D} - r\mathcal{A})$.

First we give some useful definitions. Let S be a non empty set of (closed) points, for simplicity assume that $S = \text{supp}(\text{div}(x)^-)$, the set of points at infinity. Let $\mathfrak{o}_S$ be the subring of $\Bbbk(\mathscr{C})$ composed by the elements that are integral at all points of S, i.e. the ring $\{\phi \,|\, v_P(\phi) \geq 0,\ \forall P \in S\}$, on the other hand define $\mathfrak{o}^S$ be the subring of $\Bbbk(\mathscr{C})$ composed by the elements that are integral at all points outside S, i.e. the ring $\{\phi \,|\, v_P(\phi) \geq 0,\ \forall P \notin S\}$. These rings are Dedekind domains, hence we can denote by $\mathfrak{I}_S$ and $\mathfrak{I}^S$ their ideal groups. Furthermore we denote by $\mathfrak{o}_\infty$ the ring of elements of $\Bbbk(\mathscr{C})$ with non-positive degree.
Since we choose S to be the set of all points at infinity, we also have that $\mathfrak{o}^S$ equals the integral closure of $\Bbbk[x]$ in $\Bbbk(\mathscr{C})$, denoted by $Cl(\Bbbk[x], \Bbbk(\mathscr{C}))$. On the other hand we have $\mathfrak{o}_S = Cl(\mathfrak{o}_\infty, \Bbbk(\mathscr{C}))$.

6.1 Computing the Riemann-Roch space

In order to construct an algorithm for the computation of the Riemann-Roch space we need an algorithm that reduces square matrices over $\Bbbk(x)$.

6.1.1 Lattices and basic reduction over $\Bbbk[x]$

Let $\alpha \in \Bbbk((x^{-1}))$ be a formal Laurent series in x, i.e $\alpha = \sum_{i=-\infty}^{n_\alpha} a_i x^i$. Define the degree of α to be the exponent of the largest x-power occurring in α. For $v \in \Bbbk((x^{-1}))^n$ we define the (column) degree of v to be maximum of the degrees of the entries of v, it is denoted by $\deg(v)$. By $hc(v)$ we denote the vector of the coefficient of the $\deg(v)$-th power of x of the entries of v.

Let $\Lambda \subset \Bbbk((x^{-1}))$ be a free $\Bbbk[x]$-module of rank m and let $v_1, \cdots, v_m$ a basis of Λ. We also assume that the elements of the basis are $\Bbbk((x^{-1}))$-linearly independent, i.e. the lattice Λ is discrete regarding the metric induced by deg. We can define the lattice discriminant of Λ to be the minimum degree of the nonzero determinants of the $m \times m$ submatrices of the matrix $(v_1, \cdots, v_m)$, since it is an invariant for the lattice.

Proposition-Definition 6.1.1. *A basis $v_1, \cdots, v_m$ for Λ is called* reduced *if one of the following equivalent conditions is fulfilled:*

i) *$\{hc(v_i) \,|\, 1 \leq i \leq m\}$ is a set of linearly independent elements of $\Bbbk^n$;*

ii) $\deg(\sum_i f_i v_i) = \max_i \deg(f_i v_i)$ *for all $f_i \in \Bbbk[x]$;*

iii) *$v_1, \cdots, v_m$ realize the successive minima;*

iv) *$\sum_i \deg(v_i)$ equals the lattice discriminant.*

We call *reduction step* the addition of a $\mathbb{k}[x]$-linear combination of v_j to a v_i, $j \neq i$, such that the degree of v_i decrease. A the basis is reduced if and only if it does not admit ant reduction step. Since the lattice discriminant represents a lower bound for $\sum_i \deg(v_i)$, the number of reduction steps required to obtain a reduced basis is finite.

For a unimodular matrix $T \in \mathbb{k}[[x^{-1}]]^{n\times n}$ we have that $\deg(Tv) = \deg(v)$. We say that two lattices Λ_1, Λ_2 are isometric if there exists a unimodular matrix $T \in \mathbb{k}[[x^{-1}]]^{n\times n}$ such that $\Lambda_1 = T\Lambda_2$, then reduced basis are sent in reduced basis via T, the successive minima is preserved and the lattice discriminant is also preserved. Lastly we call orthogonal lattice of rank m and successive minima $-d_1 \leq \cdots \leq -d_m$ the unique lattice with basis $v_j = (x^{-d_j}\delta_{i,j}) \in \mathbb{k}((x^{-1}))^n$.

Proposition 6.1.2. *Every lattice $\Lambda \subset \mathbb{k}((x^{-1}))^n$ of rank m is isometric to a unique orthogonal lattice.*

Proof. Since the ring $\mathbb{k}[[x^{-1}]]$ is an Euclidean ring, any basis of the lattice Λ can be put, using row operation, in Hermite Normal Form, i.e. in an upper triangular shape where the entries over the diagonal are zero or have larger degree than the diagonal entry below, and the diagonal entries are of the form t^a. If we start with a reduced basis then, since $\{hc(v_i)\}$ is a set of linear independent elements, the HNF is already in a diagonal form. □

Remark. Note that we use only row operation, indeed we use only multiplication of unimodular matrices by the left.

Corollary 6.1.3. *Let $M \in \mathbb{k}(x)^{n\times n}$. Then there exist matrices $T_1 \in \mathfrak{o}_\infty^{n\times n}$ and $T_2 \in \mathbb{k}[x]^{n\times n}$ and integers $d_1 \geq \cdots, \geq d_n$ such that*

$$T_1 M T_2 = (x^{-d_j}\delta_{i,j})_{i,j},$$

where T_2 is the matrix obtained by the reduction algorithm applied to the columns and T_1 is the unimodular matrix of the previous proposition.

Proof. Since $M \in \mathbb{k}(x)^{n\times n}$, we have $T_1 \in \mathfrak{o}_\infty^{n\times n}$. □

Note that if M is a matrix in $\mathbb{k}(x)^{n\times n}$, then we can write $M = M_0/g$ with $M_0 \in \mathbb{k}[x]^{n\times n}$ and $g \in \mathbb{k}[x]$.

Corollary 6.1.4. *Let M_1 and M_2 be respectively a $\mathbb{k}[x]$-module and a $\mathfrak{o}_\infty$-module free of rank n. Then there exists a basis $v_1, \cdots, v_n$ of M_1 and a basis $w_1, \cdots, w_n$ of M_2 such that $(v_1, \cdots, v_n)N = (w_1, \cdots, w_n)$, where N is of the shape $(x^{-d_j}\delta_{i,j})_{i,j}$.*

Proof. Apply the previous corollary to the transformation matrix of arbitrary bases of M_1 and M_2. □

Example. We give an example for the reduction algorithm. We consider the matrix

$$\begin{pmatrix} x^3 + x & x^2 \\ x & x \end{pmatrix}.$$

It is not reduced because the sum of the column degrees is 5, but the degree of the discriminant is 4. We subtract x times the second column from the first, we exchange the two columns and negate the second column, we get

$$\begin{pmatrix} x^2 & -x \\ x & x^2 - x \end{pmatrix},$$

a reduced matrix. In order to obtain the normal form we subtract $1/x$ times the first raw from the second, then add $x/(x^2 - x - 1)$ the last raw from the first and scale the last raw by $x^2/(x^2 - x - 1)$, we get the normal form

$$\begin{pmatrix} x^2 & 0 \\ 0 & x^2 \end{pmatrix}.$$

6.1.2 Basis of $\mathscr{L}(\mathcal{D})$

First we give a way to represent divisor using ideals of $\mathfrak{o}_S$ and $\mathfrak{o}^S$.

Proposition 6.1.5. *There is a valuation preserving bijection between the set of (closed) points of the curve $\mathscr{C}$ and the set of prime ideals of $\mathfrak{o}_S$ and $\mathfrak{o}^S$. This bijection leads to an isomorphism*

$$\begin{array}{rcl} \mathrm{Div}(\mathscr{C}) & \longrightarrow & \mathfrak{I}^S \times \mathfrak{I}_S \\ \mathcal{D} & \mapsto & (\mathcal{D}^S, \mathcal{D}_S) \end{array}$$

Moreover we have $\mathscr{L}(\mathcal{D}) = (\mathcal{D}^S)^{-1} \cap (\mathcal{D}_S)^{-1}$.

Proof. Since $\mathfrak{o}_S$ and $\mathfrak{o}^S$ are Dedekind domains and the fraction field is in both cases $\Bbbk(\mathscr{C})$, we get the bijection from a well knows result from commutative algebra (see for example [AM69] chapter 9). For the last statement let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}^S$ and P the corresponding closed point, $P \notin S$, and r such that $\mathfrak{p}^r || \mathcal{D}^S$, hence $r = v_P(\mathcal{D})$. Since $\mathfrak{o}^S$ is a Dedekind domain then a function ϕ is in $(\mathcal{D}^S)^{-1} \subset \Bbbk(\mathscr{C})$ if and only if $v_P(\phi) \geq -r$ (see [AM69]). In the same way we get that $\forall P \in S$, $\phi \in (\mathcal{D}_S)^{-1}$ if and only if $v_P(\phi) \geq -v_P(\mathcal{D})$. So that $\mathscr{L}(\mathcal{D}) = (\mathcal{D}^S)^{-1} \cap (\mathcal{D}_S)^{-1}$. □

Remark.

- Note that, from a theoretical point a view, we did the same when we introduced the Mumford representation. Indeed for a divisor $\mathcal{E} - gP_\infty$, the corresponding ideal $(u, y - v)$ is in $\mathfrak{I}^S$, with $S = \{P_\infty\}$.

- If $\mathcal{D}$ has representation $(\mathcal{D}^S, \mathcal{D}_S)$, then $\mathcal{D} + r\mathrm{div}(x)^+$ is represented by $(x^r \mathcal{D}^S, \mathcal{D}_S)$ and $\mathcal{D} + r\mathrm{div}(x)^-$ by $(\mathcal{D}^S, x^{-r}\mathcal{D}_S)$.

- Note that the ideals in $\mathfrak{I}^S$ and in $\mathfrak{I}_S$ are respectively free $\Bbbk[x]$-modules and $\mathfrak{o}_\infty$-modules of rank $n = [\Bbbk(\mathscr{C}) : \Bbbk(x)]$. Then we can use the results of the previous section on lattice reduction, in particular we can apply the Corollary 6.1.4.

The following is the main theorem of the chapter and it gives us a way to compute the basis for the Riemann-Roch spaces. The proof is constructive and it will be part of the Algorithm 8.

Theorem 6.1.6. *For every divisor $\mathcal{D}$ of $\mathscr{C}$ there exist a unique sequence of integers $d_1 \geq \cdots \geq d_n$ and unique elements $v_i, \cdots, v_n \in \Bbbk(\mathscr{C})$ such that the set*

$$\{x^j v_i \mid 1 \leq i \leq n,\ 0 \leq j \leq d_i + r\}$$

is a $\Bbbk$ basis of $\mathscr{L}(\mathcal{D} + r\mathrm{div}(x)^-)$ for all $r \in \mathbb{Z}$. Moreover the elements $v_i, \cdots, v_n$ are $\Bbbk(x)$-linear independent.

Proof. First we prove the existence. Fix a divisor $\mathcal{D}$ and its representation $(\mathcal{D}^S, \mathcal{D}_S)$. Choose a basis $v_1, \cdots, v_n$ for $(\mathcal{D}^S)^{-1}$, a basis $w_1, \cdots, w_n$ for $(\mathcal{D}_S)^{-1}$ and a matrix $M \in \Bbbk(x)^{n \times n}$ such that $(w_1, \cdots, w_n)M = (v_1, \cdots, v_n)$. By Corollary 6.1.4 we can assume that M is of the form $(x^{-d_j}\delta_{i,j})_{i,j}$, hence $x^{-d_i}w_i = v_i$ with uniquely determined integers $-d_i$.

Fix now the divisor $\mathcal{D}+r\mathrm{div}(x)^-$, it is represented by the couple $(\mathcal{D}^S, x^{-r}\mathcal{D}_S)$. The bases of the fractional ideals $(\mathcal{D}^S)^{-1}$ and $x^r(\mathcal{D}_S)^{-1}$ are then given by $v_1, \cdots, v_n$ and $w_1' = x^r w_1, \cdots, w_n' = x^r w_n$, they are already related by a diagonal transformation. Fix now an element $z = \sum_i \lambda_i v_i$ in $(\mathcal{D}^S)^{-1}$, with $\lambda_i \in \Bbbk[x]$. We can write $z = \sum_i \lambda_i x^{-d_i - r} w_i'$, then z is in $x^r(\mathcal{D}_S)^{-1}$ if and only if $\lambda_i x^{-d_i - r} \in \mathfrak{o}_\infty$ for all i. This means that $\deg \lambda_i \leq d_i + r$. This prove that $\{x^j v_i \mid 1 \leq i \leq n,\ 0 \leq j \leq d_i + r\}$ is a $\Bbbk$ basis of $\mathscr{L}(\mathcal{D} + r\mathrm{div}(x)^-)$.

For the last statement suppose that $\sum \lambda_i v_i = 0$ with $\lambda_i \in \Bbbk[x]$ not all zero, then the $x^j v_i$, with $j \leq \deg \lambda_i$, are $\Bbbk$-linear dependent. This is a contradiction since we proved the $\Bbbk$-linear independence for every r.

It remains to prove that the uniqueness of the d_i is independent from the choice of v_i. Suppose that $\{x^j v_i \mid 1 \leq i \leq n,\ 0 \leq j \leq d_i + r\}$ is a basis for $\mathscr{L}(\mathcal{D} + r\mathrm{div}(x)^-)$.

- Fix any $\phi \in (\mathcal{D}^S)^{-1}$, then there exists an r such that $\phi \in \mathscr{L}(\mathcal{D} + r\mathrm{div}(x)^-)$ and then we can write

$$\phi = \sum_{i=1}^{n} \left(\sum_{j=0}^{d_i + r} \mu_i x^j \right) v_i,$$

  and this proves that $(v_i)_i$ is a $\Bbbk[x]$-basis for $(\mathcal{D}^S)^{-1}$.

- Fix any element $\phi \in (\mathcal{D}_S)^{-1}$, then there exist a polynomial $h \in \Bbbk[x]$ such that $\phi \in \mathscr{L}(\mathcal{D} + \mathrm{div}(h)^+)$. If $r = \deg h$, then $r\mathrm{div}(x)^- = \mathrm{div}(h)^-$ and $\mathcal{D} + \mathrm{div}(h)^+ = \mathcal{D} + r\mathrm{div}(x)^- + \mathrm{div}(h)$. Hence $(h^{-1})x^j v_i$, with $0 \leq j \leq d_i + r$ is a $\Bbbk$-basis for $\mathscr{L}(\mathcal{D} + \mathrm{div}(h)^+)$. This proves that $(x^{d_i} v_i)_i$ is a $\mathfrak{o}_\infty$-basis for $(\mathcal{D}_S)^{-1}$.

Since $(v_i)_i$ and $(x^{d_i} v_i)_i$ are related by a diagonal transformation, we can deduce by Corollary 6.1.4 that the d_i's are unique. □

6.1.3 Algorithm for the computation of the Riemann-Roch spaces

We will assume that we are able to compute bases for $\mathcal{D}^S$ and $\mathcal{D}_S$, equivalently we are able to compute integral bases for $Cl(\mathfrak{o}_\infty, \Bbbk(\mathscr{C}))$ and $Cl(\Bbbk[x], \Bbbk(\mathscr{C}))$, and then bases for their ideals and fractional ideals.

Algorithm 8.

INPUT: *A divisor of the curve $\mathscr{C}$.*

OUTPUT: *A $\Bbbk$-basis for $\mathscr{L}(\mathcal{D})$.*

1. *Compute a $\Bbbk[x]$-basis $v'_1, \cdots, v'_n$ of $(\mathcal{D}^S)^{-1}$ and a $\mathfrak{o}_\infty$-basis $w'_1, \cdots, w'_n$ of $(\mathcal{D}_S)^{-1}$;*
2. *Compute $M \in \Bbbk(x)^{n\times n}$ such that $(w'_1, \cdots, w'_n)M = (v'_1, \cdots, v'_n)$;*
3. *Compute the unimodular matrix $T_2 \in \Bbbk[x]^{n\times n}$ and the integers d_i as in Corollary 6.1.3.*
4. *Return the basis $\{x^j v_i \mid 1 \le i \le n,\ 0 \le j \le d_i\}$, or equivalently just the elements $(v_i)_i$ and $(d_i)_i$, where $(v_1, \cdots, v_n) = (v'_1, \cdots, v'_n)T_2$.*

Example

Consider the hyperelliptic curve defined over $\Bbbk = \mathbb{Q}$ given by $y^2 = f(x)$, with

$$f(x) = x(x-1)(x+1)(x-2)(x+3).$$

Let S be the set $\{P_\infty\}$. Then $\mathfrak{o}^S = Cl(\Bbbk[x], \Bbbk(\mathscr{C})) = \Bbbk[x][y]/(y^2 - f(x))$ and the ring $\mathfrak{o}_S = Cl(\mathfrak{o}_\infty, \Bbbk(\mathscr{C}))$. The element y/x^3 is integral over $\mathfrak{o}_\infty$ with minimum polynomial $g(\alpha) = \alpha^2 - g(x)/x^6$. We have also $\mathfrak{o}_S = \mathfrak{o}_\infty[y/x^3]$.

Consider the affine points $P_1 = (1,0)$ and $P_2 = (3,12)$, it is clear that the corresponding ideals in $\mathfrak{o}^S$ are respectively $\mathfrak{p}_1 = (x-1, y)$ and $\mathfrak{p}_2 = (x-3, y-12)$. Consider now the point at infinity P_∞, in order to compute the corresponding prime ideal we have to factorize $(1/x)\mathfrak{o}_S$ in prime ideals. Since $g(y) \equiv y^2 \mod \mathfrak{o}_\infty[y]$ we have that $(1/x)\mathfrak{o}_S$ is a square power of a prime ideal $\mathfrak{q}$ of $\mathfrak{o}_S$. Moreover $\mathfrak{q} = (y/x^3)\mathfrak{o}_S$.

We want to find the smallest l such that $\mathscr{L}(-P_1 - P_2 + lP_\infty)$ has positive dimension, then the intersection $\mathfrak{p}_1\mathfrak{p}_2 \cap \mathfrak{q}^{-l}$ has to be computed. First we have to compute a $\Bbbk[x]$-basis for $\mathfrak{p}_1\mathfrak{p}_2$. A set of generators is

$$\{(x-1)(x-3), (x-3)y, (x-1)(y-12), (y-12)y\},$$

in order to find a basis we can reduced the matrix

$$\begin{pmatrix} (x-1)(x-3) & 0 & -12(x-1) & f(x) \\ 0 & x-3 & x-1 & -12 \end{pmatrix}.$$

First add from the first column $\frac{x-3}{12}$ times the third column and $-\frac{x-1}{12}$ times the second column, we get

$$\begin{pmatrix} 0 & 0 & -12(x-1) & f(x) \\ 0 & x-3 & x-1 & -12 \end{pmatrix}.$$

Then substract the second column from the third, divide by 2 the third column and add $\frac{f(x)}{6(x-1)}$ times the third column from the fourth, we get

$$\begin{pmatrix} 0 & 0 & -6(x-1) & 0 \\ 0 & x-3 & 1 & \frac{f(x)}{6(x-1)} - 12 \end{pmatrix}.$$

Note that $(x-3)$ divides $\frac{f(x)}{6(x-1)} - 12$, then we can erase the first and the fourth columns and we can say that $(y(x-3), y-6x+6)$ is a $\Bbbk[x]$-basis for $\mathfrak{p}_1\mathfrak{p}_2$.

An $\mathfrak{o}_\infty$-basis for $\mathfrak{q}^{-1}$ is clearly given by $\left(\frac{x^3}{y}, 1\right)$, and a $\mathfrak{o}_\infty$-basis for $\mathfrak{q}^{-l}$ is given by $\left(\frac{x^3}{y}\right)^l \left(1, \frac{y}{x^3}\right)$.

Suppose now $l = 3$, then we have

$$(y(x-3), y-6x+6) = \left(x, \frac{x^4}{y}\right) \cdot \begin{pmatrix} 0 & -\frac{6(x-1)}{x} \\ \frac{f(x)(x-3)}{x^4} & \frac{f(x)}{x^4} \end{pmatrix}.$$

The previous matrix is not reduced, but we can reduce it by adding $-(x-3)$ times the second column to the first, i.e. multiply on the right by the matrix, then the matrix becomes

$$\begin{pmatrix} -\frac{6(x-1)(x-3)}{x} & -\frac{6(x-1)}{x} \\ 0 & \frac{f(x)}{x^4} \end{pmatrix}.$$

It is reduced. The indices corresponding to the degree of the functions in the diagonal are $-d_1 = 1$ and $-d_2 = 1$. So that d_1 and d_2 are both negative, then the Riemann-Roch space $\mathscr{L}(-P_1 - P_2 + 3P_\infty)$ has dimension 0.

Suppose $l = 4$, then we get

$$(y(x-3), y-6x+6) = \left(x^2, \frac{y}{x}\right) \cdot \begin{pmatrix} 0 & -\frac{6(x-1)}{x^2} \\ x(x-3) & x \end{pmatrix}.$$

The matrix is not reduced. multiply on the right by the matrix T_2 and we get

$$\begin{pmatrix} \frac{6(x-1)(x-3)}{x^2} & -\frac{6(x-1)}{x^2} \\ 0 & x \end{pmatrix},$$

a reduced matrix. Note that $-\frac{6(x-1)(x-3)}{x^2}$ has degree 0 and x has degree 1, then $d_1 = 1, d_2 = -1$. The base change gives us

$$(y(x-3), y-6x+6)\, T_2 = ((x-3)(x-1), y-6x+6).$$

Then a basis for $\mathscr{L}(-P_1 - P_2 + 4P_\infty)$ is given by the rational function $(x-3)(x-1)$.

Remark. Note that $\operatorname{div}(x)^- = 2P_\infty$, then with this two computation we can recover all the bases for the space $\mathscr{L}(-P_1 - P_2 + rP_\infty)$, with $r \in \mathbb{Z}$, using Theorem 6.1.6. In order to avoid two computations we can use Theorem 6.1.6 with a function that has a unique pole in P_∞ instead of x, but in this case it not exist, indeed for any point $P = (a, b)$ on the curve we have

$$(x-a, y-b) = (1, x^3/y)\begin{pmatrix} x-a & -b \\ 0 & f(x)/x^3 \end{pmatrix},$$

the matrix is reduced and it has indices $d_1 = -1, d_2 = -2$, then $\mathscr{L}(-P + P_\infty)$ has dimension 0.

Running time

As already seen in 6.1.5, for a fixed closed point we can associate a prime ideal in $\mathfrak{o}^S$ or $\mathfrak{o}_S$. We can use two different types of representation of a divisor:

i) the first is the *ideal representation*, it associates a divisor $\mathcal{D}$ to (the inverse of) the two ideals $\mathcal{D}^S$ and $\mathcal{D}_S$, as already seen in 6.1.5;

ii) the second is called *free representation*, here every divisor is represented by the power product of the prime ideals corresponding to the points in $\mathrm{supp}(\mathcal{D})$.

Clearly we can recover easily the ideal representation from a free representation (just multiplying out the prime ideal). Conversely, in order to recover a divisor in free representation from a divisor in ideal representation, it requires a factorization of the ideals $\mathcal{D}^S$ and $\mathcal{D}_S$. This change requires a polynomial running time in n, $h(\mathcal{D})$ and C_f, where

$$h(\mathcal{D}) := \deg(\mathcal{D}^+) + \deg(\mathcal{D}^-)$$

is the height of the divisor $\mathcal{D}$ and

$$C_f := \max\{\lceil \deg_x(a_i)/i \rceil | 1 \leq i \leq n\}$$

where $f(x, y) = y^n + a_1 y^{n-1} + \cdots + a_n \in \Bbbk[x, y]$ is the affine equation of the curve.

Moreover the cost of the divisor arithmetic is also polynomial in n, $h(\mathcal{D})$ and C_f. Therefore the running time for the computation of the Riemann-Roch space is polynomial in n, $h(\mathcal{D})$ and C_f, in fact the size of the entries of the matrix M is polynomial in n, $h(\mathcal{D})$ and C_f.

6.2 Divisor reduction

Recall from the introduction of the chapter that, in order to compute the maximal reduction of a divisor $\mathcal{D}$, we are looking for the largest integer r such that the space $\mathscr{L}(\mathcal{D} - r\mathcal{A})$ still has positive dimension and then obtain the elementary reduction along $\mathcal{A}$. In order to avoid exponential time computations, the elementary reduction should only be performed for divisor of small height.

We can write $\mathcal{D} = \sum_{i=0}^m 2^i \mathcal{D}_i$ where the $\mathcal{D}_i$ are sum or subtraction of single distinct points. It is possible to avoid the time computation issue using double-and-add tricks if the number of points in $\mathcal{D}_i$ is not too large.

From a theoretical point of view we can compute the reduction after each addiction (or subtraction) in the double-and-add algorithm, then we can write the maximal reduction of a divisor $\mathcal{E} = \sum_{i=0}^{m} 2^i \mathcal{E}_i$ to be

$$\mathcal{E} = 2^{m-j}\widetilde{\mathcal{E}}_{m-j} + \sum_{i=0}^{m-j-1} 2^i \mathcal{E}_i + \left(\sum_{i=m-j}^{m} 2^i r_i \right) \mathcal{A} - \sum_{i=m-j}^{m} 2^i \mathrm{div}(a_i), \tag{6.1}$$

where j goes from -1 to m, $\mathcal{E}_{m+1} := 0$. More precisely we can write

$$\mathcal{E}_m = \widetilde{\mathcal{E}}_m + r_m \mathcal{A} - \mathrm{div}(a_m),$$

the elementary reduction of $\mathcal{E}_m$, then we double this expression and we can add $\mathcal{E}_{m-1}$ and compute the reduction

$$\begin{aligned} 2\mathcal{E}_m + \mathcal{E}_{m-1} &= 2\widetilde{\mathcal{E}}_m + \mathcal{E}_{m-1} + 2r_m \mathcal{A} - 2\mathrm{div}(a_m) \\ &= \widetilde{\mathcal{E}}_{m-1} + (2r_m + r_{m-1})\mathcal{A} + 2\mathrm{div}(a_m) + \mathrm{div}(a_{m-1}). \end{aligned}$$

We can do it inductively and obtain the formula 6.1. Note that the elementary reduction of $2\widetilde{\mathcal{E}}_{m-j} + \mathcal{E}_{m-j-1}$ is $\widetilde{\mathcal{E}}_{m-j-1} + (r_{m-j-1})\mathcal{A} - \mathrm{div}(a_{m-j-1})$.

Then we get

$$\mathcal{E} = \widetilde{\mathcal{E}}_0 + \left(\sum_{i=0}^{m} 2^i r_i \right) \mathcal{A} - \sum_{i=0}^{m} 2^i \mathrm{div}(a_i). \tag{6.2}$$

For a computational point of view the size of the orders of $\mathcal{E}$ contributes only logarithmically, but the number of places in each $\mathcal{E}_i$ is still a problem.

Now, return to our divisor $\mathcal{D} = \sum_{i=0}^{m} 2^i \mathcal{D}_i$, before applying the previous procedure, we can reduce every divisor $\mathcal{D}_i$ in order to decrease the number of places. If the divisor $\mathcal{D}_i$ is equal to $\sum_{k=1}^{t} P_k^i$, we can sum up the point P_r successively, applying the elementary reduction after each step, namely

$$\begin{aligned} \mathcal{D}_i &= (P_1^i + P_2^i) + \sum_{k=3}^{t} P_k^i \\ &= (\mathcal{P}_2^i + P_3^i) + \sum_{k=4}^{t} P_k^i + \ell_2 \mathcal{A} - \mathrm{div}(b_{i,2}) \\ &= (\mathcal{P}_3^i + P_4^i) + \sum_{k=5}^{t} P_k^i + \sum_{j=1}^{3} \ell_j \mathcal{A} - \sum_{j=1}^{3} \mathrm{div}(b_{i,j}) \\ &\vdots \\ &= \mathcal{P}_t^i + \sum_{j=1}^{t} \ell_j - \sum_{j=1}^{t} \mathrm{div}(b_{i,j}) \end{aligned} \tag{6.3}$$

where $\ell_1 = 0$ and $b_{i,1} = 1$. Write $l_i = \sum_{j=1}^{t} \ell_j$, $b_i = \prod_{j=1}^{t} b_{i,j}$ and $\mathcal{D}'_i = \mathcal{P}_t^i$, then we can write

$$\mathcal{D}_i = \mathcal{D}'_i + l_i \mathcal{A} - \mathrm{div}(b_i).$$

Now we can apply the procedure for 6.2 to $\mathcal{E} = \sum 2^i \mathcal{D}'_i$ and we get

$$\mathcal{D} = \widetilde{\mathcal{E}}_0 + \left(\sum_{i=0}^{m} 2^i (r_i + l_i) \right) \mathcal{A} - \sum_{i=0}^{m} 2^i \mathrm{div}(a_i \cdot b_i).$$

The choice of r can be done in two ways. The first is to choose the integer r such that $g \leq \deg(\mathcal{D} - f\mathcal{A}) < g + \deg(\mathcal{A})$, it gives a reduced divisor $\widetilde{\mathcal{D}}$ such that $g \leq \deg(\widetilde{\mathcal{D}}) < g + \deg(\mathcal{A})$. The second is to choose the integer r such that $0 < \dim(\mathcal{D} - r\mathcal{A}) \leq \deg(\mathcal{A})$, it gives a divisor $\widetilde{\mathcal{D}}$ such that $\deg(\widetilde{\mathcal{D}}) < g + \deg(\mathcal{A})$. The latter return the maximal reduced divisor, but several tries of values of r might be necessary (in this case we can use the binary search method).

In case $\mathcal{A} = \mathrm{div}(x)^-$ then, because of theorem 6.1.6, the maximal r is given by d_1, hence no tries are required.

We can sum up in the next Algorithm.

Algorithm 9.

INPUT: *The divisors $\mathcal{D}$ and $\mathcal{A}$.*

OUTPUT: *A divisor $\widetilde{\mathcal{D}}$, an integer $r \in \mathbb{Z}$ and element $a_i, b_i \in \Bbbk(\mathscr{C})^\times$ such that $\mathcal{D} = \widetilde{\mathcal{D}} + r\mathcal{A} - \sum_i 2^i \mathrm{div}(a_i \cdot b_i)$.*

1. *Compute m and divisors $(\mathcal{D}_i)_i$, whose orders have absolute value 1, such that $\mathcal{D} = \sum_{i=0}^m 2^i \mathcal{D}_i$.*
2. *Compute the divisors $\mathcal{D}'_i$ using the elementary reduction after each addition of a point of $\mathcal{D}_i$ as we seen in 6.3, and obtain the representation $\mathcal{D}_i = \mathcal{D}'_i + l_i\mathcal{A} - \mathrm{div}(b_i)$.*
3. *Put $\mathcal{E} = \sum 2^i \mathcal{D}'_i = \sum 2^i \mathcal{E}_i$. Let $\mathcal{E}_{m+1} = 0$ and compute the elementary reduction of $2\widetilde{\mathcal{E}}_{m-j} + \mathcal{E}_{m-j-1}$ inductively for $-1 \leq j \leq m$. So that $2\widetilde{\mathcal{E}}_{m-j} + \mathcal{E}_{m-j-1} = \widetilde{\mathcal{E}}_{m-j-1} + (r_{m-j-1})\mathcal{A} - \mathrm{div}(a_{m-j-1})$ holds.*
4. *Let $\widetilde{\mathcal{D}} = \widetilde{\mathcal{D}}_0$ and $r = \sum_i 2^i (r_i + l_i)$. Return the divisor $\widetilde{\mathcal{D}}$, the integer r and the rational functions a_i and b_i.*

Conclusion

As we said in the introduction, the aim of this thesis was to study methods for the implementation of the addiction law on Jacobians of algebraic curves.

We showed explicitly formulæ for the addiction on elliptic curves. In this context it is of the utmost importance, for a computational point of view, to find algorithms which let us save even one field operation. The best algorithm found is related to Edwards elliptic curves: it needs 7**M** + 5**S** for the addition and only 3**M** + 4**S** for a doubling.

In the last decades, cryptographic studies found developments on the use of algebraic curves of small genus, both hyperelliptic and not. In this thesis we have seen methods for the implementation of the addition on Jacobian of non-hyperelliptic curves of genus 3, of superelliptic of genus 3 and 4, and, using Mumford representation, of hyperelliptic curves of arbitrary genus.

Studies of the addition law on these particular curves lead to search for a method for the implementation of the addition law on Jacobians of generic curves. We presented the method described by Heß. The natural continuation of this work would be to implement this general algorithm.

Acknowledgements

I would like to express my special thanks to my advisor, Damien Robert, who has supported me during this work.
I would also like to express my acknowledgements to the people of ALGANT: its professors, staff, and my fellow students for the good time in this two years.

Bibliography

[AM69] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to commutative algebra*. Vol. 2. Addison-Wesley Reading, 1969.

[Are+11] Christophe Arene et al. "Faster computation of the Tate pairing". In: *Journal of number theory* 131.5 (2011), pp. 842–857.

[Bas+05] Abdolali Basiri et al. "The arithmetic of Jacobian groups of superelliptic cubics". In: *Mathematics of computation* 74.249 (2005), pp. 389–410.

[Ber+08] D. Bernstein et al. "Twisted edwards curves". In: *Progress in Cryptology–AFRICACRYPT 2008* (2008), pp. 389–405.

[BL07a] Daniel J Bernstein and Tanja Lange. "Faster addition and doubling on elliptic curves". In: *Advances in cryptology–ASIACRYPT 2007*. Springer, 2007, pp. 29–50.

[BL07b] D.J. Bernstein and T. Lange. *Explicit-formulas database*. 2007. URL: `http://hyperelliptic.org/EFD`.

[Cai10] Maurizio Cailotto. *CAP - Curve Algebriche Piane*. 2010. URL: `http://www.math.unipd.it/~maurizio/cap/`.

[Coh+10] Henri Cohen et al. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman and Hall/CRC, 2010.

[Edw07] Harold Edwards. "A normal form for elliptic curves". In: *Bulletin of the American Mathematical Society* 44.3 (2007), pp. 393–422.

[Eng99] Andreas Enge. *Elliptic curves and their applications to cryptography: an introduction*. Kluwer Academic Pub, 1999.

[FOR07] S. Flon, R. Oyono, and C. Ritzenthaler. *Fast addition on non-hyperelliptic genus 3 curves*. World Scientific, 2007.

[Ful69] W. Fulton. *Algebraic curves*. W.A. Benjamin, 1969.

[Heß02] Florian Heß. "Computing Riemann–Roch spaces in algebraic function fields and related topics". In: *Journal of Symbolic Computation* 33.4 (2002), pp. 425–445.

[JTV10] M. Joye, M. Tibouchi, and D. Vergnaud. "Huffs model for elliptic curves". In: *Algorithmic Number Theory* (2010), pp. 234–250.

[Lan05] T. Lange. “Formulae for arithmetic on genus 2 hyperelliptic curves”. In: *Applicable Algebra in Engineering, Communication and Computing* 15.5 (2005), pp. 295–328.

[Men+96] Alfred Menezes et al. *An elementary introduction to hyperelliptic curves.* Faculty of Mathematics, University of Waterloo, 1996.

[Mil91] J.S. Milne. *Abelian varieties.* 1991. URL: `http://www.jmilne.org/math/CourseNotes/av.html`.

[Mor93] Carlos Moreno. *Algebraic curves over finite fields.* Vol. 97. Cambridge University Press, 1993.

[MRM70] David Mumford, Chidambaran Padmanabhan Ramanujam, and Yuri Ivanovich Manin. *Abelian varieties.* Vol. 48. Oxford Univ Press, 1970.

[Mum69] David Mumford. “Varieties defined by quadratic equations”. In: *Questions on Algebraic Varieties (CIME, III Ciclo, Varenna, 1969)* (1969), pp. 29–100.

[Mum75] David Mumford. *Curves and their Jacobians.* University of Michigan Press Ann Arbor, 1975.

[Mum84] David Mumford. *Tata lectures on theta II.* Vol. 43. Progress in Mathematics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Boston, MA: Birkhäuser Boston Inc., 1984, pp. xiv+272. ISBN: 0-8176-3110-0.

[Mum99] David Mumford. *The red book of varieties and schemes.* Vol. 1358. Lecture Notes in Mathematics. Second, expanded edition. Includes the Michigan lectures (1974) on curves and their Jacobians. With contributions by Enrico Arbarello. Springer, 1999.

[Wal50] Robert John Walker. *Algebraic curves.* Vol. 642. Princeton University Press Princeton, 1950.