On the Jacobian Varieties of Picard curves: explicit Addition Law and Algebraic Structure

Jorge Estrada Sarlabous*
Ernesto Reinaldo Barreiro
Jorge Alejandro Piñeiro Barceló
Department of Geometry and Combinatorics.
ICIMAF. Ministry of Sciences.
Calle E No.309, esquina a 15
Vedado 4, C. Habana. Cuba.

Abstract

In this paper a system of coordinates for the effective divisors on the Jacobian Variety of a Picard curve is presented. These coordinates possess a nice geometric interpretation and provide us with an unifying environment to obtain an explicit structure of algebraic variety on the Jacobian as well as an efficient algorithm for the addition of divisors.

1 Introduction

In the middle '80, D. Mumford laid a corner stone for the study of families of special curves and their Jacobian Varieties. In his book "Tata Lectures on Theta II", [15], he presented a coordinate system on an Zariski open subset of the Jacobian Variety of an hyperelliptic curve, which facilitated him and several authors obtainig many concrete and explicit information: a projective model of hyperelliptic jacobians, a characterization of period matrices arising from hyperelliptic curves, algebraic and differential identities for hyperelliptic theta functions, among others. In particular, D. Cantor [1] used these coordinates to develop an algorithm to compute the addition of divisors on hyperelliptic jacobians .
More recently, another special families of curves has been focused with increasing interest: the Picard curves (and a generalization containing both Picard and hyperelliptic curves, the

*Supported partially by a DFG grant

n-gonal cyclic curves, also called cycloelliptic or superelliptic). These curves play a central role in some approaches to generalizations of Hilbert problems 7, 12, 21 and 22, in special differential equations and many other researches [4], [5], [6], [9], [10], [11], [12].
The authors felt motivated to find out, to which extent the Picard curves (or more general, the n-gonal cyclic curves) could share with the hyperelliptic curves the nice property of making things to become explicit. In this paper, we show our first results in this direction.
We wish to thank R.-P. Holzapfel for his valuable comments, discussions and encouragement.

2 Preliminaries

Let k be an arbitrary field. we write $\overline{k}$ for its algebraic closure. The affine space A_k^n consists of all the points $\{(x_1, x_2, ..., x_n)\ x_i \in \overline{k}\}$. Points in the projective space P_k^n consist of equivalence classes of points in $A_k^{n+1} \setminus \{(0, 0, .., 0)\}$ where $(x_0, x_1, .., x_n)$ and $(y_0, y_1, .., y_n)$ are equivalent if there is $c \in \overline{k}$ $(c \neq 0)$, such that $x_i = cy_i$ for all $i = 0, 1, .., n$. Note that A_k^2 is naturally embedded in P_k^2 by the map $(x, y) \to (x, y, 1)$.
If $G \in k[x, y]$ is an homogeneous polynomial then, G define an algebraic subset of P_k^2. If H is other polynomial, we write $G = H$ if G and H are equivalent up to a non-constant factor. An irreducible plane projective curve of degree n is defined as the zero-set of a given irreducible, homogeneous polynomial of the same degree. We say that a curve is non-singular if its polynomial has a well defined tangent in every point. We let ∞ denote a fixed point of C.
We use the notation of Fulton [7]. A divisor D on C is a formal sum $D = \sum_{P \in C} n_P P$ of points in C where $n_P = ord_P(D)$ is an integer and $n_P = 0$ for all but a finite number of points P. The set of points $supp(D) = \{P \in C / n_P \neq 0\}$ is called the support of D. The degree of D is $\sum_{P \in C} n_P$ and D is effective if $n_P \geq 0$ for all P. We say $D \succeq D_1$ if $D - D_1$ is effective and put $D' = D - n_\infty \infty$. A divisor D is called affine if $D = D'$.
The set of all divisors on C form an additive group $Div(C)$ of which the divisors of degree t form a subset $Div^t(C)$ and $Div^0(C)$ is a subgroup. $Div^{+,t}(C)$ is the subset of efective divisor of $Div^t(C)$
The field $k(C)$ of rational functions on C is the field of fractions of the graded ring $k[x, y, z]/(F)$, where F is the homogeneous polynomial definig C. The local ring $\mathcal{O}_{C,P}$ of C at P is the collection of rational functions defined at P. If P is non-singular then, $\mathcal{O}_{C,P}$ is a discrete valuation ring and there exist a local parameter $t \in \mathcal{O}_{C,P}$, such that every $z \in \mathcal{O}_{C,P}$ can be written as $z = ut^n$ where u is a unit and $n \in \boldsymbol{Z}$ is the order of z at P, written $ord_P^C(z)$. With help of this representation we can express every $z \in K(C)$ as $z = \sum_{i=0}^{l-1} a_i t^i + m_l$ $(a_i \in K(C)$ and $m_l \in \{t^l K(C)\})$. To require z to have order at least l at P is then equivalent to the system of equations $a_i = 0$ (for $i = 0$ to $l - 1$), which are linear in the coefficients of z.
The divisor of $f = F_1/F_2$ is uniquely defined by :

$$(f) = \sum_{P \in C} ord_P^C(f)P$$

where :

$$ord_P^C(f) = ord_P^C(F_1) - ord_P^C(F_2)$$

It follows from Bezout's theorem that every such divisor has degree 0. A divisor of the form (f) for some rational function f is called principal. We write $\mathcal{P}$ for the subgroup of $Div^0(C)$ of principal divisors and two divisors D and D_1 are called linearly equivalent ($D \cong D_1$) whenever D and D_1 are in the same coset of $Div^0(C)/\mathcal{P}$ i.e. when there is a rational function f such that $(f) + D = D_1$.
For any divisor D one define :

$$\mathcal{L}(D) = \{f \in K(C)/(f) \geq -D\} \cup \{0\}$$

Let $\Omega_k(C)$ be the space of differentials of $k(C)$ over k. Let $\omega \in \Omega$ be a differential ($\omega \neq 0$) and $P \in C$. If we choose a local parameter $t \in \mathcal{O}_{C,P}$ we may write $\omega = fdt$ for some $f \in k(C)$, and so define $ord_P^C(\omega) = ord_P^C(f)$.
Similar to (f) the divisor of ω is uniquely defined by :

$$(\omega) = \sum_{P \in C} ord_P^C(\omega) P$$

and to any divisor D we may associate :

$$\Omega(D) = \{\omega \in \Omega/(\omega) \geq D\} \cup \{0\}$$

If we put $l(D) = dim_k(\mathcal{L}(D))$ and $\delta(D) = dim_k(\Omega(D))$ then the Riemann-Roch Theorem states :

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

where $g_C = \delta(0)$ is called the genus of C.

Definition 2.1 *(Cyclic n-gonal curves.)*
An algebraic curve C defined over a field k is called $n-gonal$ cyclic is there exists a non trivial $\sigma \in Aut_k(C)$, such that $\sigma^n = id_C$, and $C/(\sigma) \cong P_k^1$.

Let $\bar{k}$ be an algebraic closed extension of k and C/k be an $n - gonal\ cyclic\ curve$ then, $(C \otimes_k \bar{k})/(\sigma) \cong P_{\bar{k}}^1$ and if $char(k) = 0$ or $n \not| \ char(k) \neq 0$, the field of rational functions of $C/\bar{k}$, $R(C)$ is a *Galois* extension of the field of rational functions of $P_{\bar{k}}^1$, $\bar{k}(x)$, therefore (see [4], [6]) there exists an element $y \in R(C)$, such that $\sigma(y) = \xi y$, $R(C) = \bar{k}(x)(y)$ and $y^n \in \bar{k}(x)$, for ξ primitive n-th root of unity. So, $C/\bar{k}$ has the affine model:

$$C : y^n = p_m(x) = a_0(x - a_1)^{m_1} \ldots (x - a_s)^{m_s}, \sigma(x, y) = (x, \xi y)$$

with $m_j \in Z$, $a_j \in \bar{k}$, $a_i \neq a_j$ for $i \neq j$, $m = \sum m_j$. Here, we may assume that $n \not| \ m$ (otherwise, we can construct a birational equivalent affine model of $C/\bar{k}$ with this property). If $n > char(k)$, $m_j = 1$ (i.e., $p_m(x)$ has not double roots) and $m = n+1$, the projective model of C, $C_h : z^{m-n}y^n = z^m p_m(x/z)$ is non singular. Since there is not wild ramification in this case, by the Riemman-Hurwitz formula we can compute the genus of $C : g(C) = n(n-1)/2$.

Local parameters 2.1 *Let C be a $n-gonal$ cyclic curve, with non singular affine model as above ($m = n+1$).*
At $P = (x_0, y_0), y_0 \neq 0$, $t = x - x_0$ is a local parameter.
At $P = (a_j, 0)$, $t = y$ is a local parameter
At the point $\infty = (0 : 1 : 0)$ on $zy^n = \prod_{i=1}^{m}(x - za_i)$, $t = y^{n-1}/x^n$ is a local parameter

Definition of Picard curves 2.1 *A Picard curve is a genus three trigonal curve, i.e., $n = 3, m = 4$.*
In what follows we deal with non-singular Picard curves, so we assume $char(k) \neq 2, 3$.

More details can be found in [5] and [6].

3 Reduction algorithm

Let C be a non-singular cyclic curve of degree n ($n > 2$) with an affine model $y^{n-1} = p_n(x)$ and $D \in J(C)$. Using the fact: $(x - x_P) = \sum_{i=0}^{n-2} \sigma^i P - (n-1)\infty$ we may obtain an equivalent divisor of the form $\sum_{i=1}^{a} P_i - a\infty$. Such a divisor is called a semireduced representant and it is called reduced representant if $a \leq g_C$. From Riemann-Roch theorem follows that every divisor D has a reduced representant. Given a divisor D, the problem of obtaining a reduced equivalent is known as The Reduction Problem. A general solution can be found in [13], nevertheless, in the case of a non-singular cyclic curve, we present in this paper a solution admiting a nice geometric interpretation. In the particular case of Picard curves, we obtain an algorithm for the reduction problem using $O(deg(D))$ operations.
Let's begin assigning to every efective divisor D with $D' \in Div^{+,t}$, $v_D \in k[x, y]$ of lowest degree at ∞ such that $(v_D)_0 \succeq D'$ and :

$$ord_\infty(v_D) \geq \begin{cases} 0 & \text{if } t \geq m(m+3)/2 \\ m(m+3)/2 - t & \text{if } t < m(m+3)/2 \end{cases}$$

where m is the degree of v_D and :

$$deg_\infty(\sum_{i,j} a_{ij} x^i y^j) = max_{i,j}(nj + (n-1)i)$$

for every $\sum_{i,j} a_{ij} x^i y^j$ polynomial function over C.

The vector space of plane curves of degree m has dimension $m(m+3)/2$ over k, so v_D always exist, and by definition, if there are two curves through P_i its difference has lower degree at ∞. Hence v_D is unique.

Let's see how v_D above permits us to translate the reduction problem to the computation of several curve intersections.

If $t \leq (n-1)(n+2)/2$ then $m < n$ and we can assure that $gcd(C, v_D) = 1$, since C is irreducible.

$$(v_D) = D' + D_1 - (ndeg(v_D) - ord_\infty(v_D))\infty \tag{1}$$

where $deg(D_1) \leq mn - m(m+3)/2$. Due to $(2n-3)^2 - (2n-4)(2n+2) < 0$ if $n > 2$ we have $mn - m(m+3)/2 < (n-2)(n+1)/2$ and so $deg(v_{D_1}) \leq n-2$ and :

$$(v_{D_1}) = D_1 + D_2 - (ndeg(v_{D_1}) - ord_\infty(v_{D_1}))\infty \tag{2}$$

Substracting (1) and (2) we have :

$$D' - (ndeg(v_D) - ord_\infty(v_D))\infty \cong D_2 - (ndeg(v_{D_1}) - ord_\infty(v_{D_1}))\infty$$

On the other hand, from the fact that the function :

$$F(m) = mn - m(m+3)/2 - (n-1)(n-2)/2$$

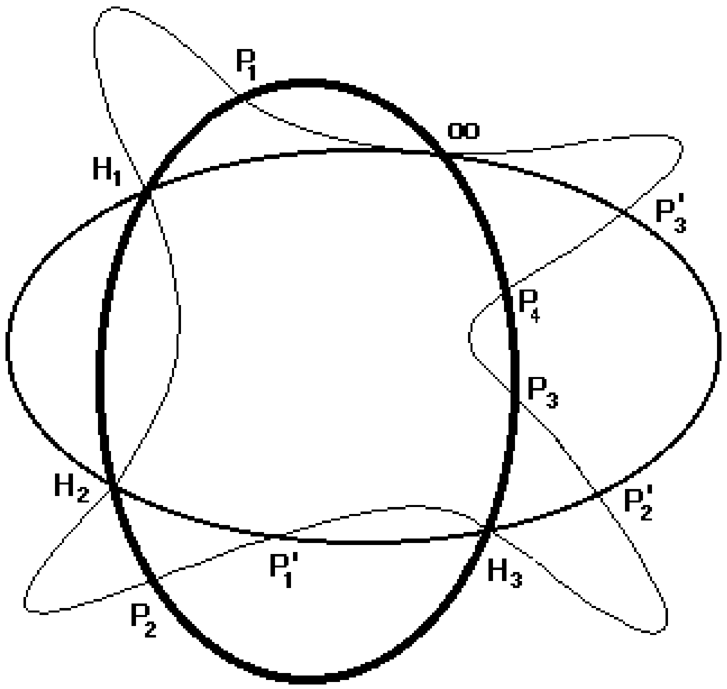
has its zeros in $m = n-1$, $m = n-2$ follows that if $m \leq n-2$ is $F(m) \leq 0$ so $deg(D_2) \leq (n-1)(n-2)/2 = g_C$.

An algorithm for reduction could be the following. Take an effective divisor D, if $deg(D') \leq g_C$ we have finished, and if it not the case, take an efective affine divisor D_0 ($D \succeq D_0$) with $g_C < deg(D_0) \leq (n-1)(n+2)/2$ and put :

$$D_a := D - D_0 + D_2 + (ndeg(v_{D_0}) - ord_\infty(v_D) - ndeg(v_{D_1}) + ord_\infty(v_{D_1}))\infty$$

D_0 , D_2 are affine with $deg(D_0) > deg(D_2)$ hence $deg(D'_a) < deg(D')$ and return to the first step with $D := D_a$.

Let's illustrate the reduction algorithm for the case of the reduction of a degree 4 effective divisor on a Picard curve to an linearly equivalent divisor of degree 3: Put $D_0 = P_1+P_2+P_3+P_4$ and consider the conic v_{D_0}, which interpolates the Picard curve C at $D_0+\infty$. This conic interpolates C in three further points H_1, H_2 and H_3. Set $D_1 = H_1 + H_2 + H_3$ and consider the conic v_{D_1} interpolating C at $D_1 + 2\infty$. The conic v_{D_1} cuts C in three additional points P'_1, P'_2 and P'_3, and the divisor $D_2 = P'_1+P'_2+P'_3$ is the desired reduction of D_0.



Geometric interpretation of the Reduction Algorithm

In the general case, the algorithm defines a sequence of divisors $D_0, D_1, D_2, .., D_{3s+2}$ such that :

$$D_{3s+2} - (ndeg(v_{D_{3s+1}}) - ord_\infty(v_{D_{3s+1}}))\infty \cong D_{3s} - (ndeg(v_{D_{3s}}) - ord_\infty(v_{D_{3s}}))\infty$$

The sequence is finite, so this procedure give us a solution for the reduction problem, nevertheless, the computation of D_i involve factorizations in each step from v_{3i} to v_{3i+1} and from v_{3i+1} to v_{3i+2} , and this may be computationally expensive. With the objetive to give to the sequence D_i a more implicit treatment we associate to D in a natural way the polynomial :

$$u_D = \prod_{i=1}^{s}(x - x_i)$$

with $D' = \sum_{i=1}^{s} P_i(x_i, y_i)$ and the polynomial :

$$w_D = R_y(v_D, C)/u_D$$

where $R_y(*,*)$ denotes the resultant with respect to y.
We denote $(D) = (u_D, v_D, w_D) \in k[x] \times k[x,y] \times k[x]$.

Suppose now that C is a Picard Curve, that is $g_C = 3$ and $deg(C) = 4$. We will concentrate in what follows in efective affine divisors D_{3i} of degree 4 and put $D_{3i+3} := D_{3i} + E_i$ to form the sequence D_i associated to D.
For D effective, the algorithm will consist in the iteration of the following steps :
1)Take $D_0 \preceq D$ (effective and affine of degree four). Put $D := D \setminus D_0$.
2)Compute (D_0).
3)If D_0 is generic then, compute (D_1) and (D_2) from (D_0) after lemma 3.3 and lemma 3.5.
4)Take a new divisor $E_1 = \alpha P_1 + \beta P_1' \preceq D$ of degree $4 - deg(u_2)$. If this E_1 does not exist then finish.
5)If $D_2 + E_1$ is generic then, based on (D_2) compute $(D_2 + E_1)$ which represents the coordinates of an effective divisor (D_3) of degree 4 and return to step 1) with $(D_0) := (D_3)$.

With help of Lemma 3.2 we find that non-generic cases are easier than generic ones, since in these cases we may explicitly compute the coordinates of the points, without factorization. lemma 3.1 give a usefull relationship between $v(D)$ and D that characterize non-generic cases.

Lemma 3.1 *Given an effective divisor D of degree 4 the following propositions are equivalent :*

i) $v(D)$ is linear or factorizes in linear factors.

ii) there exist among $P_i \in Supp(D + \infty)$ three collinear points.

iii) $v(D) = a_{20}x^2 + a_{10}x + a_{00} + a_{11}xy + a_{01}y$ and $a_{00}a_{11}^2 - a_{10}a_{01}a_{11} + a_{20}a_{01}^2 = 0$.

Proof: ii)$\Rightarrow$ i) If $P_1 + P_2 + P_3 \in Supp(D + \infty)$ and $(r)_0 \succeq P_1 + P_2 + P_3$ for some line r then, r and $v(D)$ have more than two points in common (counting multiplicity) because $deg(v(D)) > 1 \Rightarrow ord_\infty(v(D)) \geq 5 - deg(D')$. By Bezout Theorem r divides $v(D)$.

i)$\Rightarrow$ iii) If $deg(v(D)) = 1 \Rightarrow a_{20} = a_{11} = 0 \Rightarrow$ iii). If $deg(v(D)) > 1$ we have already seen $ord_\infty(v(D)) \geq 1$ so $v(D) = r_1 r_2$ with $ord_\infty(r_1) \geq 1$. This imply $r_1 = (x - \dot{x})$ with $a_{20}\dot{x}^2 + a_{10}\dot{x} + a_{00} = a_{11}\dot{x} + a_{01} = 0$, so :

$$R_x(a_{20}x^2 + a_{10}x + a_{00}, a_{11}x + a_{01}) = a_{00}a_{11}^2 - a_{10}a_{01}a_{11} + a_{20}a_{01}^2 = 0$$

iii)$\Rightarrow$ ii) If $a_{11} = a_{20} = 0$, ii) is clear. If $a_{11} = a_{01} = 0$ then :

$$v(D) = a_{20}x^2 + a_{10}x + a_{00} = r_1 r_2$$

Else, it can be shown :

$$v(D) = (a_{20}x + a_{11}y + a_{10} - a_{20}a_{01}/a_{11})(x + a_{01}/a_{11}) = r_1 r_2$$

In any case $Supp(D + \infty)$ has five points, so at least three of then belong to r_1 or to r_2. $\square$

From lemma 3.1 we obtain $deg_\infty(v_{3i}) < 8$ and by (1) is $deg(D_{3i+1}) < deg(D_{3i}) = 4$. Furthermore, if $deg(v_{3i}) > 1$ the degree at ∞ of v_{3i} is not less than 6 so $deg(D_{3i+1}) > 1$ and we can show $v_{3k+2} = v_{3k+1}$ as follows :

If $deg(u_{3k+1}) = 2 \Rightarrow deg(v_{3k+1}) = deg(v_{3k+2}) = 1$ and so $v_{3k+1} = v_{3k+2}$. If the points in support of D_{3k+1} are collinear, by lemma 3.1 there exist three points P_1, P_2, P_3 in $Supp(D_{3i})$ that belong to $Supp((x - \dot{x})_0)$, so $v_{3i+1} = (x - \dot{x})(x - x_4)$ with $P_4 = D_{3i} - (P_1 + P_2 + P_3)$ and so $deg(u_{3k+1}) = 2$. That is, if $deg(u_{3k+1}) = 3$, the points in support of D_{3k+1} are not collinear and $deg(v_{3k+2}) = deg(v_{3k+1}) = 2$, hence $v_{3k+1} = v_{3k+2}$.

Lemma 3.2 *Suppose that we know E_1 and E_2 in the sequence D_i associated to an effective divisor D. If $deg(v_0) > 1$, $deg(v_3) > 1$ and $Supp(D_5)$ have a pair of conjugate then, we may compute D_5 and D_6 without making any factorization in each of the following cases :*

a) We know the vectors (D_i) for $i = 0$ to 5.

b) we have (D_5) and explicitly know D_3.

Proof:

$$D_5 = P + \sigma P + Q$$

$$v_5 = v_4 = (x - x_P)(x - x_Q)$$

$$D_4 = \sigma^2 P + \sigma Q + \sigma^2 Q$$

$$v_3 = r_3(x - x_Q)$$

We obtain the x-coordinate of $\sigma^2 P$ as the root of the linear equation $u_5/v_5 = 0$ and the y-coordinate is obtained from $r_3(\sigma^2 P) = 0$. In order to find Q we proceed as follows :

1) Take the value x_Q as the root of the linear polynomial v_5^2/u_5.

2) If we explicity know D_3 take the point in D_3 that does not belong to r_3 and finish. Else, supose that Q_σ is the set of affine points of C over x_Q then, take the set :

$$S = Q_\sigma \cap (Supp(E_1) \cup Supp((v_2)_0))$$

$Q \in S$ so, $0 < card(S) < 4$ and if L is a point of $S \setminus \{Q\}$, $L \in D_3 \Rightarrow r_3(L) = 0$.

3) If $card(S) = 3$ and v_2 does not depend on y then for $k \neq 3p$ is :

$$D_2 = T + \sigma^k T + R$$

If $T \neq Q$ then $(r_3)_0 \succeq T + \sigma^k T \Rightarrow \sigma^2 P = \infty$ so, $T = Q$, $r_3(\sigma^k Q) = 0$ and :

$$D_2 = Q + \sigma^k Q + R$$

$$D_1 = \sigma^2 R + \sigma R + \sigma^{2k} Q$$

$$v_0 = r_0(x - x_R)$$

Then $r_0(\sigma^{2k} Q) = 0$ since otherwise $D_0 = (r_0)_0$. We can take Q as the point L of S such that $r_0(L) \neq 0$ and $r_3(L) \neq 0$.

4) If $card(S) = 3$ and v_2 does depend on y then :

$$E_1 = \sigma^k Q + \sigma^{k+1} Q$$

If $k = 3p + 1$ we have :

$$D_3 + D_4 \succeq Q + 2\sigma Q + 2\sigma^2 Q \Rightarrow (r_3)_0 \succeq \sigma Q + \sigma^2 Q \Rightarrow \sigma^2 P = \infty$$

Hence, we can take Q as the point L in $Supp(E_1)$ with $r_3(L) \neq 0$.

5) If $card(S) = 1$ take $Q \in S$.

6) if $card(S) = 2$ then take $Q_1 \in Supp(E_1)$ laying over x_Q. If $r_3(Q_1) \neq 0$ then $Q = Q_1$, else take Q as the point in $S \setminus \{Q_1\}$.

Given Q , $\sigma^2 P$ and E_2 we can construct D_5 and D_6. $\square$

Lemma 3.3 *Suppose that we know the vectors (D_i) for $i = 0$ to 6 and E_1, E_2 and E_3 in the sequence D_i associated to an effective divisor D. If $deg(v_{3i}) > 1$ for $0 \leq i < 3$ then, we may compute (D_7), (D_8) and (D_9) without making any factorization.*

Proof: Denote

$$u_7 = \sum_{l=0}^{deg(u_7)} (-1)^l s_l x^l$$

$$u_8 = \sum_{l=0}^{deg(u_8)} (-1)^l s'_l x^l$$

Now note that if $i = 7, 8$ $u_i = w^*_{i-1}$ where w^*_{i-1} means the quotient of w_{i-1} by its leading coefficient. On the other hand, using u_8 and the points in E_3 we can obtain u_9, so let's concentrate in the v_i.

Let's state several cases for the step from v_6 to v_7 $(1, .., 5)$ and from v_8 to v_9 $(i-1, .., i-3)$:

Case 1: $D_6 = P_1 + P_2 + P_3 + P_4$ (without three collinear points or pairs of conjugate).

Case 1.1: $a_{11} \neq 0$, so the curves :

$$v_6 = a_{20}x^2 + a_{10}x + a_{00} + a_{11}xy + a_{01}y$$

$$v_7 = b_{20}x^2 + b_{10}x + b_{00} + b_{01}y$$

are sharing three points besides ∞, which is equivalent to the equation :

$$R_y(v_6, v_7) = b_{01}(a_{20}x^2 + a_{10}x + a_{00}) - (a_{11}x + a_{01})(b_{20}x^2 + b_{10}x + b_{00}) = \lambda u_7 \qquad (3)$$

and solving the system we obtain :

$$b_{20} = -\lambda / a_{11}$$

$$b_{10} = \lambda(s_2 a_{20} a_{01} + a_{20} a_{11} s_3 - a_{11} a_{00}(s_1 + a_{01}/a_{11}) + a_{01} a_{10}(s_1 + a_{01}/a_{11}))/(-a_{00}a_{11}^2 + a_{10}a_{01}a_{11} - a_{20}a_{01}^2)$$

$$b_{00} = \lambda(s_2 a_{11} a_{00} - a_{20} a_{01} s_3 + a_{11} a_{10} s_3 + a_{01} a_{00}(s_1 + a_{01}/a_{11}))/(-a_{00}a_{11}^2 + a_{10}a_{01}a_{11} - a_{20}a_{01}^2)$$

$$b_{01} = \lambda(s_2 a_{11} a_{01} + a_{11}^2 s_3 + a_{01}^2(s_1 + a_{01}/a_{11}))/(-a_{00}a_{11}^2 + a_{10}a_{01}a_{11} - a_{20}a_{01}^2)$$

Case 1.2: $a_{11} = 0$, that is :

$$v_6 = a_{20}x^2 + a_{10}x + a_{00} + a_{01}y$$

$$v_7 = b_{10}x + b_{00} + b_{01}y$$

$$b_{01}(a_{20}x^2 + a_{10}x + a_{00}) - (a_{01})(b_{10}x + b_{00}) = \lambda u_7$$

$$b_{01} = \lambda / a_{20}$$

$$b_{10} = \lambda(-s_1/a_{01} + a_{10}/a_{20}a_{01})$$

$$b_{00} = \lambda(-s_2/a_{01} + a_{00}/a_{20}a_{01})$$

Case 2: $D_6 = P + \sigma P + Q_1 + Q_2$ (with $Q_1 \neq \sigma Q_2$, $\sigma^2 Q_2$ and $Q_i \neq \sigma^2 P$).
By lemma 3.1, $v_6 = r_6(x - x_P)$ and, if v_5 factorizes, we may apply lemma 3.2 in order to find the coordinates of $\sigma^2 P$. If is not the case we may obtain these coordinates from $Supp(E_2)$ and evaluating x_P in v_5. Now if $r_6(P) = 0$ or $r_6(\sigma P) = 0$ then :

$$v_7 = (x - x_P)R_y(C, r_6)(x - x_P)/u_6$$

Otherwise, if there are not collinear points in $Supp(D_6)$ proceed as in case 1 :

$$R_y(r_6, v_7) = b_{01}(-a_{20}/a_{11}x + a_{20}a_{01}/a_{11}^2 - a_{10}/a_{11}) + (b_{20}x^2 + b_{10}x + b_{00}) = \lambda u_7/(x - x_P)$$

$b_{20} = \lambda, b_{00} = \lambda s_2 + (a_{10} - a_{20}a_{01})b_{01}, b_{10} = \lambda s_1 - a_{20}b_{01}$. If r_6 and v_7 have order of contact s in $\sigma^2 P$, b_{01} is chosen such that v_7 and C have at least contact $s+1$ at this point (It is possible due to the dimension over k of the space of plane conics). Case 3: $D_6 = Q_1 + Q_2 + Q_3 + Q_4$ (without pair of conjugate, but with three collinear points).
$v_6 = r_6(x - x_P)$ and $R_y(C, r_6)(x - x_P)/u_6$ is linear. Hence :

$$v_7 = (x - x_P)R_y(C, r_6)(x - x_P)/u_6$$

Case 4: $D_6 = P + \sigma P + \sigma^2 P + Q$.
$v_6 = (x - x_Q)(x - x_P)$, $u_6/v_6 = ax^2 + bx + c$ and :

$$v_7 = v_6/(x + b/2a)$$

Case 5: $D_6 = P + \sigma P + Q + \sigma Q$.
Either we may apply lemma 3.2, or we can construct D_6 as the divisor E_2 + the points on v_5 with the same x-coordinates as the points of E_2. Consider the line r through $\sigma^2 P$ and $\sigma^2 Q$ then, $v_7 = r$.

Case i-1: $D_8 = Q_1 + Q_2 + Q_3$ (without pairs of conjugate).
If $(v_8)_0 \succeq P_3 = E_3$ and $u_8(x_3) \neq 0$, then $v_9 = v_8$. Else, proceed as in case 1.1 to obtain :

$$a'_{20} = (a'_{11}(b_{10} + s'_1 b_{20}) + b_{20}a'_{01})/b_{01}$$
$$a'_{10} = (a'_{11}(b_{00} - s'_2 b_{20}) + b_{10}a'_{01})/b_{01}$$
$$a'_{00} = (a'_{11}s'_3 b_{20} + b_{00}a'_{01})/b_{01}$$

Now, proceed as in case 2 taking a'_{01} and a'_{11} ($a'_{11} \neq 0$), such that $(v_9)_0 \succeq E_3 + D_8$.

Case i-2: $D_8 = P + \sigma P + Q$ (with $Q \neq \sigma^2 P$).
Use lemma 3.2 to find the line r through P_3 and Q, then :

$$v_9 = r(x - x_P)$$

Case i-3: $D_8 = Q_1 + Q_2$.
In this case $E_3 = P_3 + P_3'$. If $Q_1 = \sigma^k Q_2$ and r is the line through P_3 and P_3' then $v_9 = r(x - x_{Q_1})$. Otherwise if Q_1 and Q_2 are not conjugate we solve some particular subcases :

i)If P_3, P_3' are conjugate then, $v_9 = v_8(x - x_3)$

ii)If $u_8(x_3) = 0$ and $v_8(P_3) = 0$, due to $deg(u_8) = 2$, we can compute the roots of $u_8 = 0$ and using v_8, the points in $supp(D_8 + E_3)$.

iii)In the remaining cases, we compute :

$$R_y(v_8, v_9) = b_{01}(a_{20}x^2 + a_{10}x + a_{00}) - (a_{11}x + a_{01})(b_{10}x + b_{00}) = \lambda u_8$$

From here, we obtain :

$$a_{10}' = (b_{10}a_{01}' + a_{11}'b_{00} - \lambda s_1')/b_{01}$$
$$a_{10}' = (b_{00}a_{01}' + \lambda s_2')/b_{01}$$
$$a_{10}' = (a_{11}'b_{10} + \lambda)/b_{01}$$

And now, we select the free parameters a_{01}' , a_{11}', such that $(v_9)_0 \succeq P_3 + P_3'$. This lead us to one of the solvable systems :

$$\begin{cases} a_{11}'(b_{10}x_3^2 + b_{00}x_3 + b_{01}x_3y_3) + a_{01}(b_{10}x_3 + b_{00} + b_{01}y_3) = s_1'x_3 - s_2' - x_3^2 \\ a_{11}'(b_{10}x_3'^2 + b_{00}x_3' + b_{01}x_3'y_3') + a_{01}(b_{10}x_3' + b_{00} + b_{01}y_3') = s_1'x_3' - s_2' - x_3'^2 \end{cases}$$

$$\begin{cases} a_{11}'(b_{10}x_3^2 + b_{00}x_3 + b_{01}x_3y_3) + a_{01}(b_{10}x_3 + b_{00} + b_{01}y_3) = s_1'x_3 - s_2' - x_3^2 \\ a_{11}'(2b_{10}x_3 + b_{00} + b_{01}y_3 + x_3b_{01}\partial y/\partial x) + a_{01}(b_{10} + b_{01}\partial y/\partial x) = s_1' - 2x_3^2 \end{cases}$$

Depending on $P_3 = P_3'$ or not. $\square$

Lemma 3.4 *Suppose that we know the vectors (D_i) for $i = 0$ to 6 and E_1, E_2, E_3 in the sequence D_i associated to an effective divisor D. If $deg(v_0) > 1$ and $deg(v_3) > 1$ then, we may decide in which case of lemma 3.3 D_6 and D_8 are.*

Proof: Let's consider D_6 :

$$v_6 = a_{20}x^2 + a_{10}x + a_{00} + a_{11}xy + a_{01}y$$

If v_6 does not factorizes and $a_{11} \neq 0$ then, D_6 is in case 1.1. If v_6 does not factorizes and $a_{11} = 0$, we are in case 1.2. If $a_{11} = a_{01} = 0$ then, we may use of lemma 3.2 to decide if we are in case 4 or 5.
If $a_{11} = a_{20} = 0$ then, the four points are collinear, that is, $D_6 \cong 0$ and we begin with new

points.
If $a_{11} \neq 0$, but v_6 factorizes, we proceed as follows :

$$v_6 = r(x - x_0)$$

First if $deg(E_2) = 2$ and the points P_2, P_2' in $Supp(E_2)$ are conjugate, we are in case 2 and if it is not the case we may go on.
If v_5 does not depend on y, or if v_5 passes through a conjugate of P_2 or of P_2' and $u_5(x_0) = 0$ then, it is case 2. Else it is case 3.

Let's consider D_8 :

$$v_7 = b_{20}x^2 + b_{10}x + b_{00} + b_{01}y$$

If $b_{20} = 0$ we are in case i-3, if $b_{01} = 0$ we are in case i-2, otherwise we are in case i-1. $\square$

Lemma 3.5 *If we know D_0 , E_1 and E_2 in the sequence D_i associated to an effective divisor D then, we can compute (D_i) for $i = 0$ to 6.*

The precedent lemmas permit us to show the theorem :

Theorem 3.1 *Given an effective affine divisor D, it is possible to compute a reduced $D_f - 3\infty$ equivalent to $D - deg(D)\infty$ performing only one factorization and $O(deg(D))$ operations.*

Proof: 1)Take an effective affine divisor D.

2)If deg(D) ¡ 4 then D is already reduced $D_f := D$ and go to 20). Else, we can take $D_0 \preceq D$ an effective divisor of degree four.

3)Compute (D_0) and put $D := D - D_0$.

4)If $deg(v_0) = 1$ then go to 2), else compute (D_1) and (D_2) from D_0 and lemma 3.5.

5)If $4 - deg(u_2) > deg(D) > 0$ compute (D_3) using D and lemma 3.5, put $(D_f) = (D_3)$ and go to 19).

6)If $deg(D) = 0$ then $(D_f) = (D_2)$ and go to 19).

7) Take an effective divisor $E_1 = \alpha_1 P_1 + \beta_1 P_1'$ $(D \succeq E_1)$ with $deg(E_1) = 4 - deg(u_2)$. Using lemma 3.5 we can construct (D_3). $D := D - E_1$.

8)If $deg(v_3) = 1$ then go to 2), else compute $(D_4), (D_5)$ applying lemma 3.5.

9)If $4 - deg(u_5) > deg(D) > 0$ compute (D_6) using D and lemma 3.5, put $(D_f) = (D_6)$ and go to 19).

10)If $deg(D) = 0$ then $(D_f) = (D_5)$ and go to 19).

11) Take an effective divisor $E_2 = \alpha_2 P_2 + \beta_2 P_2'$ $(D \succeq E_2)$, with $deg(E_2) = 4 - deg(u_5)$. Using lemma 3.5 we can construct (D_6). $D := D - E_2$.

12)If $deg(v_6) = 1$ then go to 2), else compute $(D_7), (D_8)$ applying lemma 3.3.

13)If $4 - deg(u_7) > deg(D) > 0$ compute (D_9) using D and lemma 3.3, put $(D_f) = (D_9)$ and go to 19).

14)If $deg(D) = 0$ then $(D_f) = (D_8)$ and go to 19).

15) Take an effective divisor $E_3 = \alpha_3 P_3 + \beta_3 P_3'$ ($D \succeq E_3$) with $deg(E_3) = 4 - deg(u_8)$. Using lemma 3.3 we can construct (D_9). $D := D - E_3$.

16)Put $(D_i) := (D_{i+3})$ for $i = 0, 1, 2, 3, 4, 5, 6$.

17) $P_i := P_{i+1}, \alpha_i := \alpha_{i+1}, \beta_i := \beta_{i+1}$ for $i = 1, 2$.

18)Go to 12).

19)If v_f does not depend on y apply lemma 3.2 to obtain D_f, if not, factorize u_f and evaluate in v_f to obtain the points in $Supp(D_f)$.

20)Finish.

If we assume unit cost for all operation in the given field k, in each step of the algorithm we perform $O(1)$ operations. We iterate these steps $O(Deg(D))$ times so, this give a total of $O(Deg(D))$ operations to compute D_f. □

3.1 Numerical examples

Example 1.
If $k = Z_{23}$, $C : y^3 = x^4 - 1$ and $D = (1, 0) + (22, 0) + (8, 1) + (18, 12)$

$$(D) = (x^4 + 20x^3 + 5x^2 + 3x + 17, 10 + 14y + 8xy + 13x^3, 17(x^3 + 16x^2 + 22x + 5))$$

and the algorithm gives the result :

$$(D_f) = (x^3 + 12x^2 + x + 8, 21 + 17x + 7y + x^2, 4(x^3 + 16x^2 + 22x + 5))$$

$$D_f = (21, 21) + (\alpha, 14 + 22\alpha) + (13 + 22\alpha, 1 + \alpha)$$

where $\alpha^2 + 10\alpha + 4 = 0$.

Example 2.
If $k = Z_{13}$ and $C : y^3 = x^4 - 1$ then,

$$(0, 4) + (4, 2) + (6, 2) + (\alpha, 11 + 4\alpha) + (12\alpha + 6, 9(1 + \alpha)) - 5\infty \cong 2(1, 0) - 2\infty$$

where $5\alpha^2 + 9\alpha + 9 = 0$.

4 Algebraic Structure

Let C be a Picard curve, $J(C)$ its Jacobian Variety, both defined over the field k. In the previous section of this paper, it is shown that for any effective divisor $D = Q_1 + Q_2 ... + Q_n$ of degree n, an effective divisor $D' = P_1 + P_2 + P_3$ can be constructed, such that P_j are defined on an algebraic extension of the field of definition of D, on $J(C)$ holds $Q_1 + Q_2 ... + Q_n - n\infty \cong P_1 + P_2 + P_3 - 3\infty$ and D' may be explicitly computed in terms of the coordinates of the points in $Supp(D)$.

If we set $Div^{+,n}(C) := \{Q_1 + Q_2 ... + Q_n\}$, then the map :

$$\begin{array}{rcl} \imath : Div^{+,n}(C) & \rightarrow & J(C) \\ Q_1 + Q_2 ... + Q_n & \rightsquigarrow & P_1 + P_2 + P_3 - 3\infty \end{array}$$

is surjective. Moreover, on $Div_0^{+,3}(C) := \{D = Q_1 + Q_2 + Q_3 / Q_j \neq \infty, \mathcal{L}(D) = k\}$, $\imath$ is also injective, since for $D_1 \neq D_2$, $\imath(D_1) = \imath(D_2)$ implies $D_1 - D_2 = (h), h \in \mathcal{L}(D_2), h \neq$ constant.

For any smooth projective curve C, it is possible to describe $Div^{+,n}(C)$ as a projective variety using the bijection $Div^{+,n}(C) \cong Symm^n(C)$, the orbit space of C^n under the action of the symmetric group permuting the factors. Given an embedding $C \hookrightarrow P^N$, we have the associated Segre embedding

$$j : C^n \hookrightarrow P^{(N+1)^n - 1}$$

In the case of Picard curves embedded in P^2, $j : C^3 \hookrightarrow P^{26}$, and the defining equations in such high dimensional projective space have not been explicitly obtained. An alternative approach should be to take as coordinates for the elements of $Div^{+,3}(C)$ the coefficients of its Chow form (see [2], [3] and [13]), which are elements of P^9. Nevertheless, the construction of an explicit set of defining equations (consisting at least of 6 polynomial equations) for the image of $Div^{+,n}(C)$ in P^6 happens to be more complicated than in the affine model that we present in this paper.

Using as coordinates the coefficients $(u_\imath, v_\jmath)$ of the conics and cubics associated to a divisor in $Div^{+,3}(C)$ in the previous section of this paper, we are able to construct a model of algebraic variety for the Jacobian Variety of a Picard curve defined over an algebraic closed field of characteristic greater than three or equal to zero. The open sets of its atlas are isomorphic to an open affine subset of A^6 , which is a complete intersection of three polynomial equations in the variables $(u_\imath, v_\jmath)$. These defining equations are computed explicitly.

The following result is strongly motivated by Mumford's works on hyperelliptic curves [15]. Therefore, many steps of the proof happen to be analogous to the hyperelliptic case and here we will simply refer Mumford's book for a detailed argumentation. Nevertheless, those aspects which needed to be generalized will be meticulously explained, since in these places special features of the geometry of Picard curves have been exploited.

Theorem 4.1 *(Explicit structure of algebraic variety for $J(C)$.)*
The Jacobian Variety $J(C)$ of a Picard curve contains a subgroup of $6-torsion$ points, $\mathcal{T}$ and a Zariski open subset, $\mathcal{Z}$, such that:
a)$\mathcal{Z}$ is isomorphic to an algebraic variety. Furthermore, $\mathcal{Z}$ is complete intersection of three polynomial equations in A^6, which may explicitly given.
b) $\mathcal{T} \cong (Z/2Z)^2 \times (Z/3Z)^3$ and $J(C) = \cup_{t\in\mathcal{T}} \ (\ \mathcal{Z} \ + \ t \ )$
c) The family $\mathcal{A} = \{\mathcal{Z} + t/t \in \mathcal{T}\}$ is the atlas of a structure of algebraic variety on $J(C)$. Moreover, $\mathcal{A}$ endows $J(C)$ with a structure of abelian variety.

Proof. a) First we will prove:

Proposition 4.1 $Div_0^{+,3}(C) = \{D = P_1 + P_2 + P_3/P_\jmath \neq \infty, P_\jmath$ *not collinear* $\}$

Proof. The canonical class K of the Picard curve C is the class of divisors of zeroes arising from the intersection of straight lines with C, since $B = \{dx/y^2, xdx/y^2, dx/y\}$ is a basis of abelian differentials on C (see [4]). Applying the Riemann-Roch theorem to $D = P_1+P_2+P_3$ $(deg(D) = 3, g = 3)$,

$$l(D) = l(K - D) + 1$$

Therefore, $l(D) > 1$ (i.e. $\mathcal{L}(D) \neq k$) if and only if $K \succeq D$, hence the points $P_\jmath$ are collinear.

Our aim is to parametrize a convenient subset of the $\imath$-image of $Div_0^{+,3}(C)$, since on $Div_0^{+,3}(C)$ the injectivity of $\imath$ holds. The coefficients of the conics and cubics associated to a divisor in the first section of this paper may be a suitable set of coordinate functions, once a bijection between open subsets can be ensured.

Set $Div_\infty^{+,3}(C) := \{D \in Div_0^{+,3}(C)$ / there are not three collinear points in $Supp(D+\infty)\}$. To any divisor $D \in Div_\infty^{+,3}(C)$ we have associated a conic

$$v(D) = v_{00} + v_{10}x + v_{20}x^2 + v_{01}y, (v(D), C) \succeq D + 2\infty$$

and a cubic

$$u(D) = u_3x^3 + u_2x^2 + u_1x + u_0, (u(D), C) \succeq D + \sigma D + \sigma^2 D$$

Since $D \in Div_\infty^{+,3}(C)$, we may assume $v_{01} = 1$ and $u_3 = 1$.

This set up a map

$$\begin{array}{rcl} Div_\infty^{+,3}(C) & \hookrightarrow & A_k^6 \\ D = P_1 + P_2 + P_3 & \rightsquigarrow & (D) = (u_0, u_1, u_2, v_0, v_1, v_2) \end{array}$$

for $v_j := v_{j0}$.

Any $D \in Div_\infty^{+,3}(C)$ defines a unique well defined vector $D = (u_i, v_j)$, since u_i are symmetric functions on the x-coordinates of the P_j and v_j are the coefficients of the unique polynomial of degree two (P_j are not collinear) interpolating the "-y"-coordinates of the points on $Supp(D)$. Reciprocally, given an efective divisor $D = P_1 + P_2 + P_3$, the x-coordinates of P_j are the roots x_j of the polynomial $u(x) = x^3 + u_2x^2 + u_1x + u_0$ and for each x_j, the corresponding y-coordinate of P_j is given by $y_j = v(x_j) = -(v_0 + v_1x_j + v_2{x_j}^2)$. The points $P_j = (x_j, y_j)$ lie on C if the polynomial $u(x)$ divides the polynomial $v(x)^3 - p_4(x)$. $P_j \neq \infty$, since $u(x)$ has three affine roots, counted with multiplicity. Obviously, no pair of conjugate points will appear.

Summarazing, there is a bijection between $\mathcal{Z} := \imath(Div_\infty^{+,3}(C))$ and the Zariski open subset of A_k^6, $\mathcal{O} := \{(u_i, v_j)/u(x)|v(x)^3 - p_4(x), v_2 \neq 0\}$

Let $r(x)$ be the remainder of the quotient of $v(x)^3 - p_4(x)$ by $u(x)$, $r(x) = r_0 + r_1x + r_2x^2$, where

$r_0 = -a_0 + {v_0}^3 + u_0\ a_3 - u_0\ {v_1}^3 + {v_2}^3{u_0}^2 - u_0\ u_2\ a_4 + u_0\ {u_2}^3{v_2}^3 + 3\ u_0\ u_1\ {v_2}^2v_1 - 2\ u_0\ u_1\ {v_2}^3u_2 - 6\ u_0\ v_2\ v_1\ v_0 + 3\ u_0\ u_2\ {v_2}^2v_0 + 3\ u_0\ u_2\ v_2\ {v_1}^2 - 3\ u_0\ {u_2}^2{v_2}^2v_1$

$r_1 = -a_1 + 3\ v_1\ {v_0}^2 + u_0\ a_4 - 3\ u_0\ {v_2}^2v_0 - 3\ u_0\ v_2\ {v_1}^2 + 2\ u_0\ {v_2}^3u_1 + 3\ u_0\ u_2\ {v_2}^2v_1 - u_0\ {u_2}^2{v_2}^3 - u_1\ {v_1}^3 + u_1\ a_3 - u_1\ u_2\ a_4 + u_1\ {u_2}^3{v_2}^3 + 3\ {u_1}^2{v_2}^2v_1 - 2\ {u_1}^2{v_2}^3u_2 - 6\ u_1\ v_2\ v_1\ v_0 + 3\ u_1\ u_2\ {v_2}^2v_0 + 3\ u_1\ u_2\ v_2\ {v_1}^2 - 3\ u_1\ {u_2}^2{v_2}^2v_1$

$r_2 = -a_2 + 3\ v_2\ {v_0}^2 + 3\ {v_1}^2v_0 + u_1\ a_4 + {u_1}^2{v_2}^3 - 3\ u_0\ {v_2}^2v_1 + 2\ u_0\ {v_2}^3u_2 - 3\ u_1\ {v_2}^2v_0 - 3\ u_1\ v_2\ {v_1}^2 + 6\ u_1\ u_2\ {v_2}^2v_1 - 3\ u_1\ {u_2}^2{v_2}^3 - {u_2}^2a_4 - u_2\ {v_1}^3 + {u_2}^4{v_2}^3 + u_2\ a_3 - 6\ u_2\ v_2\ v_1\ v_0 + 3\ {u_2}^2{v_2}^2v_0 + 3\ {u_2}^2v_2\ {v_1}^2 - 3\ {u_2}^3{v_2}^2v_1$

The r_j are polynomials in (u_i, v_j) and coefficients in k and taking u_i, v_j as coordinates, $\mathcal{O} \cong V(r_j)_{v_2}$, i.e., $\mathcal{O}$ is an affine variety.

We can parametrize $Div_\infty^{+,3}(C)$ by points of C:

$$\begin{array}{ccc} C^3 & \to\to & Div_0^{+,3}(C) \\ (P_1, P_2, P_3) & \rightsquigarrow & (u_i, v_j) \end{array}$$

and consider the Zariski open subset $(C^3)_0$ defined as:

$$C^3 \setminus (C^3)_0 = (\cup_{i=1}^3 p_i^{-1}(\infty)) \bigcup (\cup_{0\leq i\leq j\leq 3} p_{i,j}^{-1}(\Gamma)) \bigcup \Gamma_1,$$

where $p_i : C^3 \to C$ is the i-th projection, $p_{i,j} : C^3 \to C^2$ is the (i,j)-th projection, $\Gamma = [locusofpoints(P, \sigma^k(P)), k = 1, 2]$ and $\Gamma_1 = \{(P_1, P_2, P_3)/P_j$ are collinear $\}$.
Then after a straightforward generalization of the hyperelliptic case, it can be shown that the variety $\mathcal{O}$ is smooth of dimension 3 and the composite map $(C^3)_0 \to\to \mathcal{Z} \cong \mathcal{O}$ is a

surjective morphism making $\mathcal{O}$ isomorphic to the orbit space for the group of permutations S_3 acting on $(C^3)_0$

b) The ramification points of $C \to P^1_k$ are ∞ and the affine points on the line $y = 0$, R_1, R_2, R_3 and R_4. Set $\mathcal{R} = \{\infty, R_1, R_2, R_3, R_4\}$ then, considering the intersection of the tangent line at $R \in \mathcal{R}$ with C, it holds

$$3R - 3\infty \cong 0,$$

hence the $\imath$-images of the elements of $\mathcal{R}$ are 3-torsion points on $J(C)$ and the subgroup of $J(C)$ that they generate is isomorphic to $(Z/3Z)^3$, since$R_4 - \infty \cong -R_1 - R_2 - R_3 + 3\infty$.

Let b be a bitangent of$C$, such that

$$(b) = 2B_1 + 2B_2 - 4\infty,$$

$B_\jmath$ may be assumed not in $\mathcal{R}$. Set BT equal to the effective divisor $B_1 + B_2$ and $\mathcal{B} := \{BT, \sigma(BT), \sigma^2(BT)\}$ then, the i-images of the elements of $\mathcal{B}$ are 2-torsion points on $J(C)$ and the subgroup that they generate is isomorphic to $(Z/2Z)^2$, since $\sigma^2(BT) - \infty \cong -BT - \sigma(BT) + 2\infty$.

Define $\mathcal{T}$:= the subgroup of $J(C)$ generated by $\imath(\mathcal{R})$ and $\imath(\mathcal{B})$. Clearly, $\mathcal{T}$ is isomorphic to $(Z/3Z)^3 \times (Z/2Z)^2$

The proof of $J(C) = \cup_{t \in T}(\mathcal{Z}+$ t) consists of many cases (some of them overlapping). First, we recall some elementary geometric properties of Picard curves:
- Any line intersecting C in two points of $\mathcal{R}$ (counted with multiplicity) intersects C in two more points of $\mathcal{R}$, also counted with multiplicity.
- Any line passing through the point ∞ intersects C in three conjugate points, i.e., three points of the form $P, \sigma P and \sigma^2 P$.
- There exist a unique line intersecting C in $\sigma^k(B_1)$ and $\sigma^k(B_2)$ for $k = 0, 1, 2$ fixed. This line is the corresponding bitangent.

Assume D is an effective divisor, $D = P_1 + P_2 + P_3$, with $\imath(D) \notin \mathcal{Z}$.
Case I. (There is a pair of conjugate points in Supp(D)).
I.1. $D = P + \sigma(P) + Q, P \notin \mathcal{R}$. Then, choose $R \in \mathcal{R}$, such that $\sigma^k(Q), k = 0, 1, 2$ do not lie on the line r joining R and $\sigma^2(P)$. If $(r) = R + \sigma^2(P) + Q_1 + Q_2 - 4\infty$, $\imath(D) \cong \imath(R + Q + Q_1 + Q_2)$ and $\imath(D + 2R) \cong \imath(Q + Q_1 + Q_2) \in \mathcal{Z}$.
I.2.a) $D = 2R + Q, P \notin \mathcal{R}$ and $Q \neq \sigma^k(B_\jmath), k = 0, 1, 2, \jmath = 1, 2$. Then, $\imath(D + R + BT) \cong \imath(Q + BT) \in \mathcal{Z}$.
I.2.b) $R = 2R + B_1$, $R \in \mathcal{R}$. Then, $\imath(D + R + \sigma(BT)) \cong \imath(B_1 + \sigma(B_1 + B_2))$ and here we are in case I.1.
I.3. $D = P + 2\infty$. Then, either there exists $B \in \mathcal{B}$, such that $\imath(D + B) \in \mathcal{Z}$ or we are in case I.1.
I.4. $D = P + \sigma(P) + \sigma^2(P) \cong 3\infty$. Then, $\imath(D + R + BT) \in \mathcal{Z}$, for $R \in \mathcal{R}$ and $BT \in \mathcal{B}$.
Case II. ($\infty \in Supp(D)$).

II.1. $D = P_1 + P_2 + \infty$, $P_\jmath \notin \mathcal{R}$. Then, there exists $R \in \mathcal{R}$, such that $\imath(D + R) \in \mathcal{Z}$.
II.2. $D = R + P + \infty, R \in \mathcal{R}$, $P \neq \infty$. Then, either there exists $B \in \mathcal{B}$, such that $\imath(D + 2R + B) \cong \imath(P + B) \in \mathcal{Z}$, or we are in case I.1.
II.3. $D = P + 2\infty$ was considered in case I.3. above.
Case III. ($D = \sum P_\jmath$, $P_\jmath$ collinear).
III.1. $D = R_1 + R_2 + R_3$, $R_\jmath \in \mathcal{R}$. Then, $\imath(D + R_4) \cong 0$ thus we are in case I.4.
III.2. $D = P_1 + P_2 + R_1$, $P_\jmath \notin \mathcal{R}$, $R_1 \in \mathcal{R}$. Then, choose $\mathcal{R} \ni R_2 \neq R_1$, and $\imath(D + 2R_1 + R_2) \cong \imath(R_2 + P_1 + P_2) \in \mathcal{Z}$.
III.3. $D = P_1 + P_2 + P_3$, $P_\jmath \notin \mathcal{R}$. The line passing through $P_\jmath$ intersects C in a further point P_4. Consider the line r joining P_4 with some $R \in \mathcal{R}$, $(r) = R + P_4 + Q_1 + Q_2 - 4\infty$. Thus, $\imath(D) \cong \imath(R + Q_1 + Q_2)$. If $P_4 \in \mathcal{R}$ then, $Q_\jmath \in \mathcal{R}$, hence either $\imath(D) \cong \imath(3R) \cong 0$ (case I.4) or we are in case III.1. If P_4 is not in $\mathcal{R}$, $\imath(D) \cong \imath(R + Q_1 + Q_2)$, and we are in case III.2.
Therefore, the translations of $\mathcal{Z}$ with elements of $\mathcal{T}$ cover $J(C)$.

c) $J(C)$ is covered by copies of $\mathcal{Z}$ translated by elements of $\mathcal{T}$. When two copies are glued together, according to their identification as subsets of $J(C)$, it remains to check that the condition required to give an atlas of algebraic variety on $J(C)$ are satisfied.

Proposition 4.1 *Given D_1, D_2, such that $\imath(D_\jmath) \in \mathcal{T}$, the set $\mathcal{Z} \times \mathcal{Z} \supset \Gamma_{D_1,D_2} := \{(H_1, H_2)/H_1 + D_1 \cong H_2 + D_2\}$ is a Zariski closed subset of $\mathcal{Z} \times \mathcal{Z}$*

Proof. The set Γ_{D_1,D_2} defined above can be rewritten as,

$$\{(H_1, H_2)/H_1 + \sigma(H_2) + \sigma^2(H_2) + D_1 + \sigma(D_2) + \sigma^2(D_2) \cong 18\infty\},$$

since we can assume $H_1 = \sum_{\jmath \leq 3} P_\jmath$, $H_2 = \sum_{\jmath \leq 3} Q_\jmath$, $D_1 = P_i + P_j + P_k$ and $D_2 = Q_l + Q_m + Q_n$.

Let's consider the vector space $\mathcal{L}$ (18∞). If f $\in \mathcal{L}$ (18∞), then $f = pf_6(x) + ypf_4(x) + y^2pf_3(x)$, $pf_\jmath(x)$ polynomial of degree $\jmath$ in x and f has zeroes at $\sum_{\imath \leq 3} P_\imath + \sum_{\imath \leq 3}(\sigma(Q_\imath) + \sigma^2(Q_\imath)) + D_1 + \sum_{k \leq 2} \sigma^k D_2$ if and only if f belongs to the ideal in the affine ring of C, $R := k[x, y]/(y^3 - p_4(x))$, given by the product,

$$\begin{aligned} I_{H_1,H_2} &= (u_1(x), y - v_1(x)) \cdot (u_2(x), y - v_2(x)) \cdot \\ &\cdot \prod_{d=i,j,k} (y - y_d, x - x_d) \cdot \prod (y - \xi y_d, x - x_d)(y - \xi^2 y_d, x - x_d) \end{aligned}$$

where
$\sum_{\jmath \leq 3} P_\jmath \longleftrightarrow (u_1, v_1)$ and $\sum_{\jmath \leq 3} Q_\jmath \longleftrightarrow (u_2, v_2)$, since C non singular implies that R is a Dedekind domain.
Clearly, if h $\in \mathcal{L}(18\infty) \cap I_{H_1,H_2}$ then, $(H_1, H_2) \in I_{D_1,D_2}$, since h has exactly 18 zeroes and poles only at ∞.
Observe that, in order to belong to the ideal I, a function must satisfy 18 linear conditions,

hence $codim I = 18$, independent of H_1 and H_2.
Let $R_{\mathcal{Z}} = k[u_i, v_i]/(r_j)$ then, we obtain a "universal" ideal I, $I \subset R_{\mathcal{Z}}^{(1)} \otimes R_{\mathcal{Z}}^{(2)}[x,y]/(y^3 - p_4(x))$ defined by the formula $(*)$, with $u_i^{(j)}, v_i^{(j)} \in R_{\mathcal{Z}}^{(j)}$ being variables.
The algebra A over $R_{\mathcal{Z}}^{(1)} \otimes R_{\mathcal{Z}}^{(2)}$ defined by $A = R_{\mathcal{Z}}^{(1)} \otimes R_{\mathcal{Z}}^{(2)}[x,y]/(y^3 - p_4(x)) + I$ is finitely generated and integrally dependent (I contains a monic monomial in x), such that for all homorphisms $R_{\mathcal{Z}}^{(1)} \otimes R_{\mathcal{Z}}^{(2)} \rightsquigarrow k$ (evaluation of coordinates) A becomes a $k-$vector space of dimension 18. Then, it can be shown (see [15]) that A is locally free, i.e., $\exists h_\alpha, g_\alpha \in R_{\mathcal{Z}}^{(1)} \otimes R_{\mathcal{Z}}^{(2)}$, such that $1 = \sum h_\alpha \cdot g_\alpha$, and $\forall l_1^{(\alpha)}, .., l_{18}^{(\alpha)}$ basis of A_{h_α} as $R_{\mathcal{Z}}^{(1)} \otimes R_{\mathcal{Z}}^{(2)}$-module.
Let be $\{f_j / i = 1, .., 16\}$ a basis of $\mathcal{L}(18\infty)$ and consider the map $\mathcal{L}(18\infty) \to A$ given by $f_i \rightsquigarrow \sum c_{i,j}^{(\alpha)} e_j^{(\alpha)}$
Then, the condition "$rk(c_{i,j}^{(\alpha)}) < 16$" defines the set Γ_{D_1,D_2} in the open set $h_\alpha \neq 0$ of $\mathcal{Z} \times \mathcal{Z}$. This sets cover $\mathcal{Z} \times \mathcal{Z}$ $(1 = \sum h_\alpha \cdot g_\alpha)$, therefore, Γ_{D_1,D_2} is a closed subset of $\mathcal{Z} \times \mathcal{Z}$. Furthermore, the $rk(c_{i,j}^{(\alpha)})$ is not less than 15, since two functions in $ker(\mathcal{L}(D) \to A)$ are linearly dependent, having the same zeroes and poles. Hence, Γ_{D_1,D_2} is defined locally by 3 $(= 18 - 15)$ equations (see [15]), thus, all componenets of Γ_{D_1,D_2} have dimension ≥ 3. Γ_{D_1,D_2} is in fact irreducible of dimension 3, since $\Gamma_{D_1,D_2} \to \mathcal{Z}$ is injective and dim $\mathcal{Z} = 3$. Therefore, applying the weak form of Zariski's Main Theorem [8], Γ_{D_1,D_2} is isomorphic to an open subset of $\mathcal{Z}$ under each projection and Γ_{D_1,D_2} may de used to glue the D_i and D_j copies of $\mathcal{Z}$ to obtain a structure of algebraic variety on $J(C)$, with atlas $\mathcal{A}$.
As algebraic variety, $J(C)$ is complete, because there is a surjective birational morphism $C^3 \to J(C)$, with C^3 projective, since C is complete. Moreover, $J(C)$ is an abelian variety, since in an analogous way as above, we can prove that for $H_j \in \mathcal{Z}$ and $D_j \in \mathcal{T}$, the set
$\{(H_1, H_2, H_3) \in \mathcal{Z} \times \mathcal{Z} \times \mathcal{Z} / H_1 + D_1 + H_2 + D_2 \cong H_3 + D_3 + 6\infty\}$
is Zariski closed in $\mathcal{Z} \times \mathcal{Z} \times \mathcal{Z}$ and projects isomorphically via $p_{1,2}$ to $\mathcal{Z} \times \mathcal{Z}$.

References

[1] Cantor, D., Computing in the jacobian of a hyperelliptic curve. Math. of Computation 48 (1987), 95-101.

[2] Chow, W.-L., On the defining field of a divisor in an algebraic variety. Amer. J. Math 72 (1950), 247-283.

[3] Chow, W.-L., The Jacobian variety of an algebraic curve, Amer. J. Math 76 (1954), 454-476.

[4] Estrada Sarlabous, J., Higher differentials on Cyclic Curves. Math. Nachr. 135 (1988), 311-317.

[5] Estrada Sarlabous, J., On the Jacobian Varieties of Picard Curves Defined over Fields of Characteristic p ¿ 0. Math. Nachr. 152 (1991), 329-340.

[6] Estrada Sarlabous, J., A finiteness theorem for Picard curves with good reduction. Appendix I of "Ball models for some Hilbert Problems" by R.-P. Holzapfel. Birkäuser-Verlag (1994).

[7] Fulton, W., Algebraic Curves. Addison-Wesley Pub. Co. (1989).

[8] Harris, J., Algebraic Geometry: a first course. Springer Graduate Texts in Math 133 (1992).

[9] Holzapfel, R.-P., Geometry and arithmetic around Euler partial differential equations. Dt. Verl. d. Wiss., Berlin/Reidel Publ. Comp., Dordrecht (1986).

[10] Holzapfel, R.-P., On algebraic values of the Picard modular function. Proc. Special Diff. Equations, Arkata (1991).

[11] Holzapfel, R.-P., Transcendental Ball Points of Algebraic Picard Integrals. Math. Nachr. 162 (1993).

[12] Holzapfel, R.-P., Ball models for some Hilbert problems. Birkhäuser-Verlag (1994).

[13] Huang, M.-D. and Ierardi, D.J., Efficient algorithms for the effective Riemann-Roch problem and for addition in the jacobian of a curve. Proc. of the Twenty-first ACM Symp. on the Foundations of Computer Science, (May 1991).

[14] Mumford, D., Curves and Their Jacobians. The University of Michigan Press (1975).

[15] Mumford, D., Tata Lectures on Theta II. Jacobian theta functions and differential equations. Progress in Math, Vol.42, Birkhauser Verlag (1984).

[16] Weil, A., Sur les courbes algebriques et les varietes qui s'en deduisent. Herman, Paris (1948).