Department of Mathematics
TUM School of Computation, Information and Technology
Technical University of Munich

Arithmetic on hyperelliptic Jacobians and singular curves

Yichen Tong

Thesis for the attainment of the academic degree

Master of Science

at the TUM School of Computation, Information and Technology of the Technical University of Munich

Supervisor:
Prof. Dr. Lorenz Panny

Advisors:
Prof. Dr. Lorenz Panny
Xianyu Hu

Submitted:
Munich, 29. April 2025

I hereby declare that this thesis is entirely the result of my own work except where otherwise indicated. I have only used the resources given in the list of references.

Munich, 29. April 2025 Yichen Tong

Abstract

The discrete logarithm problem (DLP) in the Jacobian group of an elliptic curve plays a crucial role in cryptographic applications. Hyperelliptic curves have also been proposed for building cryptosystems. For smooth hyperelliptic curves, the Mumford representation is commonly used to perform arithmetic on the Jacobian. However, arithmetic on the Jacobians of singular hyperelliptic curves has been less explored. In this thesis, we study the arithmetic on the Jacobians of singular hyperelliptic curves. For curves with geometric genus zero, we propose the generalized Mumford representation, which provides a structured representation for each divisor class in the Jacobian. Additionally, we establish a decomposition of the Jacobian group as a product of Jacobian groups of singular curves of arithmetic genus 1. Building on this result, we construct an explicit group isomorphism between the Jacobian and products of multiplicative and additive groups of the base field. Given any singular hyperelliptic curve C, we define a (partial) normalization C' and a canonical (partial) normalization map Φ from $J(C)$ to $J(C')$. This induces an exact sequence of group schemes:

$$0 \to \ker(\Phi) \to J(C) \xrightarrow{\Phi} J(C') \to 0.$$

For singular curves of geometric genus 0, we show that the exact sequence splits according to the isomorphism we have obtained. However, for certain families of singular hyperelliptic curves with positive geometric genus, we demonstrate that the exact sequence associated with their normalization map does not split.

Contents

1 Introduction

1.1 Context and our work

In 1985, Mumford introduced a representation, known as the Mumford representation [Mum82], to represent each divisor class in the Jacobian group of nonsingular hyperelliptic curves. Building on this, Cantor's algorithm [Can87] provided an implementation of the addition law for the Jacobian group using the Mumford representation. While nonsingular hyperelliptic curves have been extensively studied and applied in cryptography, the arithmetic on the Jacobian groups of singular hyperelliptic curves has been comparatively less explored.

Enver Ozdemir proposed a representation for the Jacobian group of singular hyperelliptic curves [Ozd09]. David Kohel also provided a representation for the Jacobian of an elliptic nodal curve [Koh12]. In this thesis, we introduce a novel representation for the Jacobian group of singular hyperelliptic curves with geometric genus zero. This representation, distinct from those proposed in [Ozd09] and [Koh12], provides a clearer and more structured description of the Jacobian group. Furthermore, we demonstrate that the Cantor composition (a component of Cantor's algorithm) can efficiently implement addition in the Jacobian group when expressed in this new representation. We refer to this representation as the Generalized Mumford Representation.

In [CNO22], a representation specifically for the Jacobian groups of curves with geometric genus zero and multiple nodal singularities was introduced. However, this representation was incomplete because it failed to account for certain divisor classes and lacked a formal proof (see Remark 3.1.23).

Additionally, for curves with geometric genus 0 and multiple nodal singularities, Section 3 in [Koh12] provided a surjective homomorphism from the Jacobian group to a singular curve of arithmetic genus 1. Using this, it gave an isomorphism between its Jacobian group and the product of Jacobian groups of singular curves of arithmetic genus 1. In this thesis, we extend this isomorphism to all geometric genus-zero curves. In other words, we construct a decomposition of the Jacobian group into the product of Jacobian groups of singular curves of arithmetic genus 1.

Theorem 2.31 in [Was08] and Section 2 of [Koh12] both demonstrated an isomorphism between the Jacobian group of an elliptic nodal curve and the multiplicative group of the base field. Moreover, in [Koh12], this result was extended to curves of geometric genus zero with multiple nodal singularities. Theorem 2.30 in [Was08] further established an isomorphism between the Jacobian group of an elliptic cuspidal curve and the additive group of the base field. In this thesis, we generalize these results to all singular curves of arithmetic genus 1. Using the decomposition described above, we construct an explicit group isomorphism between the Jacobian group of any geometric genus zero curve to products of additive and multiplicative groups over the base field.

For any singular hyperelliptic curve C, we define a singular hyperelliptic curve C' which contains some of the singularities of C, and refer to it as a (partial) normalization of C. There exists a canonical surjective (partial) normalization map from $J(C)$ to $J(C')$. We prove that the kernel of this (partial) normalization map is isomorphic to products of additive and multiplicative groups over the base field. Based on this, we show that the exact sequence associated with a partial normalization map splits for curves of geometric genus zero. However, for certain families of curves with positive geometric genus, we establish that the exact sequence associated with the normalization map does not split.

1.2 Organization of the thesis

Throughout this thesis, all curves are assumed to be defined over $\mathbf{C}$ (any algebraically closed field also suffices). Let C denote the singular hyperelliptic curve of arithmetic genus g given by

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

where $h(x) = \prod_{i=1}^{k}(x - c_i)^{n_i}$, $c_i \neq c_j$, $\forall i \neq j$, $\deg(f(x)) = 2g + 1$ and $e(x)$ has no repeated roots. This thesis is organized as follows:

In Chapter 2, we review fundamental knowledge of the arithmetic on Jacobians of smooth hyperelliptic curves. We first introduce divisors in Section 2.1, which define elements of the Jacobian group. Next, we present the Mumford Representation in Section 2.2 and Cantor's Algorithm in Section 2.3. Many of these concepts and methods carry over to the singular case.

In Chapter 3, we discuss the arithmetic on Jacobians of geometric genus-zero curves. In this case, $e(x) = x$ and $g = \sum_{i=1}^{k} n_i$. We begin by introducing the generalized Mumford representation for $J(C)$ in Section 3.1. Next, in Section 3.2, we first define a (partial) normalization C' for any singular hyperelliptic curves and introduce the canonical surjective (partial) normalization map Φ from $J(C)$ to $J(C')$. Using the formula for the partial normalization map for geometric genus-zero curves, we prove the decomposition

$$J(C) \cong \prod_{i=1}^{k} J(C_i),$$

where $C_i : y^2 = (x - c_i)^{2n_i}x$, $\forall 1 \leq i \leq k$. In Section 3.3, we provide explicit group isomorphisms

$$\begin{gathered} J(C : y^2 = x^{2g+1}) \cong \mathbf{C}^g, \\ \text{and } J(C : y^2 = x^{2g}(x - c)) \cong \mathbf{C}^{g-1} \times \mathbf{C}^*. \end{gathered}$$

Using these results, we construct an explicit group isomorphism

$$J(C) \cong \mathbf{C}^{g-l} \times (\mathbf{C}^*)^l,$$

where l is number of nonzero c_i, for $1 \leq i \leq k$.

In Chapter 4, we study the arithmetic on Jacobians of singular hyperelliptic curves with positive geometric genus. In this case, $\deg(e(x)) \geq 3$. Let C' be any (partial) normalization of C and Φ denote the (partial) normalization map $\Phi : J(C) \to J(C')$. In Section 4.1, we prove that $\ker(\Phi)$ splits as a product of copies of $\mathbf{C}$ and $\mathbf{C}^*$. Next, in Section 4.2, we investigate the splitting property of the exact sequence of group schemes

$$0 \to \ker(\Phi) \to J(C) \xrightarrow{\Phi} J(C') \to 0.$$

We demonstrate that the exact sequence splits when C has geometric genus zero. While for curves with positive geometric genus satisfying one of the following:

(1) $\gcd(h(x), e(x)) \neq 1$,

(2) $\gcd(h(x), e(x)) = 1$, and there exists $(x - c) \mid h$ such that

$$\gcd(e(x), s(x - c) + 2e(c)) = 1,$$

where $s := \frac{e(x)-e(c)}{x-c}\Big|_{x=c}$, the exact sequence associated with the normalization map does not split.

2 Arithmetic on Jacobians of smooth hyperelliptic curves

In this chapter, we briefly review the arithmetic on Jacobians of smooth hyperelliptic curves. We begin by introducing divisors on curves. We then review the Mumford representation, which corresponds each divisor class in the Jacobian to a pair of polynomials. Next, we recall Cantor's algorithm, which implements the addition law for divisor classes in Mumford representation.

2.1 Divisors

Definition 2.1.1. *A smooth hyperelliptic curve C of arithmetic genus g is defined by*

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

where $f(x)$ is a polynomial of degree $2g+1$ with no repeated roots.

Remark 2.1.2. *It is worth noting that there is a point at infinity on C, denoted by ∞.*

Definition 2.1.3. *A divisor D on C is a finite linear combination of symbols $[P]$ $(P \in C)$ with integer coefficients:*

$$D = \sum_{j=1}^{n} c_j [P_j],$$

where $c_j \in \mathbf{Z}, P_j \in C$ for each $j = 1, \cdots, n$.

The degree of a divisor is defined as

$$\deg(\sum_{j=1}^{n} c_j [P_j]) = \sum_{j=1}^{n} c_j.$$

Remark 2.1.4. *Strictly speaking, the divisor defined above is a Weil divisor. For simplicity, we refer to it simply as a divisor throughout this thesis.*

The group of divisors, denoted by $\mathrm{Div}(C)$, is therefore the free abelian group generated by the symbols $[P]$ with $P \in C$. It is easy to check that divisors of degree 0 form a subgroup, which we denote by $\mathrm{Div}^0(C)$.

Given a point $P \in C$, the local ring $O_{\mathrm{C},P}(C)$ is a discrete valuation ring (see Chapter 7 in [Gal12]). The uniformizer at P is defined as a prime element (unique up to associates) in $O_{\mathrm{C},P}(C)$, and can be given as follows:

$$u_P = \begin{cases} y, & \text{if } w(P) = P, \\ x - x_0, & \text{if } w(P) \neq P, \\ \frac{x}{y}, & \text{if } P = \infty. \end{cases}$$

where w is the Hyperelliptic involution, defined as a map $w : C \longrightarrow C, (x, y) \longmapsto (x, -y)$.

A function g on C is a rational function in $\mathbf{C}(x, y)$ that is defined for at least one point on C. Viewing g as a map from points on C to $\mathbf{P}^1_{\mathrm{C}}$, we define the order of g at P. Denoted by $\mathrm{ord}_P(g)$, it is the number r such that

$$g \cdot u_P^{-r}(P) \neq 0, \infty.$$

Example 2.1.5. *For the curve $y^2 = x(x^2+1)$, we have:*

$$\mathrm{ord}_{(0,0)}(x) = 2, \mathrm{ord}_{(0,0)}(y) = \mathrm{ord}_{(\pm i,0)}(y) = 1,$$
$$\mathrm{ord}_{(1,\pm\sqrt{2})}(\frac{y}{(x-1)^2}) = -2, \ \textit{and}\ \mathrm{ord}_{\infty}(\frac{x^2+1}{y}) = -1.$$

Definition 2.1.6. *Let g be a function on C that is not identically zero, the divisor of f is defined as*

$$\mathrm{div}(g) = \sum_{P\in C} \mathrm{ord}_P(g)[P].$$

The divisor of a function is called a principal divisor.

Proposition 2.1.7. *Let g and g' be functions on C that are not identically zero, then*

$$\deg(\mathrm{div}(g)) = 0,$$
$$\mathrm{div}(g\cdot g') = \mathrm{div}(g) + \mathrm{div}(g'),$$
$$\mathrm{div}(\frac{1}{g}) = -\mathrm{div}(g),$$
$$\mathrm{div}(g) = \mathbf{0} \iff g \in \mathbf{C}^*.$$

Proof. See Proposition II. 3.1 in [Sil09]. □

The above proposition implies that principal divisors on C form a subgroup of $\mathrm{Div}^0(C)$. This allows us to define the Picard group.

Definition 2.1.8. *For a smooth hyperelliptic curve C, the Picard group* $\mathrm{Pic}^0(C)$ *consists of divisors of degree 0 modulo principal divisors.*

The Jacobian of a hyperelliptic curve $J(C)$ is isomorphic to the Picard group $\mathrm{Pic}^0(C)$. In this thesis, we use divisor to refer to any point in the Jacobian. More details about Weil divisors and construction of Jacobians of smooth hyperelliptic curves can be found in Chapter 11 and Chapter 13 in [Was08].

2.2 Mumford Representation

Definition 2.2.1. *A divisor $D = \sum_{j=1}^n c_j([P_j]-[\infty])$ with $P_j = (x_j, y_j)$, is called semi-reduced if the following hold:*

(1) $c_j \geq 0$ for all j.

(2) If $[P_j]$ occurs in the sum (i.e., $c_j > 0$), then $[w(P_j)]$ does not occur.

If, in addition, $\sum_j c_j \leq g$, then D is called reduced.

It turns out that any divisor $D = \sum_{j=1}^n([P_j] - [\infty])$ is equivalent to a semi-reduced divisor. To prove this, we proceed as follows: we first remove all terms of the form $[P] + [w(P)] - 2[\infty]$ in D, as it is a principal divisor $(x - x_P)$, where $P = (x_P, y_P)$. Then, for each P_j with $c_j < 0$, we add D by $(-c_j)([P_j] + [w(P_j)] - 2[\infty])$. In this way, the resulting divisor is semi-reduced and equivalent to D. For semi-reduced divisors, there is a one-to-one correspondence between them and a pair of polynomials satisfying certain conditions.

Theorem 2.2.2 ([Was08]). *There exists a one-to-one correspondence between semi-reduced divisors $D = \sum_{j=1}^n c_j([P_j] - [\infty])$ in $J(C)$ and pairs of polynomials $(U(x), V(x))$ satisfying*

(1) U is monic,

(2) $\deg(U) = \sum_{j=1}^n c_j$ and $\deg(V) < \deg(U)$,

(3) $U \mid f - V^2$.

Under this correspondence, $D = \gcd(\mathrm{div}(U), \mathrm{div}(y - V))$, i.e., $D = \sum_{j=1}^n c_j([(x_j, V(x_j))] - [\infty])$, where $U(x) = \prod_{j=1}^n (x - x_j)^{c_j}$.

Proof. See Theorem 13.5 in [Was08]. □

Theorem 2.2.3 ([Was08])**.** *Each divisor class in $J(C)$ contains a unique reduced divisor.*

Proof. See Proposition 13.6 in [Was08]. □

Theorem 2.2.4 ([Was08])**.** *[Mumford representation] There is a one-to-one correspondence between divisor class in $J(C)$ and pairs of polynomials satisfying*
(1) U is monic,
(2) $\deg(V) < \deg(U) \leq g$,
(3) $U \mid f - V^2$.

Proof. Straightforward from Theorem 2.2.2 and Theorem 2.2.3. □

For each divisor class in $J(C)$, the corresponding pair of polynomials (U, V) for its reduced divisor is called the **Mumford representation** of this divisor class.

Proposition 2.2.5. *Let (U, V) be a pair representing a semi-reduced divisor D in $J(C)$. The reduction of (U, V) proceeds as follows:*
1. Compute $\widetilde{U} = \frac{f-V^2}{U}$, and multiply U by a constant to make U monic.
2. Compute $\widetilde{V} \equiv -V \pmod{\widetilde{U}}$ such that $\deg(\widetilde{V}) < \deg(\widetilde{U})$.
3. Output $(\widetilde{U}, \widetilde{V})$.

Remark 2.2.6. *The reduction described above differs from the reduction procedure in Theorem 13.9 in [Was08]. The latter is in fact repeated reductions (given in Proposition 2.2.5) until $\deg(U) \leq g$. Throughout this thesis, unless specifically stated otherwise, "reduction" refers only to the one given in Proposition 2.2.5. We clarify this to avoid any confusion.*

We refer to $(\widetilde{U}, \widetilde{V})$ as the **reduction result** of (U, V), or simply say that (U, V) **is reduced to** $(\widetilde{U}, \widetilde{V})$. The divisor represented by $(\widetilde{U}, \widetilde{V})$ is equivalent to the one represented by (U, V), the proof can be found in Theorem 13.9 in [Was08]. Moreover, when $\deg(U) > g$, we have

$$\deg(\widetilde{U}) + \deg(U) = \deg(f - V^2) = max\{2g + 1, 2\deg(V)\} < 2\deg(U).$$

This implies $\deg(\tilde{U}) < \deg(U)$.

Given any divisor D (represented by (U, V)) in $J(C)$, by repeatedly applying the reduction until $\deg(U) \leq g$, we can obtain the Mumford representation of the divisor class of D. This process (called reduction procedure in Theorem 13.9 in [Was08]) provides an algorithm to obtain the Mumford representation of any divisor class in $J(C)$.

2.3 Cantor's algorithm

Theorem 2.3.1 ([Can87])**.** *[Cantor's algorithm] Let D_1 and D_2 be semi-reduced divisors in $J(C)$, represented by (U_1, V_1) and (U_2, V_2), respectively, as in Theorem 2.2.2.*
1. Compute $d = gcd(U_1, U_2, V_1 + V_2)$ and set d to be monic. Find polynomials h_1, h_2, h_3 such that

$$d = U_1h_1 + U_2h_2 + (V_1 + V_2)h_3.$$

2. Compute

$$V_0 = (U_1V_2h_1 + U_2V_1h_2 + (f + V_1V_2)h_3)/d.$$

3. Compute

$$U = U_1U_2/d^2,\ V \equiv V_0 \pmod{U} \ \textit{with} \deg(V) < \deg(U).$$

4. Compute

$$\widetilde{U} = \frac{f - V^2}{U}.$$

And multiply U by a constant to make U monic.

5. Compute

$$\widetilde{V} \equiv -V \pmod{\widetilde{U}} \text{ \textit{with} } \deg(\widetilde{V}) < \deg(\widetilde{U}).$$

6. If $\deg(U) > g$, go back to step 4; otherwise, continue.

7. Output (U, V).

The pair (U, V) is the Mumford representation of the divisor class of $D_1 + D_2$.

The algorithm given in the above theorem is called Cantor's algorithm, it provides an implementation of the addition law of divisor classes in Mumford representations. The proof can be found in Theorem 13.10 in [Was08]. We divide Cantor's algorithm into two parts, step 1-3 and step 4-6. The first 3 steps are referred to as **Cantor Composition**, which computes the pair of polynomials corresponding to divisor $D_1 + D_2$. Step 4-6 are reduction procedure (given by Theorem 13.9 in [Was08]). It outputs the pair of polynomials corresponding to the reduced divisors equivalent to $D_1 + D_2$. Cantor composition plays a crucial role in Chapter 3 and Chapter 4 as it can be used to implement the addition of divisor classes in the Jacobians of singular hyperelliptic curves.

3 Arithmetic on Jacobians of singular hyperelliptic curves of geometric genus zero

A singular curve C of geometric genus zero is defined by $y^2 = f(x) = h^2(x)x$, where $\deg(h(x)) = g$. We write $h(x) = \prod_{i=1}^{k}(x - c_i)^{n_i}$ with $c_i \neq c_j$, $\forall i \neq j$. In Section 3.1, we introduce the generalized Mumford representation, which corresponds to each divisor class in $J(C)$ with a pair of polynomial $(a^2, a\bar{V})$ satisfying the following conditions:

(1) $a \mid h$, and a is monic.

(2) $\deg(\bar{V}) < \deg(a)$.

(3) $\gcd(a, \frac{f}{a^2} - \bar{V}^2) = 1$.

Moreover, we demonstrate that Cantor composition can be used to implement the addition of divisor classes in the generalized Mumford representation.

In Section 3.2, we prove the decomposition $J(C) \cong \prod_{i=1}^{k} J(C_i)$, where $C_i : y^2 = (x - c_i)^{2n_i}x$, $\forall 1 \leq i \leq k$. In Section 3.3, we first provide two explicit group isomorphisms:

$$J(C : y^2 = x^{2g+1}) \longrightarrow \mathbf{C}^g,$$
$$\sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n}(\frac{x_j}{y_j}, \frac{x_j^2}{y_j}, \cdots, \frac{x_j^g}{y_j}).$$

and

$$J(C : y^2 = x^{2g}(x - c)) \longrightarrow \mathbf{C}^{g-1} \times \mathbf{C}^*,$$
$$\sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto (\sum_{j=1}^{n} \frac{x_j(x_j - c)}{y_j}, \cdots, \sum_{j=1}^{n} \frac{x_j^{g-1}(x_j - c)}{y_j}, \prod_{j=1}^{n} \frac{y_j + \beta x_j^g}{y_j - \beta x_j^g})$$

where β is a square root of $-c$. Combining these two isomorphisms with the decomposition proved in Section 3.2, we then construct an explicit group isomorphism from $J(C)$ to $\mathbf{C}^{g-l} \times (\mathbf{C}^*)^l$, where l is number of c_i $(1 \leq i \leq k)$ which are not equal to 0.

3.1 Generalized Mumford Representation

In this section, we introduce the generalized Mumford representation for the Jacobian group of singular hyperelliptic curves of geometric genus 0. This representation also applies to divisor classes in a subgroup of the Jacobians of singular curves of positive geometric genus.

Definition 3.1.1. *A singular hyperelliptic curve C of arithmetic genus g is defined by*

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

where $\deg(f(x)) = 2g + 1$, *$e(x)$ has no repeated roots, and both h and e are monic polynomials.*

Remark 3.1.2. *By construction,* $\deg(e(x))$ *is odd. The geometric genus of C is* 0 *if and only if* $\deg(e(x)) = 1$. *When* $\deg(e(x)) = 1$, *for simplicity, we fix $e(x) = x$ as this can always be achieved through an appropriate linear transformation without loss of generality.*

When $\deg(e(x)) \geq 3$, *C has positive geometric genus, which we will discuss in Chapter 4.*

Definition 3.1.3. *A singular hyperelliptic curve C of geometric genus 0 is defined by*

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

where $h(x)$ is a monic polynomial and $\deg(h(x)) = g$.

Remark 3.1.4. *A point $(x, y) \in C$ is called singular if $2y = f'(x) = 0$, where f' is the derivative of f. For the curve C defined by $y^2 = h^2(x)e(x)$, singular points are $\{(c, 0) \mid h(c) = 0\}$.*

Definition 3.1.5. *Given a singular hyperelliptic curve C, the Jacobian group of C, denoted by $J(C)$ is isomorphic to $\mathrm{Pic}^0(C)$, which consists of Weil divisors of degree 0 that only have support on nonsingular points. Two divisors D and D' in $\mathrm{Pic}^0(C)$ are equivalent if and only if there exists a rational function $g(x, y) \in \mathbb{C}(C)$ such that $\mathrm{div}(g(x, y)) = D - D'$ and $g(x, y)$ does not vanish at singular points.*

Remark 3.1.6. *For more details about this definition, see Chapter 9 in [BLR12]. Strictly speaking, the Jacobian described above is the generalized Jacobian, which can also be defined on nonsingular curves.*

Proposition 3.1.7. *Given a singular hyperelliptic curve C, there is a one-to-one correspondence between semi-reduced divisors $D = \sum_{j=1}^{n}([P_j] - [\infty])$ in $J(C)$ and pairs of polynomials $(U(x), V(x))$ satisfying*
(1) U is monic and is nonzero at singular points,
(2) $\deg(U) = \sum_{j=1}^{n} c_j$ and $\deg(V) < \deg(U)$,
(3) $U \mid f - V^2$.
Under this correspondence, $D = \gcd(\mathrm{div}(U), \mathrm{div}(y - V))$, i.e., $D = \sum_{j=1}^{n} c_j([(x_j, V(x_j))] - [\infty])$, where $U(x) = \prod_{j=1}^{n}(x - x_j)^{c_j}$.

Proof. As none of P_j is singular, U is nonzero at singular points. The proof of correspondence is the same as Theorem 2.2.2. □

Remark 3.1.8. *Due to the one-to-one correspondence established in Proposition 3.1.7, by abuse of notation, we identify a pair (U, V) satisfying the above conditions with its corresponding divisor in $J(C)$. For simplicity, we may refer to (U, V) directly, assuming by default that the conditions are satisfied.*

Remark 3.1.9. *If both (U, V) and its reduction result $(\widetilde{U}, \widetilde{V})$ represent some divisors in $J(C)$, then (U, V) is equivalent to $(\widetilde{U}, \widetilde{V})$. The proof is the same as in Theorem 13.9 in [Was08].*

Remark 3.1.10. *For any pair (U, V) representing a divisor in $J(C)$, multiplying U by a nonzero constant does not affect the computations in this thesis. For simplicity, we omit this step from the notation for the rest of the thesis.*

For a nonsingular hyperelliptic curve, the Riemann-Roch Theorem establishes that each divisor class contains a unique reduced divisor (see the proof of Theorem 2.2.3). Consequently, there is a one-to-one correspondence between divisor classes and pairs (U, V) satisfying certain conditions. Such pairs (U, V) are called the Mumford representation. However, in the singular case, some divisor classes may not contain a reduced divisor, making the Mumford representation unsuitable for representing all elements in the Jacobian group. Therefore, we propose a novel representation of divisor classes in the Jacobian group of singular hyperelliptic curves of geometric genus zero.

Theorem 3.1.11. *Let C be a singular hyperelliptic curve of geometric genus 0. There is a one-to-one correspondence between divisor classes in $J(C)$ and pairs of polynomials $(a^2, a\bar{V})$ satisfying the following conditions:*
(1) $a \mid h$, a is monic.
(2) $\deg(\bar{V}) < \deg(a)$.
(3) $\gcd(a, \frac{f}{a^2} - \bar{V}^2) = 1$.
We call the pair $(a^2, a\bar{V})$ the generalized Mumford representation.

We will prove the theorem through a series of intermediate theorems and propositions in this section. First, we establish that the pair $(a^2, a\bar{V})$ indeed represents a unique divisor class in $J(C)$ in Theorem 3.1.12. Next, in Theorem 3.1.16, we show that addition is closed within divisor classes represented by this new representation. Moreover, we demonstrate that addition of divisor classes in this representation can be efficiently performed using Cantor composition. Finally, we prove that every divisor class can be uniquely expressed using this representation in Propositions 3.1.18 and 3.1.19. Consequently, this representation provides a complete description of the Jacobian group, which we refer to as the Generalized Mumford Representation.

Theorem 3.1.12. *Let C be a singular hyperelliptic curve. A pair of polynomials $(a^2(x), a(x)\bar{V}(x))$ satisfying the following conditions represents a divisor class in $J(C)$:*

(1) $a \mid h$, and a is monic.

(2) $\deg(\bar{V}) < \deg(a)$.

(3) $\gcd(a, \frac{f}{a^2} - \bar{V}^2) = 1$.

Any divisor (U, V) that can be reduced to $(a^2, a\bar{V})$, i.e., $a^2 = \frac{f-V^2}{U}$, and $a\bar{V} \equiv -V \pmod{a^2}$ with $\deg(\bar{V}) < \deg(a)$, is a representative of this divisor class.

Proof. As $a \mid h$, there does not exist a divisor D corresponding to $(a^2, a\bar{V})$ through the relation given in Proposition 3.1.7. However, we can show that:

1. There exist infinitely many divisors that can be reduced to $(a^2, a\bar{V})$.
2. All such divisors are equivalent and hence represent the same divisor class.

Step 1. Show existence of infinitely many divisors that can be reduced to $(a^2, a\bar{V})$.

Define $V(x) := a^2(x)w(x) - a(x)\bar{V}(x)$, $U(x) := \frac{f(x)-V^2(x)}{a^2(x)}$, where $w(x)$ is chosen to satisfy:

$$\deg(V) > \max\{g, \deg(a^2)\}, \text{ and } \gcd(h, U) = 1. \qquad (\star)$$

Under these conditions, $\deg(V) > g$ and $\deg(V) > \deg(a^2)$, so $\deg(U) = \deg(f - V^2) - \deg(a^2) = \deg(V^2) - \deg(a^2) > \deg(V)$. Hence, (U, V) corresponds to a divisor by construction. And it is clear that $(a^2, a\bar{V})$ is the reduction result of (U, V). Moreover, there exist infinitely many $w(x)$ satisfying condition $(\star)$, so there are infinitely many divisors which can be reduced to $(a^2, a\bar{V})$.

Step 2. Show the equivalence of divisors that can be reduced to $(a^2, a\bar{V})$.

Assume both (U_1, V_1) and (U_2, V_2) can be reduced to $(a^2, a\bar{V})$. Then:

$$U_i = \frac{f}{a^2} - (\frac{V_i}{a})^2, \text{ and } -V_i \equiv a\bar{V} \pmod{a^2}, \; i = 1, 2.$$

Define:

$$H(x, y) := (\frac{y}{a} - \frac{V_1}{a})(\frac{y}{a} + \frac{V_2}{a}).$$

We claim that $\operatorname{div}(H(x, y)) = (U_1, V_1) - (U_2, V_2)$. This holds because $H(x, y)$ vanishes exactly at points in the Weil divisor of $(U_1, V_1) - (U_2, V_2)$. We only need to check that $H(x, y)$ does not vanish at any singular points.

Write $V_i = a^2 w_i - a\bar{V}$ for some w_i, $i = 1, 2$, so:

$$U_i = \frac{f}{a^2} - (aw_i - \bar{V})^2, i = 1, 2.$$

Since $\gcd(U_i, h) = 1$, evaluating U_i at a singular point $(c, 0)$ where $(x - c) \nmid a$ gives:

$$U_i|_{x=c} = (aw_i - \bar{V})^2|_{x=c} \neq 0 \implies (aw_i - \bar{V})|_{x=c} \neq 0,\ i = 1, 2. \tag{3.1}$$

Expand H:

$$H(x, y) = (\frac{y}{a} - aw_1 + \bar{V})(\frac{y}{a} + aw_2 - \bar{V}) = \frac{f}{a^2} + y(w_2 - w_1) - (aw_1 - \bar{V})(aw_2 - \bar{V}).$$

At any singular point $(c, 0)$, we evaluate $H(x, y)$ at $(c, 0)$:
1. If $x - c \mid a$, then $H(c, 0) = (\frac{f}{a^2} - \bar{V}^2)|_{x=c} \neq 0$ by condition 3 we imposed.
2. If $x - c \nmid a$, then $H(c, 0) = -(aw_1 - \bar{V})(aw_2 - \bar{V})|_{x=c} \neq 0$ by Equation (3.1).

Thus, H does not vanish at any singular points, the difference $(U_1, V_1) - (U_2, V_2)$ is a principal divisor. So $(U_1, V_1) \sim (U_2, V_2)$.

Since any two divisors that can be reduced to $(a^2, a\bar{V})$ are equivalent, we can let $(a^2, a\bar{V})$ represent the divisor class of divisors that can be reduced to it. The existence of infinite many such divisors guarantees that $(a^2, a\bar{V})$ is a valid representation. The equivalence of such divisors ensures that $(a^2, a\bar{V})$ represents a unique divisor class in $J(C)$. □

Remark 3.1.13. *It is worth noting that the pair* $(1, 0)$ *also satisfies conditions in Theorem 3.1.12, as we allow* $\deg(0) = -1$. *Since any divisor* (U, V) *that can be reduced to* $(1, 0)$ *is a principal divisor,* $\operatorname{div}(y - V)$*, it follows that* $(1, 0)$ *represents the zero divisor class in* $J(C)$*. This coincides with the Mumford Representation in the smooth case.*

Proposition 3.1.14. *Let C be a singular hyperelliptic curve. Let $(a^2, a\bar{V})$ be a pair of polynomials satisfying three conditions in Theorem 3.1.12. If in addition* $\gcd(h, \frac{f}{a^2} - \bar{V}^2) = 1$*, then $(\widetilde{U}, \widetilde{V})$ is a representative of $(a^2, a\bar{V})$, where:*

$$\widetilde{U} = \frac{f}{a^2} - \bar{V}^2,\ \textit{and}\ \widetilde{V} \equiv -a\bar{V} \pmod{\widetilde{U}}\ \textit{with}\ \deg(\widetilde{V}) < \deg(\widetilde{U}),$$

i.e., $(\widetilde{U}, \widetilde{V})$ is the reduction result of $(a^2, a\bar{V})$.

Proof. Choose a proper w satisfying condition $(\star)$ such that the corresponding (U, V) is a representative of $(a^2, a\bar{V})$, where:

$$U = \frac{f}{a^2} - (aw - \bar{V})^2, V = a^2 w - a\bar{V}.$$

To show that (U, V) is equivalent to $(\widetilde{U}, \widetilde{V})$, we define:

$$H(x, y) := (\frac{y}{a} - (aw - \bar{V}))(\frac{y}{a} - \bar{V}).$$

We claim that $\operatorname{div}(H(x, y)) = (U, V) - (\widetilde{U}, \widetilde{V})$. Observe that H vanishes precisely at points in the Weil divisor of $(U, V) - (\widetilde{U}, \widetilde{V})$. We only need to show that H does not vanish at any singular points.

Expanding H gives:

$$H(x, y) = \frac{f}{a^2} + (aw - \bar{V})\bar{V} - wy.$$

Take any singular point $(c, 0)$, we evaluate $H(x, y)$ at $(c, 0)$:
1. If $(x - c) \mid a$, then $H(c, 0) = (\frac{f}{a^2} - \bar{V}^2)|_{x=c} \neq 0$ since $\gcd(a, \frac{f}{a^2} - \bar{V}^2) = 1$.

2. If $(x-c) \nmid a$, then $\frac{f}{a^2}|_{x=c} = 0$, so:

$$\gcd(\frac{h}{a}, \frac{f}{a^2} - \bar{V}^2) = 1 \implies 0 \neq (\frac{f}{a^2} - \bar{V}^2)|_{x=c} = -\bar{V}^2|_{x=c} \implies \bar{V}|_{x=c} \neq 0.$$

From condition 3.1, $(aw - \bar{V})|_{x=c} \neq 0$. Thus, $H(c,0) = (aw - \bar{V})\bar{V}|_{x=c} \neq 0$.

Hence $H(x,y)$ does not vanish at any singular points, Therefore, $\mathrm{div}(H(x,y)) = (U,V) - (\widetilde{U}, \widetilde{V})$. This shows that $(\widetilde{U}, \widetilde{V})$ lies in the divisor class represented by $(a^2, a\bar{V})$, i.e., $(\widetilde{U}, \widetilde{V})$ is the representative of $(a^2, a\bar{V})$. □

Lemma 3.1.15. *Let $(a_1^2, a_1\bar{V}_1), (a_2^2, a_2\bar{V}_2)$ satisfy the three conditions in Theorem 3.1.12. Let $d = \gcd(a_1^2, a_2^2, a_1\bar{V}_1 + a_2\bar{V}_2)$, and let $(c, 0)$ be a singular point such that $(x-c) \mid a_1$ and $(x-c) \mid a_2$. Then, we have:*

$$(x-c) \mid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d} \text{ or } (x-c) \nmid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d}.$$

Proof. Let the multiplicity of $(x-c)$ in h be n, and let the multiplicities of $(x-c)$ in a_1 and a_2 be m_1 and m_2, respectively. W.l.o.g, we assume $m_1 \leq m_2 \leq n$.

1. If $m_1 < m_2 \leq n$, then $\frac{f}{a_1^2}|_{x=c} = 0$. And from $\gcd(a_1, \frac{f}{a_1^2} - \bar{V}_1^2) = 1$, we have:

$$(\frac{f}{a_1^2} - \bar{V}_1^2)|_{x=c} = -\bar{V}_1^2|_{x=c} \neq 0 \implies \bar{V}_1(c) \neq 0.$$

Thus, the multiplicity of $(x-c)$ in $a_1\bar{V}_1 + a_2\bar{V}_2$ is m_1. Consequently, the multiplicity of $(x-c)$ in d is m_1, so:

$$(x-c) \mid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d}.$$

2. If $m_1 = m_2 \leq n$, the multiplicities of $(x-c)$ in $\frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d}$ are identical. Therefore:

$$(x-c) \mid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d} \text{ or } (x-c) \nmid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d}.$$

This completes the proof. □

Theorem 3.1.16. *Let C be a singular hyperelliptic curve, and let S denote the set of pairs of polynomials $(a^2, a\bar{V})$ that satisfy the conditions in Theorem 3.1.12. Identifying each element of S with its corresponding divisor class, S is closed under addition, and addition can be performed using Cantor composition.*

Proof. The proof sketch is:

(1) Given any two divisor classes $(a_1^2, a_1\bar{V}_1)$ and $(a_2^2, a_2\bar{V}_2)$ in S, we apply Cantor composition to $(a_1^2, a_1\bar{V}_1) + (a_2^2, a_2\bar{V}_2)$ and get result $(a_3^2, a_3\bar{V}_3)$.

(2) We show $(a_3^2, a_3\bar{V}_3) \in S$, i.e, it satisfies three conditions in Theorem 3.1.12.

(3) We show $(a_1^2, a_1\bar{V}_1) + (a_2^2, a_2\bar{V}_2) = (a_3^2, a_3\bar{V}_3)$.

Step 1. Apply Cantor composition to $(a_1^2, a_1\bar{V}_1) + (a_2^2, a_2\bar{V}_2)$.

Let (U, V) be the result of Cantor composition of $(a_1^2, a_1\bar{V}_1) + (a_2^2, a_2\bar{V}_2)$. Define $d = \gcd(a_1^2, a_2^2, a_1\bar{V}_1 + a_2\bar{V}_2)$ with d chosen to be monic. There exist h_1, h_2, h_3 such that

$$d = a_1^2h_1 + a_2^2h_2 + (a_1\bar{V}_1 + a_2\bar{V}_2)h_3, \quad \text{or equivalently,} \quad 1 = \frac{a_1^2}{d}h_1 + \frac{a_2^2}{d}h_2 + \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d}h_3. \tag{3.2}$$

We then compute:

$$U = \frac{a_1^2 a_2^2}{d^2},\ V \equiv (a_1^2 a_2 \bar{V}_2 h_1 + a_2^2 a_1 \bar{V}_1 h_2 + (f + a_1 a_2 \bar{V}_1 \bar{V}_2) h_3)/d \pmod{U} \text{ with } \deg(V) < \deg(U).$$

To simplify notation, let:

$$a_3 = \frac{a_1 a_2}{d},\ \bar{V}_3 \equiv a_1 \bar{V}_2 h_1 + a_2 \bar{V}_1 h_2 + \frac{f}{a_1 a_2} h_3 + \bar{V}_1 \bar{V}_2 h_3 \pmod{a_3} \text{ with } \deg(\bar{V}_3) < \deg(a_3). \tag{3.3}$$

Thus (U, V) can be expressed as $(a_3^2, a_3 \bar{V}_3)$.

Step 2. Show $(a_3^2, a_3\bar{V}_3) \in S$.

Fix any $i = 1, \cdots, k$, let $(x - c_i)$ divide a_1 with multiplicity m_1, and a_2 with multiplicity m_2. Without loss of generality, assume $m_1 \leq m_2 \leq n_i$. The multiplicity of $(x - c_i)$ in $a_1\bar{V}_1 + a_2\bar{V}_2$ is at least m_1, then the multiplicity of $(x - c_i)$ in d is at least m_1. Therefore, the multiplicity of $(x - c_i)$ in $\frac{a_1a_2}{d}$ is at most $m_2 \leq n_i$. Thus, $a_3 = \frac{a_1a_2}{d}$ divides h, and since a_1, a_2, d are monic, a_3 is monic. From the definition of $\bar{V}_3$, it is evident that $\deg(\bar{V}_3) < \deg(a_3)$ due to the modular reduction. What's left is to show that $\gcd(a_3, \frac{f}{a_3^2} - \bar{V}_3^2) = 1$. Take any singular point $(c, 0)$ where $(x - c) \mid a_3$, there are two cases:

Case 2.1. $(x - c)$ *divides both* a_1 *and* a_2

According to Lemma 3.1.15, we have $(x - c) \mid \frac{a_1^2}{d}, (x - c)\frac{a_2^2}{d}$ as $(x - c) \mid \frac{a_1a_2}{d}$. From Equation (3.2), it follows that $1 \equiv \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d} h_3 \pmod{x - c}$. Moreover, from Equation (3.3), we obtain $\bar{V}_3 \equiv \frac{f}{a_1a_2}h_3 + \bar{V}_1\bar{V}_2h_3 \pmod{x - c}$. When we compute $\frac{f}{a_3^2} - \bar{V}_3^2$ modulo $x - c$, we substitute these expressions and find:

$$\begin{aligned}
\frac{f}{a_3^2} - \bar{V}_3^2 &\equiv \frac{f}{a_1^2a_2^2/d^2} - (\frac{f}{a_1a_2} + \bar{V}_1\bar{V}_2)^2 h_3^2 \\
&\equiv h_3^2[\frac{(a_1\bar{V}_1 + a_2\bar{V}_2)^2}{d^2} \cdot \frac{f}{a_1^2a_2^2/d^2} - (\frac{f}{a_1a_2} + \bar{V}_1\bar{V}_2)^2] \\
&\equiv -h_3^2(\frac{f}{a_1^2} - \bar{V}_1^2)(\frac{f}{a_2^2} - \bar{V}_2^2) \not\equiv 0. \pmod{x - c}
\end{aligned}$$

Case 2.2. $(x - c)$ *divides only one of* a_1 *or* a_2

We assume $(x - c) \mid a_1$ and $(x - c) \nmid a_2$ without loss of generality. In this case, we have $(x - c) \nmid d$, $(x - c) \mid \frac{f}{a_1a_2}$. Using Equation (3.2) and Equation (3.3), we get $d \equiv a_2^2h_2 + a_2\bar{V}_2h_3 \pmod{x - c}$ and $\bar{V}_3 \equiv a_2\bar{V}_1h_2 + \bar{V}_1\bar{V}_2h_3 \pmod{x - c}$. Substituting these expressions when computing $\frac{f}{a_3^2} - \bar{V}_3^2$ modulo $x - c$, we can get

$$\begin{aligned}
\frac{f}{a_3^2} - \bar{V}_3^2 &\equiv \frac{f}{a_1^2a_2^2/d^2} - (a_2\bar{V}_1h_2 + \bar{V}_1\bar{V}_2h_3)^2 \equiv \frac{1}{a_2^2}(\frac{f}{a_1^2/d^2} - (a_2^2\bar{V}_1h_2 + a_2\bar{V}_1\bar{V}_2h_3)^2) \\
&\equiv \frac{d^2}{a_2^2}(\frac{f}{a_1^2} - \bar{V}_1^2) \not\equiv 0. \pmod{x - c}
\end{aligned}$$

In both case, $(\frac{f}{a_3^2} - \bar{V}_3^2)$ does not vanish modulo $x - c$ for any $(x - c) \mid a_3$, which implies that $\gcd(a_3, \frac{f}{a_3^2} - \bar{V}_3^2) = 1$. Thus $(a_3^2, a_3\bar{V}_3)$ satisfies all three conditions in Theorem 3.1.12, and is a valid representation in S.

Step 3. Show $(a_1^2, a_1\bar{V}_1) + (a_2^2, a_2\bar{V}_2) = (a_3^2, a_3\bar{V}_3)$.

We choose proper w_j satisfying condition ($\star$) such that the corresponding (U_j, V_j) lies in $(a_j^2, a_j\bar{V}_j)$, where

$$V_j = a_j^2 w_j - a_j\bar{V}_j, \quad U_j = \frac{f}{a_j^2} - (a_j w_j - \bar{V}_j)^2, \quad \forall j = 1, 2, 3.$$

To show $(a_1^2, a_1\bar{V}_1) + (a_2^2, a_2\bar{V}_2) = (a_3^2, a_3\bar{V}_3)$ is equivalent to show that $(U_1, V_1) + (U_2, V_2) \sim (U_3, V_3)$. Consider

$$H(x, y) = (\frac{y}{a_1} - (a_1 w_1 - \bar{V}_1))(\frac{y}{a_2} - (a_2 w_2 - \bar{V}_2))(\frac{y}{a_3} + (a_3 w_3 - \bar{V}_3)),$$

we claim that $\mathrm{div}(H(x, y)) = (U_1, V_1) + (U_2, V_2) - (U_3, V_3)$.

It is evident from the factorization form of $H(x, y)$ that $H(x, y)$ vanishes precisely at points in the Weil divisor of $(U_1, V_1) + (U_2, V_2) - (U_3, V_3)$. To complete the proof, we need to demonstrate that H does not vanish at singular points. Take any singular point $(c, 0)$, there are three cases.

Case 3.1. $(x - c) \nmid a_1$ *and* $(x - c) \nmid a_2$

In this case, we also have $(x - c) \nmid a_3$. This means that $\frac{y}{a_j}|_{(c,0)} = 0$ for $j = 1, 2, 3$. Thus, $H(c, 0) = \prod_{j=1}^{3}(a_j w_j - \bar{V}_j)|_{(c,0)} \neq 0$ by Equation (3.1).

Case 3.2. $(x - c) \mid a_1$ *and* $(x - c) \nmid a_2$

In this case, $(x - c)$ only divides one of a_1 and a_2. Without loss of generality, we assume $(x - c) \mid a_1, (x - c) \nmid a_2$. Then $(x - c) \nmid d, (x - c) \mid \frac{a_1a_2}{d} = a_3$, and $(x - c) \mid \frac{f}{a_1a_2}$. Substituting these when evaluating $H(x, y)$ at $(c, 0)$, we have:

$$H(c, 0) = (\frac{y}{a_1} + \bar{V}_1)\underbrace{(-(a_2 w_2 - \bar{V}_2))}_{\textcircled{1}}(\frac{y}{a_1a_2/d} - \bar{V}_3)|_{(c,0)}.$$

Since $\textcircled{1}|_{(x=c)} \neq 0$ by Equation (3.1), $H(c, 0) \neq 0$ if and only if $H'(x, y) = (\frac{y}{a_1} + \bar{V}_1)(\frac{y}{a_1a_2/d} - \bar{V}_3)$ does not vanish at $(c, 0)$. Expand $H'(x, y)$, we get:

$$H'(x, y) = \underbrace{\frac{f}{a_1^2a_2/d} - \bar{V}_1\bar{V}_3}_{\textcircled{2}} + \frac{y}{a_1a_2/d}\underbrace{(\bar{V}_1 - \frac{a_2}{d}\bar{V}_3)}_{\textcircled{3}}.$$

Equation (3.2) and Equation (3.3) implies that $\bar{V}_3 \equiv a_2\bar{V}_1h_2 + \bar{V}_1\bar{V}_2h_3 \pmod{x - c}$, and $d \equiv a_2^2h_2 + a_2\bar{V}_2h_3$ $(\mathrm{mod}\ x - c)$. So we compute:

$$\textcircled{2} \equiv \frac{f}{a_1^2a_2/d} - \bar{V}_1(a_2\bar{V}_1h_2 + \bar{V}_1\bar{V}_2h_3) \equiv \frac{f}{a_1^2a_2/d} - \bar{V}_1^2\frac{d}{a_2} \equiv \frac{d}{a_2}(\frac{f}{a_1^2} - \bar{V}_1^2) \not\equiv 0. \quad (\mathrm{mod}\ x - c)$$

And

$$\begin{aligned}\textcircled{3} &\underset{Eq(3.3)}{\equiv} \bar{V}_1 - \frac{a_2}{d}(a_1\bar{V}_2h_1 + a_2\bar{V}_1h_2 + \frac{f}{a_1a_2}h_3 + \bar{V}_1\bar{V}_2h_3) \equiv \bar{V}_1(1 - \frac{a_2^2}{d}h_2) - \frac{a_2}{d}(\frac{f}{a_1a_2}h_3 + \bar{V}_1\bar{V}_2h_3)\\ &\underset{Eq(3.2)}{\equiv} (\frac{a_1^2}{d}h_1 + \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d}h_3)\bar{V}_1 - \frac{a_2}{d}(\frac{f}{a_1a_2}h_3 + \bar{V}_1\bar{V}_2h_3) \equiv \frac{a_1}{d}(a_1\bar{V}_1h_1 + \bar{V}_1^2h_3 - \frac{f}{a_1^2}h_3). \quad (\mathrm{mod}\ \frac{a_1a_2}{d})\end{aligned}$$

Thus,

$$\frac{y}{a_1a_2/d} \times \textcircled{3} = \frac{y}{a_1a_2/d} \cdot \frac{a_1}{d}(\cdots) + y(\cdots) = \frac{y}{a_2}(\cdots) \implies \frac{y}{a_1a_2/d} \times \textcircled{3}|_{(c,0)} = 0.$$

Hence, $H'(c,0) = (② + \frac{y}{a_1a_2/d} \times ③)|_{(c,0)} \neq 0$, which implies $H(c,0) \neq 0$.

Case 3.3. $(x-c) \mid a_1$ *and* $(x-c) \mid a_2$

In this case, $(x-c) \mid d$. Expand H:

$$\begin{aligned}
H(x,y) &= (\frac{y}{a_1} - (a_1w_1 - \bar{V}_1))(\frac{y}{a_2} - (a_2w_2 - \bar{V}_2))(\frac{y}{a_1a_2/d} + (\frac{a_1a_2}{d}w_3 - \bar{V}_3)) \\
&= \underbrace{\overbrace{(\frac{f}{a_1a_2} + (a_1w_1 - \bar{V}_1)(a_2w_2 - \bar{V}_2))}^{①.a}\overbrace{(\frac{a_1a_2}{d}w_3 - \bar{V}_3)}^{①.b}}_{①} + \underbrace{\frac{f}{a_1^2a_2^2/d^2}(-\frac{a_1^2w_1 + a_2^2w_2}{d} + \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d})}_{②} \\
&\quad + \frac{y}{a_1a_2/d}\underbrace{[\frac{f}{a_1a_2} + (a_1w_1 - \bar{V}_1)(a_2w_2 - \bar{V}_2) + (-\frac{a_1^2w_1 + a_2^2w_2}{d} + \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d})(\frac{a_1a_2}{d}w_3 - \bar{V}_3)]}_{③}.
\end{aligned}$$

By Lemma 3.1.15, either $(x-c) \mid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d}$ or $(x-c) \nmid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d}$. We evaluate H at $(c,0)$ into these two subcases.

Case 3.3.a. $(x-c) \mid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1a_2}{d}$

In this subcase, we have $1 \equiv \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d}h_3 \pmod{x-c}$ and $\bar{V}_3 = (\frac{f}{a_1a_2} + \bar{V}_1\bar{V}_2)h_3 \pmod{x-c}$ by Equation (3.2) and 3.3. Consequently, $① + ②$ modulo $(x-c)$ can be computed as:

$$\begin{aligned}
① + ② &\equiv (\frac{f}{a_1a_2} + \bar{V}_1\bar{V}_2)^2(-h_3) + \frac{f}{a_1^2a_2^2/d^2} \cdot \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d} \\
&\equiv -h_3[(\frac{f}{a_1a_2} + \bar{V}_1\bar{V}_2)^2 - \frac{f}{a_1^2a_2^2/d^2}(\frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d})^2] \equiv -h_3(\frac{f}{a_1^2} - \bar{V}_1^2)(\frac{f}{a_2^2} - \bar{V}_2^2) \not\equiv 0. \pmod{x-c}
\end{aligned}$$

This shows that $(① + ②)|_{x=c} \neq 0$. And ③ modulo $\frac{a_1a_2}{d}$ can be computed as:

$$\begin{aligned}
③ &\equiv \frac{f}{a_1a_2} - a_1w_1\bar{V}_2 - a_2w_2\bar{V}_1 + \bar{V}_1\bar{V}_2 - (-\frac{a_1^2w_1 + a_2^2w_2}{d} + \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d})\bar{V}_3 \\
&\underset{Eq(3.3)}{\equiv} \frac{f}{a_1a_2} - a_1w_1\bar{V}_2 - a_2w_2\bar{V}_1 + \bar{V}_1\bar{V}_2 - (-\frac{a_1^2w_1 + a_2^2w_2}{d} + \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d})(a_1\bar{V}_2h_1 + a_2\bar{V}_1h_2) \\
&\quad + \frac{a_1^2w_1 + a_2^2w_2}{d}\bar{V}_1\bar{V}_2h_3 - \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d}(\frac{f}{a_1a_2}h_3 + \bar{V}_1\bar{V}_2h_3) \\
&\underset{Eq(3.2)}{\equiv} \frac{f}{a_1a_2} - a_1w_1\bar{V}_2 - a_2w_2\bar{V}_1 + \cancel{\bar{V}_1\bar{V}_2} + \frac{a_1^3}{d}w_1\bar{V}_2h_1 + \frac{a_2^3}{d}w_2\bar{V}_1h_2 - \cancel{(\frac{a_1^2}{d}h_1 + \frac{a_2^2}{d}h_2)}\bar{V}_1\bar{V}_2 \\
&\quad \frac{a_1^2w_1 + a_2^2w_2}{d}\bar{V}_1\bar{V}_2h_3 - \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d}h_3 \cdot \frac{f}{a_1a_2} - \cancel{\frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d}}h_3\bar{V}_1\bar{V}_2 \\
&\equiv \frac{f}{a_1a_2}(1 - \frac{a_1\bar{V}_1 + a_2\bar{V}_2}{d}h_3) + a_1w_1\bar{V}_2(-1 + \frac{a_1^2}{d}h_1 + \frac{a_1\bar{V}_1}{d}h_3) + a_2w_2\bar{V}_1(-1 + \frac{a_2^2}{d}h_2 + \frac{a_2\bar{V}_2}{d}h_3) \\
&\underset{Eq(3.2)}{\equiv} \frac{f}{a_1a_2}(\frac{a_1^2}{d}h_1 + \frac{a_2^2}{d}h_2) + a_1w_1\bar{V}_2 \cdot \frac{a_2}{d}(\cdots) + a_2w_2\bar{V}_1 \cdot \frac{a_1}{d}(\cdots) \\
&\equiv (\frac{f}{a_2^2}h_1 + \frac{f}{a_1^2}h_2)\frac{a_1a_2}{d} \equiv 0. \pmod{\frac{a_1a_2}{d}}
\end{aligned}$$

Thus, $\frac{y}{a_1a_2/d} \cdot ③|_{(c,0)} = y(\cdots)|_{(c,0)} = 0$. Therefore, $H(c,0) = (① + ② + \frac{y}{a_1a_2/d} \cdot ③)|_{(c,0)} \neq 0$.

Case 3.3.b. $(x - c) \nmid \frac{a_1^2}{d}, \frac{a_2^2}{d}, \frac{a_1 a_2}{d}$

In this subcase, $\frac{y}{a_1 a_2/d}(\cdots)||_{(c,0)} = 0$, so $(\textcircled{2}+\textcircled{3})|_{(c,0)} = 0$. From Equation (3.1), we know that $\textcircled{1}.b|_{x=c} \neq 0$. Additionally, we compute:

$$\begin{aligned}(\textcircled{1}.a)^2 \equiv& (\frac{f}{a_1 a_2} + \bar{V}_1 \bar{V}_2)^2 \equiv (\frac{f}{a_1^2} - \bar{V}_1^2)(\frac{f}{a_2^2} - \bar{V}_2^2) + \frac{f}{a_1^2 a_2^2}(a_1 \bar{V}_1 + a_2 \bar{V}_2)^2 \\ \equiv& (\frac{f}{a_1^2} - \bar{V}_1^2)(\frac{f}{a_2^2} - \bar{V}_2^2) \not\equiv 0. \pmod{x - c}\end{aligned}$$

Thus, $H(c, 0) = (\textcircled{1}.a \times \textcircled{1}.b + \textcircled{2} + \textcircled{3})|_{(c,0)} \neq 0$.

In all cases, $H(x, y)$ does not vanish at singular points. Therefore, $\operatorname{div}(H(x, y)) = (a_1^2, a_1 \bar{V}_1) + (a_2^2, a_2 \bar{V}_2) - (a_3^2, a_3 \bar{V}_3)$. This confirms that the Cantor composition implements addition in S. □

Remark 3.1.17. *Theorem 3.1.16 establishes that addition is closed in S. It is straightforward to verify that $(1, 0)$ serves as the neutral element in S, and for any divisor $(a^2, a\bar{V}) \in S$, the divisor class $(a^2, -a\bar{V}) \in S$ acts as its inverse. Therefore, S forms a subgroup of $J(C)$.*

Let C be a singular hyperelliptic curve. By Theorem 3.1.12, each element of S uniquely represents a divisor class in $J(C)$. Additionally, Theorem 3.1.16 establishes that the addition operation, implemented via Cantor composition, endows S with a group structure. Consequently, S forms a subgroup of $J(C)$. This property holds for any singular hyperelliptic curve and will be used in Chapter 4.

In particular, when C has geometric genus 0, we will show in the following two propositions that every divisor class in $J(C)$ has a unique representation in S. This will complete the proof of Theorem 3.1.11.

Proposition 3.1.18. *Let S be the set defined in Theorem 3.1.16. If C has geometric genus of 0, then every divisor class in $J(C)$ can be represented by an element in S.*

Proof. Since each divisor is a finite sum of $[P] - [\infty]$ for some nonsingular points P and addition is closed in S by Theorem 3.1.16, it suffices to show that the divisor class of $[P] - [\infty]$ can be represented by an element in S. Given any nonsingular point $(x_0, y_0) \in C$, let $\alpha := \frac{y_0}{h(x_0)}$. Then:

$$x_0 = \alpha^2, \text{ and } y_0 = \alpha h(\alpha^2),$$

i.e., (x_0, y_0) can be written as $(\alpha^2, \alpha h(\alpha^2))$ with a unique α. We claim that $(h^2, -\alpha h)$ represents the divisor class of $[(x_0, y_0)] - [\infty]$. Since $(\alpha^2, \alpha h(\alpha^2))$ is a nonsingular point, we have $h(\alpha^2) \neq 0$. And thus

$$\gcd(h, x - \alpha^2) = 1.$$

This shows $(h^2, -\alpha h) \in S$.

Observe that $(x - \alpha^2, \alpha h(\alpha^2))$ is the reduction result of $(h^2, -\alpha h)$. By Proposition 3.1.14, $(x - \alpha^2, \alpha h(\alpha^2))$ is a representative of $(h^2, -\alpha h)$. Since $(x - \alpha^2, \alpha h(\alpha^2))$ corresponds to $[(x_0, y_0)] - [\infty]$ through the relation in Proposition 3.1.7, $(h^2, -\alpha h) \in S$ represents the divisor class of $[(x_0, y_0)] - [\infty]$. □

Proposition 3.1.19. *Under the same setting and notation as in Theorem 3.1.16, any two distinct elements of S represent distinct divisor classes in $J(C)$.*

Proof. Let $(a_1^2, a_1 \bar{V}_1), (a_2^2, a_2 \bar{V}_2) \in S$. By Theorem 3.1.16, the elements $(a_1^2, a_1 \bar{V}_1)$ and $(a_2^2, a_2 \bar{V}_2)$ represents the same divisor class if and only if the result of Cantor composition of $(a_1^2, a_1 \bar{V}_1) + (a_2^2, -a_2 \bar{V}_2)$ is $(1, 0)$.

To check this, consider the greatest common divisor:

$$d = \gcd(a_1^2, a_2^2, a_1 \bar{V}_1 - a_2 \bar{V}_2).$$

If $\frac{a_1^2 a_2^2}{d^2} = 1$, then $a_1^2 = d = a_2^2$. Since a_1 and a_2 are monic, it follows that $a_1 = a_2$.

By the second condition in Theorem 3.1.12, we have:

$$\deg(d) = \deg(a_1^2) = \deg(a_2^2) > \deg(a_1\bar{V}_1 - a_2\bar{V}_2).$$

Thus $d \mid a_1\bar{V}_1 - a_2\bar{V}_2$ implies that

$$a_1\bar{V}_1 - a_2\bar{V}_2 = 0 \implies \bar{V}_1 = \bar{V}_2.$$

Therefore $(a_1^2, a_1\bar{V}_1) = (a_2^2, a_2\bar{V}_2)$ if and only if $a_1 = a_2$ and $\bar{V}_1 = \bar{V}_2$. This confirms that any two distinct elements in S represents distinct divisor classes. □

Let C be a singular hyperelliptic curve of geometric genus 0. Theorem 3.1.12 demonstrates that each pair of polynomials in S uniquely represents a divisor class in $J(C)$. Proposition 3.1.18 and Proposition 3.1.19 together imply that every divisor class in $J(C)$ can be uniquely represented by a pair in S. Thus, there is a one-to-one correspondence between divisor classes in $J(C)$ and their representations in S, which completes the proof of Theorem 3.1.11.

Example 3.1.20. *For a singular curve with a (higher) cusp $C : y^2 = x^{2g+1}$, we have:*

$$J(C) = \{(x^{2k}, x^k\bar{V}) \mid 1 \leq k \leq g,\ \deg(\bar{V}) < k,\ x \nmid \bar{V}\} \cup \{(1,0)\}. \tag{3.4}$$

Example 3.1.21. *For a singular curve with a (higher) node $C : y^2 = x^{2g}(x-c)$, we have:*

$$J(C) = \{(x^{2k}, x^k\bar{V}) \mid 1 \leq k \leq g,\ \deg(\bar{V}) < k,\ \gcd(x, x^{2g-2k}(x-c) - \bar{V}^2) = 1\} \cup \{(1,0)\}. \tag{3.5}$$

Example 3.1.22. *Let $C : y^2 = h^2(x)x$ be a singular curve with multiple nodes, with $h(x) = (x-c_1)\cdots(x-c_g)$, and $c_i \neq c_j, \forall i \neq j$. Then:*

$$J(C) = \{(a^2, a\bar{V}) \mid a \mid h,\ a \text{ is monic},\ \deg(\bar{V}) < \deg(a),\ \gcd(a, \frac{f}{a^2} - \bar{V}^2) = 1\}. \tag{3.6}$$

Remark 3.1.23. *[CNO22] also introduced a representation for the Jacobian group of singular curves with multiple nodes. They argued that $J(C) = \{(h^2, h\bar{V}) \mid h \text{ is monic},\ \deg(\bar{V}) < g, \gcd(h, x - \bar{V}^2) = 1\}$. Compared to Equation (3.6), this representation only covers the case when $a = h$, which is incomplete.*

Moreover, there is a flaw in the addition algorithm proposed in [CNO22]. For example, let $f(x) = (x-1)(x+1)$, $h_1(x) = x - 1$ and $h_2(x) = 2$, then:

$$\gcd(f(x), h_1(x) + h_2(x)) = x + 1.$$

There do not exist polynomials $g_1(x)$ and $g_2(x)$ satisfying the desired conditions in step 2 of the addition algorithm. The incompleteness of group elements causes the addition operation to fail.

3.2 Decomposition of the Jacobian group

In this section, we introduce a (partial) normalization C' of any singular hyperelliptic curve C and a canonical surjective (partial) normalization map from $J(C)$ to $J(C')$. When C has geometric genus 0 and defined by $y^2 = (\prod_{i=1}^k (x-c_i)^{2n_i})x$, we demonstrate that $J(C) \cong \prod_{i=1}^k J(C_i)$ using the partial normalization map, where $C_i : y^2 = (x-c_i)^{2n_i}x$ for any $1 \leq i \leq k$.

Definition 3.2.1. *Let $C : y^2 = f(x) = h^2(x)e(x)$ be a singular hyperelliptic curve. Given any $s \mid h$, we define $C' : y^2 = f'(x) = s^2(x)e(x)$ such that C' contains some of the singularities of C; we call this a partial normalization of C. There is a canonical map from $J(C)$ to $J(C')$:*

$$\Phi : J(C) \to J(C'), \sum_{j=1}^n ([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^n ([(x_j, \frac{y_j}{(h/s)(x_j)})] - [\infty]), \tag{3.7}$$

which we call the partial normalization map.

In particular, when $s = 1$ and $\deg(e(x)) \geq 3$, C' becomes a smooth hyperelliptic curve, known as the ***normalization*** *of C and Φ is called the normalization map.*

Remark 3.2.2. *When $s = 1$ and $\deg(e(x)) = 1$, the curve C' is isomorphic to $\mathbf{P}^1_{\mathbf{C}}$, and $J(C')$ is the trivial group. Since there is nothing to study in this case, we exclude it when referring to (partial) normalization in this thesis.*

Remark 3.2.3. *Given a singular hyperelliptic curve $C : y^2 = h^2(x)e(x)$, there is a unique normalization, but there may be multiple partial normalizations depending on the choice of the factor s of h.*

Proposition 3.2.4. *Let $C : y^2 = f(x) = h^2(x)e(x)$ and $C' : y^2 = f'(x) = s^2(x)e(x)$ with $s \mid h$ be a (partial) normalization of C. Then the (partial) normalization map $\Phi : J(C) \longrightarrow J(C')$ is a surjective group homomorphism.*

Proof. We first show the well-definedness of Φ, then demonstrate the surjectivity of Φ.

Step 1. Show Φ is a well-defined group homomorphism.

Given any principal divisor $D = \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) = \operatorname{div}(g(x,y))$ in $J(C)$, we define $g'(x,y) := g(x, \frac{h}{s}y)$. It's easy to see that $g(x_0, y_0) = 0$ if and only if $g'(x_0, \frac{y_0}{(h/s)(x_0)}) = 0$ for any nonsingular point (x_0, y_0) on C. Thus, we have:

$$\operatorname{div}(g'(x,y)) = \sum_{j=1}^{n}([(x_j, \frac{y_j}{(h/s)(x_j)})] - [\infty]) = \Phi(D).$$

It follows that the image of a principal divisor is still a principal divisor, which implies that Φ is well-defined. Furthermore, by the construction of Φ, it is clear that $\Phi(D_1 + D_2) = \Phi(D_1) + \Phi(D_2)$ for any Weil divisors D_1 and D_2 on C. Therefore, Φ is a well-defined homomorphism.

Step 2. Show the surjectivity of Φ.

To prove surjectivity, it is enough to show that for any divisor class of $[(c, y_c)] - [\infty] \in J(C')$ where $(x - c) \mid \frac{h}{s}$, there exists a preimage under Φ.

Consider the divisor $\operatorname{div}((y - y_c) - k(x - c))$ for some $k \in \mathbf{C}$. The term $[(c, y_c)] - [\infty]$ occurs in $\operatorname{div}((y - y_c) - k(x - c))$ at least twice if and only if k is the slope of the tangent line to C' at (c, y_c). For any divisor $[c', y_{c'}] - [\infty] \in J(C')$ where $(x - c') \mid h$ and $c' \neq c$, it occurs in $\operatorname{div}((y - y_c) - k(x - c))$ if and only if k is the slope of the line passing through (c, y_c) and $(c', y_{c'})$. By avoiding such choices of k, we obtain:

$$\operatorname{div}((y - y_c) - k(x - c)) = [(c, y_c)] - [\infty] + \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]),$$

where $h(x_j) \neq 0, \forall 1 \leq j \leq n$. Thus $[(c, y_c)] - [\infty]$ is equivalent to $\sum_{j=1}^{n}([(x_j, -y_j)] - [\infty])$. Since $\sum_{j=1}^{n}([(x_j, -y_j \cdot \frac{h}{s}(x_j))] - [\infty])$ maps to $\sum_{j=1}^{n}([(x_j, -y_j)] - [\infty])$, it follows that the preimage of $[(c, y_c)] - [\infty]$ is given by

$$\sum_{j=1}^{n}([(x_j, -y_j \cdot \frac{h}{s}(x_j))] - [\infty]).$$

Hence, Φ is surjective. □

Theorem 3.2.5. *We choose the same setting and notation as in Proposition 3.2.4. Let S (resp. S') be the set defined in Theorem 3.1.16 for curve C (resp. C'). Then we have:*

$$\Phi(S) = S'.$$

Moreover, when restricted to S, Φ can be expressed in terms of the generalized Mumford representation as:

$$\Phi|_S : (a^2, a\bar{V}) \mapsto (\frac{a^2}{d^2}, \frac{a}{d}\bar{V}'), \tag{3.8}$$

where $d = \gcd(a, \frac{h}{s})$ is monic, and $\frac{h/s}{d}\bar{V}' \equiv \bar{V} \pmod{\frac{a}{d}}$ with $\deg(V') < \deg(\frac{a}{d})$.

Proof. Since $1 = \gcd(\frac{a}{d}, \frac{h/s}{d})$, there exists polynomials ψ_1 and ψ_2 such that $1 = \psi_1\frac{a}{d} + \psi_2\frac{h/s}{d}$. Thus $\bar{V}' \equiv \psi_2\bar{V}$ $\pmod{\frac{a}{d}}$. We first verify Equation (3.8), then show $S' = \Phi(S)$.

Step 1. Show $\Phi|_S$ can be expressed by Equation (3.8).

We first show that the image of $(a^2, a\bar{V}) \in S$ given by Equation (3.8) is a valid representation in $S' \subset J(C')$. It is easy to see that it satisfies the first two conditions in Theorem 3.1.12, so we have to check the third. Given any singular point $(c, 0)$ with $(x - c) \mid \frac{a}{d}$, we have

$$\frac{f'}{a^2/d^2} - \bar{V}'^2 \equiv \frac{f'}{a^2/d^2} - \psi_2^2\bar{V}^2 \equiv \psi_2^2(\frac{h^2/s^2}{d^2} \cdot \frac{f'}{a^2/d^2} - \bar{V}^2) \equiv \psi_2^2(\frac{f}{a^2} - \bar{V}^2) \not\equiv 0. \quad (\text{mod } x - c)$$

Therefore, $\gcd(\frac{a}{d}, \frac{f'}{a^2/d^2} - \bar{V}'^2) = 1$, and $(\frac{a^2}{d^2}, \frac{a}{d}\bar{V}')$ is a generalized Mumford representation in S'.

We choose a proper w (resp. w') satisfying condition ($\star$) such that the corresponding (U, V) (resp (U', V')) are representatives of $(a^2, a\bar{V})$ (resp. $(\frac{a^2}{d^2}, \frac{a}{d}\bar{V}')$). Then, we have:

$$U = \frac{f}{a^2} - (aw - \bar{V})^2, V = a^2w - a\bar{V}. \tag{3.9}$$

$$U' = \frac{f'}{a^2/d^2} - (\frac{a}{d}w' - \bar{V}')^2, V' = \frac{a^2}{d^2}w' - \frac{a}{d}\bar{V}'. \tag{3.10}$$

Let (U_s, V_s) be the image of (U, V) under Φ using Equation (3.7). By the construction of Φ, we know that $U_s = U$ and $V_s(x) = \frac{V(x)}{h/s(x)}$ for any x with $U(x) = 0$. To show that Equation (3.8) agrees with Equation (3.7), it suffices to show that (U', V') is equivalent to (U_s, V_s) in $J(C')$. Define

$$H(x, y) := (\frac{y}{a} \cdot \frac{h}{s} - (aw - \bar{V}))(\frac{y}{a/d} + (\frac{a}{d}w' - \bar{V}')).$$

We claim that $\operatorname{div}(H(x, y)) = (U_s, V_s) - (U', V')$.

To verify this, we observe that for any nonsingular points $(x, y) \in C'$,

$$y \cdot \frac{h}{as} - (aw - \bar{V}) = 0 \Longleftrightarrow \begin{cases} y^2 \cdot (\frac{h}{as})^2 - (aw - \bar{V})^2 \underset{Eq(3.9)}{=} U(x) = U_s(x) = 0, \\ y \underset{\gcd(U,h)=1}{=} \frac{s}{h}(a^2w - a\bar{V})(x) \underset{Eq(3.9)}{=} \frac{V(x)}{h/s(x)} = V_s(x). \end{cases}$$

Similarly,

$$\frac{y}{a/d} + (\frac{a}{d}w' - \bar{V}') = 0 \Longleftrightarrow \begin{cases} \frac{y^2}{a^2/d^2} - (\frac{a}{d}w' - \bar{V}')^2 \underset{Eq(3.10)}{=} U'(x) = 0, \\ y = -(\frac{a^2}{d^2}w' - \frac{a}{d}\bar{V}')(x) \underset{Eq(3.10)}{=} -V'(x). \end{cases}$$

Thus, H vanishes exactly at points in the Weil divisor of $(U_s, V_s) - (U', V')$. What's left is to show that H does not vanish at singular points. Expanding H, we obtain:

$$H(x,y) = \underbrace{\frac{f'}{a^2/d^2} \cdot \frac{h/s}{d} - (aw - \bar{V})(\frac{a}{d}w' - \bar{V}')}_{①} + \frac{y}{a/d} \underbrace{(\frac{h/s}{d}(\frac{a}{d}w' - \bar{V}') - (aw - \bar{V}))}_{②}.$$

Given any singular point $(c, 0)$ on C', we evaluate H at $(c, 0)$. Using the congruence $\psi_2 \frac{h/s}{d} \equiv 1$and $\bar{V}' \equiv \psi_2 \bar{V}$ $(\text{mod } \frac{a}{d})$, we can get

$$② \equiv -\frac{h/s}{d}\bar{V}' + \bar{V} \equiv -\frac{h/s}{d}\psi_2\bar{V} + \bar{V} \equiv 0 \pmod{\frac{a}{d}} \implies (\frac{y}{a/d} \times ②)|_{(c,0)} = y(\cdots)|_{(c,0)} = 0.$$

There are two cases of c when we evaluate ①. In the first case, $(x - c) \mid \frac{a}{d}$. We compute:

$$① \equiv \frac{f'}{a^2/d^2} \cdot \frac{h/s}{d} - \bar{V}\bar{V}' \equiv \frac{f'}{a^2/d^2} \cdot \frac{h/s}{d} - \psi_2\bar{V}^2 \equiv \psi_2(\frac{f}{a^2} - \bar{V}^2) \not\equiv 0. \pmod{x - c}$$

In the second case, $(x - c) \nmid \frac{a}{d}$, but $(x - c) \mid s$. We note that $\frac{h}{a} = s \cdot \frac{(h/s)/d}{a/d}$, so $\frac{h^2 e}{a^2}|_{x=c} = \frac{s^2 e}{a^2/d^2}|_{x=c} = 0$. From Equation (3.9), Equation (3.10) and the choice of w and w' which ensure that $U(c) \neq 0$ and $U'(c) \neq 0$, we obtain:

$$(aw - \bar{V})|_{x=c} \neq 0, \text{ and } (\frac{a}{d}w' - \bar{V}')|_{x=c} \neq 0.$$

Therefore:

$$①|_{(c,0)} = -(aw - \bar{V})(\frac{a}{d}w' - \bar{V}')|_{x=c} \neq 0.$$

Thus, $H(c, 0) \neq 0$ for any singular points $(c, 0)$. This implies that $\text{div}(H(x, y)) = (U_s, V_s) - (U', V')$, and consequently, $\Phi|_S$ can be expressed using Equation (3.8).

Step 2. Show $\Phi(S) = S'$.

By Equation (3.8), it is evident that $\Phi(S) \subset S'$. It suffices to show that any divisor class in S' has a preimage in S. Given any $(a'^2, a'\bar{V}') \in S'$, assume:

$$s = \prod_{i=1}^{k}(x - c_i)^{m_i}, a' = \prod_{i=1}^{k}(x - c_i)^{k_i}, \text{ where } 0 \leq k_i \leq m_i \leq n_i.$$

Define:

$$d := \prod_{i=1}^{k}(x - c_i)^{l_i}, \text{ where } l_i = \begin{cases} n_i - m_i, & if\ k_i > 0 \\ 0, & if\ k_i = 0 \end{cases}, \forall\ 1 \leq i \leq k.$$

By construction, $\gcd(a', \frac{h/s}{d}) = 1$, and $a'd$ has the same linear factors as a'.

There exist ψ_1 and ψ_2 such that $1 = \psi_1 a' + \psi_2 \frac{h/s}{d}$. We choose $a = a'd$ and $\bar{V} \equiv \frac{h/s}{d}\bar{V}'$ $(\text{mod } a)$ with $\deg(\bar{V}) < \deg(a)$. We claim that $(a^2, a\bar{V})$ lies in S and maps to $(a'^2, a'\bar{V}')$. For any $1 \leq i \leq k$, the multiplicity of $(x - c_i)$ in a is at most $k_i + n_i - m_i \leq n_i$, so $a \mid h$.

Take any $(x - c) \mid a'$, we compute:

$$\frac{f}{a^2} - \bar{V}^2 \equiv \frac{h^2 e}{a'^2 d^2} - (\frac{h/s}{d}\bar{V}')^2 \equiv \frac{h^2/s^2}{d^2} \cdot (\frac{f'}{a'^2} - \bar{V}'^2) \not\equiv 0. \pmod{x - c}$$

Thus, $\gcd(a', \frac{f}{a^2} - \bar{V}^2) = 1$, i.e., $\gcd(a, \frac{f}{a^2} - \bar{V}^2) = 1$. This ensures that $(a^2, a\bar{V}) \in S$. Furthermore, since $\gcd(a', \frac{h/s}{d}) = 1$, it follows that $\gcd(a, \frac{h}{s}) = d$. We also have:

$$\psi_2 \bar{V} \equiv \psi_2 \frac{h/s}{d} \bar{V}' \equiv \bar{V}'. \quad (\bmod\ a')$$

Then it's straightforward to verify $\Phi((a^2, a\bar{V})) = (a'^2, a'\bar{V}')$ according to Equation (3.8), which proves that $\Phi(S) = S'$. □

We suppose C to be any singular curve in Definition 3.2.1, Proposition 3.2.4 and Theorem 3.2.5. These concepts and results will be utilized in Chapter 4.

In particular, when the geometric genus of C is 0, Theorem 3.1.11 ensures that $J(C) = S$. Therefore, Equation (3.8) holds for each divisor class in $J(C)$. We will use this equation to derive a decomposition of $J(C)$ in the following theorem.

Theorem 3.2.6. *Let $C : y^2 = h^2(x)x$ be a singular hyperelliptic curve of geometric genus 0. Assume $h = \prod_{i=1}^{k}(x - c_i)^{n_i}$ with $c_i \neq c_j$, $\forall i \neq j$. Let $C_i : y^2 = (x - c_i)^{2n_i}x$, and define*

$$\Phi_i : J(C) \to J(C_i), \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n}([(x_j, \frac{y_j}{h(x_j)/(x_j - c_i)^{n_i}})] - [\infty])$$

for each $i = 1, \cdots, k$. Then, the map $\Phi = \prod_{i=1}^{k} \Phi_i : J(C) \to \prod_{i=1}^{k} J(C_i)$ is a group isomorphism.

Proof. By Proposition 3.2.4, Φ is a well-defined group homomorphism. Assume $\Phi(D) = \mathbf{0}$, where the divisor class of D can be represented by $(a^2, a\bar{V}) \in J(C)$. Then,

$$\Phi_i((a^2, a\bar{V})) = (1, 0), \ \forall i.$$

Using Equation (3.8), we obtain:

$$a = \gcd(a, \frac{h}{(x - c_i)^{n_i}}), \ \forall i.$$

This implies that $(x - c_i) \nmid a, \forall i$. Hence, $a = 1$, i.e., $D \sim 0$. Therefore, Φ is injective.

Consider any divisor class $D_i = ((x - c_i)^{2m_i}, (x - c_i)^{m_i}\bar{V}_i) \in J(C_i)$, for any $i = 1, \cdots, k$. Fix any i, if $D_i = (1, 0)$, we choose $E_i = (1, 0) \in J(C)$. Otherwise, we define

$$E_i := ((x - c_i)^{2m_i}, (x - c_i)^{m_i}\bar{W}_i),$$

where:

$$\bar{W}_i \equiv \prod_{j \neq i}(x - c_j)^{n_j}\bar{V}_i \quad (\bmod\ (x - c_i)^{m_i}) \text{ with } \deg(\bar{W}_i) < m_i.$$

By the definition of generalized Mumford representation of $J(C_i)$, we have:

$$(\frac{(x - c_i)^{2n_i}x}{(x - c_i)^{2m_i}} - \bar{V}_i^2)|_{x=c_i} \neq 0, \ \forall i.$$

Thus, for any $i = 1, \cdots, k$:

$$\begin{aligned} \frac{\prod_{i=1}^{k}(x - c_i)^{2n_i}x}{(x - c_i)^{2m_i}} - \bar{W}_i^2 &\equiv \frac{\prod_{i=1}^{k}(x - c_i)^{2n_i}x}{(x - c_i)^{2m_i}} - \prod_{j \neq i}(x - c_j)^{2n_j}\bar{V}_i^2 \\ &\equiv \prod_{j \neq i}(x - c_j)^{2n_j}(\frac{(x - c_i)^{2n_i}x}{(x - c_i)^{2m_i}} - \bar{V}_i^2) \not\equiv 0. \quad (\bmod\ x - c_i) \end{aligned}$$

This shows that $E_i \in J(C)$, for any $i = 1, \cdots, k$.

Using Equation (3.8), it is straightforward to verify that

$$\Phi_i(E_i) = D_i, \forall i. \text{ and } \Phi_j(E_i) = (1, 0), \forall j \neq i.$$

Hence, $\sum_{i=1}^{k} E_i$ maps to $\prod_{i=1}^{k} D_i$, showing that Φ is surjective. Combining injectivity and surjectivity, we conclude that Φ is an isomorphism. □

3.3 Isomorphism between the Jacobian and products of additive and multiplicative groups of the base field

Let C be a singular curve of geometric genus 0, defined by $y^2 = h^2(x)x$, where $h(x) = \prod_{i=1}^{k}(x - c_i)^{n_i}$ with $c_i \neq c_j$, $\forall i \neq j$. In this section, we construct an explicit group isomorphism from $J(C)$ to $\mathbb{C}^{g-l} \times (\mathbb{C}^*)^l$, where $g = \sum_{i=1}^{k} n_i$ and l is the number of nonzero c_i for $1 \leq i \leq k$.

Since we have established that $J(C) \cong \prod_{i=1}^{k} J(C_i)$, where $C_i : y^2 = (x - c_i)^{2n_i}x$, $\forall i$ (see Theorem 3.2.6), it suffices to consider curves of the form $C : y^2 = (x - c)^{2g}x$, or equivalently, $C : y^2 = x^{2g}(x - c)$. There are two cases for the value of c:

1. Case $c = 0$: we can show that $J(C : y^2 = x^{2g+1}) \cong \mathbb{C}^g$.
2. Case $c \neq 0$: we demonstrate that $J(C : y^2 = x^{2g}(x - c)) \cong \mathbb{C}^{g-1} \times \mathbb{C}^*$.

To begin, we recall the isomorphisms for $g = 1$, as given by Theorem 2.30 and 2.31 in [Was08]. For singular elliptic curves of the form $y^2 = x^3$ and $y^2 = x^2(x + a)$, the sum of any two nonsingular points remains nonsingular. In other words, the set of nonsingular points is closed under addition. This endows the set of nonsingular points with a group structure, which is isomorphic to the Jacobian group. Moreover, there exists a group isomorphism between the Jacobian group and $\mathbb{C}$ or $\mathbb{C}^*$.

Theorem 3.3.1. *Let E be the curve $y^2 = x^3$ and let $E_{ns}(\mathbb{C})$ be the nonsingular points on this curve with coordinates in $\mathbb{C}$. The map*

$$E_{ns}(\mathbb{C}) \longrightarrow \mathbb{C}, (x, y) \mapsto \frac{x}{y}, \infty \mapsto 0$$

is a group isomorphism between $E_{ns}(\mathbb{C})$ and $\mathbb{C}$, regarded as an additive group.

Proof. See Theorem 2.30 in [Was08]. □

Theorem 3.3.2. *Let E be the curve $y^2 = x^2(x + a)$ with $a \in \mathbb{C}^*$. Let $E_{ns}(\mathbb{C})$ be the nonsingular points on E with coordinates in $\mathbb{C}$. Let α be a square root of a. Then the map:*

$$E_{ns}(\mathbb{C}) \longrightarrow \mathbb{C}, (x, y) \mapsto \frac{y + \alpha x}{y - \alpha x}, \infty \mapsto 1.$$

gives a group isomorphism from $E_{ns}(\mathbb{C})$ to $\mathbb{C}^*$.

Proof. See Theorem 2.31 in [Was08]. □

Lemma 3.3.3. *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x]$ with $a_0 \neq 0$, and $\{x_i \in \mathbb{C}^* \mid i = 1, \cdots, n\}$ be the roots of equation $f(x) = 0$. Define $q_k := \sum_{i=1}^{n} \frac{1}{x_i^k}$ for each $k \in \{1, \cdots, n\}$. Then, for each $k \in \{1, \cdots, n\}$, the following relation holds:*

$$\sum_{i=1}^{k} a_{k-i} q_i + k a_k = 0.$$

Proof. Define $g(x) := \sum_{i=0}^{n} a_{n-i} x^i$, then $x^n f(\frac{1}{x}) = g(x)$. So that $\{\frac{1}{x_i} | i = 1, \cdots, n\}$ are exactly the roots of $g(x) = 0$. Let $f_k (1 \leq k \leq n)$ be elementary functions of $\frac{1}{x_i} (1 \leq i \leq n)$, then $(-1)^k f_k = \frac{a_k}{a_0}, \forall k \in \{1, \cdots, n\}$ by Vieta's formulas.

Newton identities [Mea92] states that

$$kf_k = \sum_{i=1}^{k}(-1)^{i-1}f_{k-i}q_i, \ \forall k \in \{1, \cdots, n\}.$$

Substituting $(-1)^k f_k = \frac{a_k}{a_0}$ into the Newton identities, we can get

$$\sum_{i=1}^{k} a_{k-i}q_i + ka_k = 0, \forall k \in \{1, \cdots, n\}.$$

□

Theorem 3.3.4. *Let $C : y^2 = x^{2g+1}$. We define the map Ψ_i for each $i \in \{1, 2, \cdots, g\}$ as:*

$$\Psi_i : J(C) \to \mathbf{C}, \quad \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n} \frac{x_j^i}{y_j}.$$

Then the map

$$\Psi = \prod_{i=1}^{g} \Psi_i : J(C) \to \mathbf{C}^g, \ \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n}(\frac{x_j}{y_j}, \frac{x_j^2}{y_j}, \cdots, \frac{x_j^g}{y_j}).$$

is a group isomorphism.

Proof. We can demonstrate that Ψ is a group isomorphism by induction on g. For $g = 1$, the statement is proven by Theorem 3.3.1. Let $C' : y^2 = x^{2g-1}$ denote the higher cuspidal curve with genus $g - 1$, and let Ψ' represent the map on $J(C')$ as defined above. Assume that Ψ' is a group isomorphism for the curve C', we can prove that Ψ is also a group isomorphism for curve C.

Choose $h = x^g, s = x^{g-1}, e = x$ in Theorem 3.2.5 such that we get a canonical surjective homomorphism Φ:

$$\Phi : J(C) \to J(C'), \ \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n}([(x_j, \frac{y_j}{x_j})] - [\infty]).$$

In terms of the generalized Mumford representation, Φ can be expressed as:

$$\Phi : \ (x^{2k}, x^k\bar{V}) \mapsto (x^{2k-2}, x^{k-1}\bar{V}'), \ \forall 1 \leq k \leq g, \text{ and } (1, 0) \mapsto (1, 0). \tag{3.11}$$

where $\bar{V}' \equiv \bar{V} \pmod{x^{k-1}}$ with $\deg(\bar{V}') < k - 1$. From formula (3.11), it is straightforward to see

$$\ker(\Phi) = \{(x^2, \alpha x) | \alpha \neq 0\} \cup \{(1, 0)\}.$$

Step 1. Show Ψ is well-defined.

To prove that Ψ is well-defined, it suffices to show that each Ψ_i is well-defined, for any $1 \leq i \leq g$. By the construction of Ψ, it's evident that $\prod_{i=2}^{g} \Psi_i = \Psi'(\Phi)$. Since both Ψ' and Φ are well-defined, it follows that $\prod_{i=2}^{g} \Psi_i$ is well-defined. What's remains is to show the well-definedness of Ψ_1, i.e., the image of any principal divisor under Ψ_1 is 0.

To show this, it suffices to verify that $\operatorname{div}(h_1(x)y+h_2(x))$ maps to 0 under Ψ_1 for any $h_1, h_2 \in \mathbb{C}[x]$ with $h_2(0) \neq 0$. Suppose that

$$\operatorname{div}(h_1(x)y+h_2(x)) = \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]).$$

Since any nonsingular point (x, y) on C can be expressed as (z^2, z^{2g+1}) for a unqinue $z \in \mathbb{C}^*$ (where we set $z := \frac{y}{x^g}$), we can rewrite (x_j, y_j) as (z_j^2, z_j^{2g+1}), for any $j = 1, \cdots, n$. Thus

$$\Psi_i(\operatorname{div}(h_1(x)y+h_2(x))) = \Psi_i(\sum_{j=1}^{n}([(z_j^2, z_j^{2g+1})] - [\infty])) = \sum_{j=1}^{n} \frac{1}{z_j^{2(g-i)+1}}, \ \forall\, i = 1, \cdots, g,$$

where z_j $(1 \leq j \leq n)$ are precisely the roots of $h_1(z^2)z^{2g+1} + h_2(z^2) = 0$.

Define $q_k := \sum_{j=1}^{n} \frac{1}{z_j^k}, \forall 1 \leq k \leq n$. Since $\prod_{i=2}^{g} \Psi_i$ is well-defined, we have $q_{2l-1} = 0, \forall\, l = 1, \cdots g-1$. Writing $h_1(z^2)z^{2g+1} + h_2(z^2) = \sum_{i=0}^{n} a_i z^i$, note that $a_0 = h_2(0) \neq 0$. By Lemma 3.3.3,

$$\sum_{i=1}^{k} a_{k-i} q_i + k a_k = 0, \ \forall k = 1, \cdots, n. \tag{3.12}$$

Observe that the coefficients of $z^{2l-1}(1 \leq l \leq g)$ in $h_1(z^2)z^{2g+1} + h_2(z^2)$ are 0, i.e., $a_{2l-1} = 0$ $(1 \leq l \leq g)$. Using Equation (3.12) for $k = 2g-1$ and substituting $a_{2l-1} = 0$ $(1 \leq l \leq g)$ and $q_{2l-1} = 0$ $(1 \leq l \leq g-1)$, we find:

$$0 = a_0 q_{2g-1} + \sum_{i=1}^{2g-2} a_{2g-1-i} q_i + (2g-1)a_{2g-1} = a_0 q_{2g-1} \implies q_{2g-1} = 0.$$

Thus $q_{2g-1} = 0$, and Ψ_1 is well-defined. By its construction, Ψ is clearly a homomorphism.

Step 2. Show Ψ is surjective.

Given any $(z_1, \cdots, z_g) \in \mathbb{C}^g$, we need to construct a preimage under Ψ. Since Ψ' and Φ are surjective, $\prod_{i=2}^{g} \Psi_i = \Psi'(\Phi)$ is also surjective. Thus, there exists $(x^{2k}, x^k \bar{V}) \in J(C)$ such that $\prod_{i=2}^{g} \Psi_i((x^{2k}, x^k \bar{V})) = (z_2, \cdots, z_g)$.

If $\Psi_1((x^{2k}, x^k \bar{V})) = z_1$, then $\Psi((x^{2k}, x^k \bar{V})) = (z_1, \cdots, z_g)$. If $\Psi_1((x^{2k}, x^k \bar{V})) \neq z_1$, according to Lemma 3.3.5, there exists $\alpha \in \mathbb{C}^*$ such that

$$\Psi((x^2, \alpha x)) = (z_1 - \Psi_1((x^{2k}, x^k \bar{V})), 0, \cdots, 0).$$

Therefore, by adding $(x^2, \alpha x)$ to $(x^{2k}, x^k \bar{V})$, we obtain

$$\Psi((x^{2k}, x^k \bar{V}) + (x^2, \alpha x)) = (z_1, \cdots, z_g).$$

This shows that Ψ is surjective.

Step 3. Show Ψ is injective.

Given $(x^{2k}, x^k \bar{V}) \in J(C)$ such that $\Psi((x^{2k}, x^k \bar{V})) = (0, \cdots, 0)$, we need to show that $(x^{2k}, x^k \bar{V}) = (1, 0)$. Since $\prod_{i=2}^{g} \Psi_i = \Psi'(\Phi)$ and Ψ' is injective, it follows that $(x^{2k}, x^k \bar{V}) \in \ker(\Phi) = \{(x^2, \alpha x) | \alpha \neq 0\} \cup \{(1, 0)\}$. By lemma 3.3.5, we know that $\Psi_1((x^2, \alpha x)) \neq 0, \forall \alpha \neq 0$. Therefore the only possibility is $(x^{2k}, x^k \bar{V}) = (1, 0)$. Hence Ψ is injective.

Combining these results of Step 1, 2, 3, we can deduce that Ψ for $C : y^2 = x^{2g+1}$ is a a group isomorphism. By induction, Ψ is a group isomorphism for any $g \in \mathbf{N}$. □

Lemma 3.3.5. *Let C and Ψ be as in Theorem 3.3.4. The image of $(x^2, \alpha x) \in J(C)$ with $\alpha \neq 0$ under Ψ is $(\frac{-(2g-1)}{\alpha}, 0, \cdots, 0)$.*

Proof. Let Φ and Ψ' be as in Theorem 3.3.4. Since $(x^2, \alpha x) \in \ker(\Phi)$, we have

$$\prod_{i=2}^{g} \Psi_i((x^2, \alpha x)) = \Psi'(\Phi((x^2, \alpha x))) = \Psi'((1, 0)) = \mathbf{0}.$$

Next, choose a representative $(x^{2g-1} - \alpha^2, -\alpha x)$ in the divisor class $(x^2, \alpha x)$. $(x^{2g-1} - \alpha^2, -\alpha x)$ represents the divisor

$$(x^{2g-1} - \alpha^2, -\alpha x) = \sum_{j=1}^{2g-1} ([(x_j, -\alpha x_j)] - [\infty]),$$

where x_j $(1 \leq j \leq 2g-1)$ are the roots of $x^{2g-1} - \alpha^2 = 0$. Then, we have

$$\Psi_1((x^2, \alpha x)) = \Psi_1(\sum_{j=1}^{2g-1} ([(x_j, -\alpha x_j)] - [\infty])) = \sum_{j=1}^{2g-1} \frac{x_j}{-\alpha x_j} = \frac{-(2g-1)}{\alpha}.$$

Thus, we conclude that

$$\Psi((x^2, -\alpha x)) = (\frac{-(2g-1)}{\alpha}, 0, \cdots, 0).$$

□

Theorem 3.3.6. *Let $C : y^2 = x^{2g}(x - c)$, and let Ψ_i be the map defined as:*

$$\Psi_i : J(C) \to \mathbf{C}, \quad \sum_{j=1}^{n} ([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n} \frac{x_j^i (x_j - c)}{y_j}, \ \forall 1 \leq i \leq g-1.$$

Additionally, let Ψ_g be the map

$$\Psi_g : J(C) \to \mathbf{C}^*, \quad \sum_{j=1}^{n} ([(x_j, y_j)] - [\infty]) \mapsto \prod_{j=1}^{n} \frac{y_j + \beta x_j^g}{y_j - \beta x_j^g},$$

where β is a square root of $-c$.

Then the map $\Psi = \prod_{i=1}^{g} \Psi_i : J(C) \to \mathbf{C}^{g-1} \times \mathbf{C}^*$, defined by

$$\sum_{j=1}^{n} ([(x_j, y_j)] - [\infty]) \mapsto (\sum_{j=1}^{n} \frac{x_j (x_j - c)}{y_j}, \cdots, \sum_{j=1}^{n} \frac{x_j^{g-1} (x_j - c)}{y_j}, \prod_{j=1}^{n} \frac{y_j + \beta x_j^g}{y_j - \beta x_j^g})$$

is a group isomorphism.

Proof. We can prove the conclusion by induction on g. When $g = 1$, the statement holds true by Theorem 3.3.2. Let $C' : y^2 = x^{2g-2}(x - c)$ be the higher nodal curve with genus $g - 1$, and let Ψ' be the map given above, defined on $J(C')$. Assuming that Ψ' is a group isomorphism for $C' : y^2 = x^{2g-2}(x - c)$, we can show Ψ is a group isomorphism for $C : y^2 = x^{2g}(x - c)$.

Using the same approach as in the proof of Theorem 3.3.4, we first establish the well-definedness of Ψ through parametrization and Lemma 3.3.3. Next, we prove the bijectivity of Ψ using the generalised

Mumford representation. By setting $h = x^g, s = x^{g-1}, e = x$ in Theorem 3.2.5, we obtain a surjective homomorphism

$$\Phi : J(C) \to J(C'), \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n}([(x_j, \frac{y_j}{x_j})] - [\infty]),$$

which can also be written in terms of generalised Mumford representation as

$$\Phi : (x^{2k}, x^k\bar{V}) \mapsto (x^{2k-2}, x^{k-1}\bar{V}'), 1 \le k \le g, \text{ and } (1,0) \mapsto (1,0). \tag{3.13}$$

where $\bar{V}' \equiv \bar{V} \pmod{x^{k-1}}$, with $\deg(\bar{V}') < k-1$. From this expression, it is clear that

$$\ker(\Phi) = \{(x^2, \alpha x) | \alpha \neq 0\} \cup \{(1,0)\}.$$

Step 1. Show Ψ is well-defined.

Since $\prod_{i=2}^{g} \Psi_i = \Psi'(\Phi)$ and Ψ' is assumed to be well-defined, it follows that $\prod_{i=2}^{g} \Psi_i$ is well-defined. We only need to show that Ψ_1 is well-defined, i.e., any principal divisor maps to 0 under Ψ_1. It is sufficient to demonstrate that $\operatorname{div}(h_1(x)y + h_2(x))$ maps to 0 under Ψ_1 for any $h_1, h_2 \in \mathbf{C}[x]$ with $h_2(0) \neq 0$.

Let $k := \frac{y}{x^g}$, so that any nonsingular point (x, y) on C can be expressed as $(k^2+c, k(k^2+c)^g)$, for a unique $k \in \mathbf{C}$ with $k^2 \neq -c$. Therefore, we have:

$$\operatorname{div}(h_1(x)y + h_2(x)) = \sum_{j=1}^{n}([(k_j^2 + c, k_j(k_j^2+c)^g)] - [\infty]),$$

where k_j $(1 \le j \le n)$ are precisely the roots of $h_1(k^2+c)(k^2+c)^g k + h_2(k^2+c) = 0$. Then,

$$\Psi_1(\operatorname{div}(h_1(x)y + h_2(x))) = \sum_{j=1}^{n} \frac{k_j}{(k_j^2+c)^{g-1}}.$$

By Lemma 3.3.9, we can write:

$$\sum_{j=1}^{n} \frac{k_j}{(k_j^2+c)^{g-1}} = \sum_{l=1}^{g-1} b_l \cdot \sum_{j=1}^{n}(\frac{1}{(k_j-\beta)^l} + (-1)^{l+1}\frac{1}{(k_j+\beta)^l}),$$

for some $b_l \in \mathbf{C}$, $l = 1, \cdots, g-1$. To show $\sum_{j=1}^{n} \frac{k_j}{(k_j^2+c)^{g-1}} = 0$, it's enough to prove that

$$\sum_{j=1}^{n} \frac{1}{(k_j-\beta)^l} = \sum_{j=1}^{n}(-1)^l \frac{1}{(k_j+\beta)^l}, \; \forall\, 1 \le l \le g-1. \tag{3.14}$$

Let $z_j^- = k_j - \beta, q_l^- = \sum_{j=1}^{n} \frac{1}{(z_j^-)^l}$, and $z_j^+ = k_j + \beta, q_l^+ = \sum_{j=1}^{n} \frac{1}{(z_j^+)^l}$, for any $1 \le j \le n$ and $1 \le l \le g-1$. By replacing k with $x+\beta$ (resp. $x-\beta$) in the equation $h_1(k^2+c)(k^2+c)^g k + h_2(k^2+c) = 0$, we obtain that z_j^- $(1 \le j \le n)$ (resp. z_j^+ $(1 \le j \le n)$) are roots of Equation (3.15) (resp. Equation (3.16)).

$$h_1(x^2+2\beta x) \cdot (x^2+2\beta x)^g \cdot (x+\beta) + h_2(x^2+\beta x) = \sum_{i=0}^{n} a_i^- x^i = 0. \tag{3.15}$$

$$h_1(x^2-2\beta x)\cdot(x^2-2\beta x)^g\cdot(x-\beta)+h_2(x^2-\beta x)=\sum_{i=0}^{n}a_i^+x^i=0. \tag{3.16}$$

Note that $a_0^- = a_0^+ = h_2(0) \neq 0$, so by Lemma 3.3.3, we have the following relations:

$$\sum_{i=1}^{k}a_{k-i}^-q_i^- + ka_k^- = 0, \text{ and } \sum_{i=1}^{k}a_{k-i}^+q_i^+ + ka_k^+ = 0, \ \forall 1 \leq k \leq n. \tag{3.17}$$

In Equation (3.15) and 3.16, x^i with $0 \leq i \leq g-1$ appear only in the second summand $h_2(x^2 \pm \beta x)$. Define $g(x) := h_2(x^2+\beta x) + h_2(x^2-\beta x)$, $g'(x) := h_2(x^2+\beta x) - h_2(x^2-\beta x)$. Then $g(x) = g(-x)$ implies that the coefficients of odd power of x in g are zero, i.e., $a_{2l-1}^- = -a_{2l-1}^+$, $\forall\ 1 \leq 2l-1 \leq g-1$. Similarly, $g'(x) = -g'(-x)$ implies that the coefficients of even power of x in g' are zero, so $a_{2l}^- = a_{2l}^+$, $\forall\ 0 \leq 2l \leq g-1$. Combining these results, we get $a_l^- = (-1)^l a_l^+$, $0 \leq l \leq g-1$.

Now we can prove by induction on l that $q_l^- = (-1)^l q_l^+$, $\forall 1 \leq l \leq g-1$. Choosing $k=1$ in Equation (3.17) gives $q_1^- = -a_1^-/a_0^-$ and $q_1^+ = -a_1^+/a_0^+$, so $q_1^- = -q_1^+$. Assume $q_i^- = (-1)^i q_i^+$, $\forall 1 \leq i \leq l-1$ where $l \leq g-1$. Take Equation (3.17) for $k = l$:

$$\underbrace{\sum_{i=1}^{l}a_{l-i}^-q_i^- + la_l^- = 0}_{\textcircled{1}}, \text{ and } \underbrace{\sum_{i=1}^{l}a_{l-i}^+q_i^+ + la_l^+ = 0}_{\textcircled{2}}. \tag{3.18}$$

Now compute $\textcircled{1} - (-1)^l \times \textcircled{2}$:

$$\begin{aligned}&\sum_{i=1}^{l-1}(a_{l-i}^-q_i^- - (-1)^l a_{l-i}^+q_i^+) + l(a_l^- - (-1)^l a_l^+) + (a_0^-q_l^- - a_0^+(-1)^l q_l^+)\\ =&\sum_{i=1}^{l-1}[(-1)^{l-i}a_{l-i}^+\cdot(-1)^i q_i^+ - (-1)^l a_{l-i}^+q_i^+] + (a_0^-q_l^- - a_0^-(-1)^l q_l^+).\end{aligned}$$

This simplifies to

$$a_0^-(q_l^- - (-1)^l q_l^+) = 0,$$

so $q_l^- = (-1)^l q_l^+$. Therefore, we have $q_l^- = (-1)^l q_l^+$, $\forall 1 \leq l \leq g-1$, and thus Equation (3.14) holds true. This completes the proof that Ψ is well-defined.

Step 2: Show Ψ is surjective

Given any $(z_1, \cdots, z_g) \in \mathbb{C}^{g-1} \times \mathbb{C}^*$, we need to show that there exists its preimage under Ψ. Since $\prod_{i=2}^{g}\Psi_i = \Psi'(\Phi)$ and Ψ' is assumed to be surjective, we can find $(x^{2k}, x^k\bar{V}) \in J(C)$ such that

$$\prod_{i=2}^{g}\Psi_i((x^{2k}, x^k\bar{V})) = (z_2, \cdots, z_g).$$

If $\Psi_1((x^{2k}, x^k\bar{V})) = z_1$, we are done. Otherwise, there exists a unique $\alpha \in \mathbb{C}^*$ such that $\Psi((x^2, \alpha x)) = (z_1 - \Psi_1((x^{2k}, x^k\bar{V})), 0, \cdots, 0, 1)$ by Lemma 3.3.8. Therefore, we have:

$$\Psi((x^{2k}, x^k\bar{V}) + (x^2, \alpha x)) = (z_1, \cdots, z_g),$$

showing that Ψ is surjective.

Step 3: Ψ is injective

Assume that $\Psi((x^{2k}, x^k\bar{V})) = (0, \cdots, 0, 1)$. Then, $(x^{2k}, x^k\bar{V})$ must lie in $\ker(\Phi)$, since $\prod_{i=2}^{g} \Psi_i = \Psi'(\Phi)$ and Ψ' is injective. We know that

$$\ker(\Phi) = \{(x^2, \alpha x) | \alpha \neq 0\} \cup \{(1, 0)\}.$$

We also know that $\Psi_1((x^2, \alpha x)) \neq 0$ by Lemma 3.3.8, meaning that $(x^{2k}, x^k\bar{V})$ can only be $(1, 0)$. Therefore, Ψ is injective.

Combining the results of Step 1,2,3, Ψ for $C : y^2 = x^{2g}(x - c)$ is a group isomorphism if we assume Ψ' for $C' : y^2 = x^{2g-1}(x - c)$ is a group isomorphism. Hence by induction, Ψ is a group isomorphism for any $g \in \mathbb{N}$. □

Remark 3.3.7. *Let Ψ_i $(1 \leq i \leq g-1)$ be the maps defined in Theorem 3.3.6. Note that $\Psi_i([(c, 0)] - [\infty]) = 0$ for all $1 \leq i \leq g-1$, since $\frac{x^i(x-c)}{y} = \frac{x^i(x-c)y}{y^2} = \frac{y}{x^{2g-i}}$, which vanish at $(c, 0)$ for any $1 \leq i \leq g-1$.*

Lemma 3.3.8. *Let C and Ψ be as defined in Theorem 3.3.6. The image of $(x^2, \alpha x) \in J(C)$ with $\alpha \neq 0$ under Ψ is $(\frac{(2g-2)c}{\alpha}, 0, \cdots, 0, 1)$.*

Proof. Let Φ and Ψ' be as defined in the proof of Theorem 3.3.6. Since $(x^2, \alpha x)$ lies in $\ker(\Phi) = \{(x^2, \alpha x) | \alpha \neq 0\} \cup \{(1, 0)\}$, we know that

$$\prod_{i=2}^{g} \Psi_i((x^2, \alpha x)) = (0, \cdots, 0, 1).$$

Consider the divisor $(x^{2g-2}(x - c) - \alpha^2, -\alpha x)$ over C, which is a representative of $(x^2, \alpha x)$. This divisor can be written as:

$$(x^{2g-2}(x - c) - \alpha^2, -\alpha x) = \sum_{j=1}^{2g-1} ([(x_j, -\alpha x_j)] - [\infty]),$$

where x_j $(1 \leq j \leq 2g-1)$ are the roots of $x^{2g-2}(x - c) - \alpha^2 = 0$. Thus, we have:

$$\Psi_1((x^2, \alpha x)) = \sum_{j=1}^{2g-1} \frac{x_j(x_j - c)}{-\alpha x_j} = \sum_{j=1}^{2g-1} \frac{(x_j - c)}{-\alpha}.$$

By Vieta's formulas, we know that $\sum_{j=1}^{2g-1} x_j = c$, so $\Psi_1((x^2, \alpha x)) = \frac{(2g-2)c}{\alpha}$. Therefore, $\Psi((x^2, \alpha x)) = (\frac{(2g-2)c}{\alpha}, 0, \cdots, 0, 1)$. □

Lemma 3.3.9. *Consider x as a variable in $\mathbb{C} \setminus \{\pm\beta\}$, then we have the following expansion:*

$$\frac{x}{(x^2 + c)^m} = \sum_{l=1}^{m} b_l \cdot (\frac{1}{(x - \beta)^l} + (-1)^{l+1} \frac{1}{(x + \beta)^l}),$$

where $c \in \mathbb{C}^*$, $b_l \in \mathbb{C}$ $\forall 1 \leq l \leq m$, $m \in \mathbb{N}_+$ and β is a square root of $-c$.

Proof. First, for any $l \in \mathbf{N}$, it is easy to show by induction on l that:

$$\underbrace{\frac{1}{(x-\beta)(x+\beta)^l}}_{①} = \frac{a_l}{x-\beta} + \sum_{k=1}^{l} \frac{c_k}{(x+\beta)^k},$$

$$\text{and } \underbrace{\frac{1}{(x+\beta)(x-\beta)^l}}_{②} = \frac{(-1)^l a_l}{x+\beta} + \sum_{k=1}^{l} \frac{(-1)^{l+1-k} c_k}{(x-\beta)^k},$$

for some $a_l, c_k \in \mathbf{C}$. So we compute:

$$\begin{aligned}(-1)^l \times ① + ② =& (-1)^l a_l \left(\frac{1}{x-\beta} + \frac{(-1)^2}{x+\beta}\right) + \sum_{k=1}^{l} (-1)^l c_k \left(\frac{1}{(x+\beta)^k} + \frac{(-1)^{k+1}}{(x-\beta)^k}\right)\\ =& \sum_{k=1}^{l} b'_k \left(\frac{1}{(x-\beta)^k} + \frac{(-1)^{k+1}}{(x+\beta)^k}\right),\end{aligned} \tag{3.19}$$

for some $b'_l \in \mathbf{C}$.

Then we can show $\frac{x}{(x^2+c)^m} = \sum_{l=1}^{m} b_l \left(\frac{1}{(x-\beta)^l} + \frac{(-1)^{l+1}}{(x+\beta)^l}\right)$ by induction on m. When $m = 1$, it is an easy calculation. Assume this formula holds for $m-1$, then:

$$\begin{aligned}\frac{x}{(x^2+c)^m} &= \frac{1}{2\beta}\left(\frac{1}{x-\beta} - \frac{1}{x+\beta}\right) \cdot \sum_{l=1}^{m-1} \left(\frac{b_l}{(x-\beta)^l} + \frac{(-1)^{l+1} b_l}{(x+\beta)^l}\right)\\ &= \sum_{l=1}^{m-1} \frac{b_l}{2\beta}\left(\frac{1}{(x-\beta)^{l+1}} + \frac{(-1)^{l+2}}{(x+\beta)^{l+1}}\right) + \sum_{l=1}^{m-1} \frac{-b_l}{2\beta}\left(\frac{(-1)^l}{(x-\beta)(x+\beta)^l} + \frac{1}{(x+\beta)(x-\beta)^l}\right)\\ &\underset{Eq(3.19)}{=} \sum_{l=1}^{m} c_l \left(\frac{1}{(x-\beta)^l} + \frac{(-1)^{l+1}}{(x+\beta)^l}\right),\end{aligned}$$

for some $c_l \in \mathbf{C}$. Hence, the formula also holds for m. By induction, the formula holds for any $m \in \mathbf{N}_+$. □

By combining the decomposition $J(C) \cong \prod_{i=1}^{k} J(C_i)$ from Theorem 3.2.6, along with the two isomorphisms from Theorem 3.3.4 and Theorem 3.3.6, we can construct an explicit group isomorphism $J(C) \cong (\mathbf{C})^{g-l} \times (\mathbf{C}^*)^l$ for any singular hyperelliptic curve of geometric genus 0.

Theorem 3.3.10. *Let C denote the singular curve given by $y^2 = f(x) = h^2(x)x = (\prod_{i=1}^{k}(x-c_i)^{n_i})^2 x$ ($c_i \neq c_j, \forall i \neq j$). Then, there exists a group isomorphism*

$$J(C) \cong (\mathbf{C})^{g-l} \times (\mathbf{C}^*)^l,$$

where $g = \sum_{i=1}^{k} n_i$, and $l = |\{c_i \mid 1 \leq i \leq k, c_i \neq 0\}|$.

Proof. Let C_i denote the curve given by $y^2 = (x-c_i)^{2n_i}x$, for each $1 \leq i \leq k$. Fix an index $i \in \{1, \cdots, k\}$, we define the map:

$$\Phi_i : J(C) \to J(C_i), \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n}([(x_j, \frac{y_j}{(h/(x-c_i)^{n_i})(x_j)})] - [\infty]).$$

Additionally, if $c_i = 0$, we define the map

$$\Psi_i : J(C_i) \longrightarrow \mathbf{C}^{n_i}, \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n}(\frac{x_j}{y_j}, \frac{x_j^2}{y_j}, \cdots, \frac{x_j^{n_i}}{y_j}).$$

Otherwise $c_i \neq 0$, we define

$$\Psi_i : J(C_i) \longrightarrow \mathbf{C}^{n_i-1} \times \mathbf{C}^*,$$

$$\sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto (\sum_{j=1}^{n} \frac{x_j(x_j - c_i)}{y_j}, \cdots, \sum_{j=1}^{n} \frac{x_j(x_j - c_i)^{n_i-1}}{y_j}, \prod_{j=1}^{n} \frac{y_j + \beta_i(x_j - c_i)^{n_i}}{y_j - \beta_i(x_j - c_i)^{n_i}}),$$

where β_i is a square root of c_i.

By Theorem 3.2.6, $\prod_{i=1}^{k} \Phi_i$ is a group isomorphism between $J(C)$ and $\prod_{i=1}^{k} J(C_i)$. Furthermore, Theorem 3.3.4 and Theorem 3.3.6 imply that:

$$J(C_i) \overset{\Psi_i}{\cong} \begin{cases} \mathbf{C}^{n_i}, & if\ c_i = 0 \\ \mathbf{C}^{n_i-1} \times \mathbf{C}^*, & if\ c_i \neq 0 \end{cases}, \forall\ 1 \leq i \leq k.$$

Therefore, the map $\prod_{i=1}^{k} \Psi_i(\Phi_i)$ is a group isomorphism from $J(C)$ to products of $\mathbf{C}$ and $\mathbf{C}^*$, which is isomorphic to $(\mathbf{C})^{g-l} \times (\mathbf{C}^*)^l$, where l is the number of nonzero c_i $(1 \leq i \leq k)$. □

Example 3.3.11. *Let $C : y^2 = h^2(x)x$ be a singular curve with multiple nodal singularities, where $h(x) = (x - c_1) \cdots (x - c_g)$, and $c_i \neq c_j, \forall i \neq j$. Define the map*

$$\Psi_i : J(C) \longrightarrow \mathbf{C}^*, \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \prod_{j=1}^{n} \frac{y_j + \beta_i h(x_j)}{y_j - \beta_i h(x_j)},$$

where β_i is a square root of c_i, for any $1 \leq i \leq g$. Then $\Psi = \prod_{i=1}^{g} \Psi_i : J(C) \longrightarrow (\mathbf{C}^*)^g$ is a group isomorphism.

In particular, for any $1 \leq i \leq g$, the image of divisor class $((x - c_i)^2, \alpha(x - c_i))$ $(\alpha \neq \pm\beta_i \prod_{j\neq i}(c_i - c_j))$ under Ψ is:

$$((x - c_i)^2, \alpha(x - c_i)) \mapsto (1, \cdots, 1, \underbrace{\frac{\alpha - \beta_i \prod_{j\neq i}(c_i - c_j)}{\alpha + \beta_i \prod_{j\neq i}(c_i - c_j)}}_{\substack{\uparrow \\ i-th\ component}}, 1, \cdots, 1).$$

Example 3.3.12. *For curve $C : y^2 = (x - c)^2 x^{2g-1}$ with $c \neq 0$, define maps:*

$$\Psi_i : J(C) \longrightarrow \mathbf{C}, \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \sum_{j=1}^{n} \frac{x_j^i(x_j - c)}{y_j}, \forall\ 1 \leq i \leq g - 1.$$

And

$$\Psi_g : J(C) \longrightarrow \mathbf{C}^*, \sum_{j=1}^{n}([(x_j, y_j)] - [\infty]) \mapsto \prod_{j=1}^{n} \frac{y_j + \beta(x_j - c)x_j^{g-1}}{y_j - \beta(x_j - c)x_j^{g-1}},$$

where β is a square root of c. Then $\Psi = \prod_{i=1}^{g} \Psi_i : J(C) \longrightarrow (\mathbf{C})^{g-1} \times \mathbf{C}^*$ is a group isomorphism.

In particular, the image of divisor class $(x^2, \alpha x)$ $(\alpha \neq 0)$ under Ψ is:

$$(x^2, \alpha x) \mapsto (\frac{(2g - 3)c}{\alpha}, 0, \cdots, 0, 1).$$

The image of divisor class $((x-c)^2, \alpha(x-c))$ $(\alpha \neq \pm\beta^{2g-1})$ *under* Ψ *is:*

$$((x-c)^2, \alpha(x-c)) \mapsto (0, \cdots, 0, \frac{\alpha - \beta^{2g-1}}{\alpha + \beta^{2g-1}}).$$

4 Arithmetic on Jacobians of singular hyperelliptic curves of positive geometric genus

For a singular hyperelliptic curve $C : y^2 = f(x) = h^2(x)e(x)$ with positive geometric genus, we cannot provide a structured description of its Jacobian as we do for curves of geometric genus zero. However, by Theorem 3.1.12 and Theorem 3.1.16, the set S (as defined in Theorem 3.1.16) forms a subgroup in $J(C)$. In other words, the divisors classes in S still admit the generalized Mumford representation, and Cantor composition can be used to implement addition between them. This, however, is not true for all divisors classes in $J(C)$.

Given a singular curve C and a (partial) normalization C' of C, there exists a canonical surjective (partial) normalization map Φ from $J(C)$ to $J(C')$. We demonstrate that $\ker(\Phi)$ is isomorphic to products of $\mathbf{C}$ and $\mathbf{C}^*$. Moreover, Φ factors through a sequence of partial normalization maps of intermediate curves. We prove that $\ker(\Phi)$ is isomorphic to the product of the kernels of these partial normalization maps.

Furthermore, there is an exact sequence of group schemes:

$$0 \to \ker(\Phi) \xrightarrow{i} J(C) \xrightarrow{\Phi} J(C') \to 0.$$

The group isomorphism obtained in Theorem 3.3 can be lifted to an isomorphism of group schemes. Using this isomorphism, in Section 4.2, we show that the exact sequence splits for curves of geometric genus zero. However, for curves of positive geometric genus that satisfy either:

(1) $\gcd(h(x), e(x)) \neq 1$, or

(2) $\gcd(h(x), e(x)) = 1$, and there exists $(x - c) \mid h$ such that

$$\gcd(e(x), s(x - c) + 2e(c)) = 1,$$

where $s := \frac{e(x)-e(c)}{x-c}\Big|_{x=c}$, the exact sequence associated with their normalization map does not split.

4.1 Kernel of partial normalization map

In this section, we show that the kernel of a (partial) normalization map is isomorphic to products of $\mathbf{C}$ and $\mathbf{C}^*$. Given a singular curve C and a (partial) normalization C' of C, we define a sequence of intermediate curves $C_l (0 \leq l \leq p)$ between C and C', such that the (partial) normalization map $\Phi : J(C) \to J(C')$ can be factored as a composition of partial normalization maps from $J(C_{l-1})$ to $J(C_l) (1 \leq l \leq p)$:

$$\Phi = \Phi_p \circ \cdots \circ \Phi_1.$$

Moreover, we establish that

$$\ker(\Phi) \cong \prod_{l=1}^{p} \ker(\Phi_l).$$

Let S be the set defined in Theorem 3.1.16, i.e., it consists of pairs of polynomials $(a(x)^2, a(x)\bar{V}(x))$ satisfying the following conditions:

(1) $a \mid h$, and a is monic.

(2) $\deg(\bar{V}) < \deg(a)$.

(3) $\gcd(a, \frac{f}{a^2} - \bar{V}^2) = 1$.

By Theorem 3.1.12, each pair $(a(x)^2, a(x)\bar{V}(x))$ in S uniquely represents a divisor class in $J(C)$. Moreover, Theorem 3.1.16 implies that S forms a subgroup of $J(C)$ and Cantor composition can be used to implement the addition within S. However, since parameterization for nonsingular points on C is not available in this case, S is a proper subset of $J(C)$, meaning not all divisor classes admit a generalized Mumford representation.

Theorem 4.1.1. *Let $C : y^2 = f(x) = h^2(x)e(x)$ and $C' : y^2 = f'(x) = s^2(x)e(x)$ where $s \mid h$, be a (partial) normalization of C. Let Φ denote the (partial) normalization map from $J(C)$ to $J(C')$. The kernel of Φ is given by:*

$$\ker(\Phi) = \{(t^2, t\bar{V}) | t \textit{ is monic}, t \mid \frac{h}{s}, \deg(\bar{V}) < \deg(t), \gcd(t, \frac{f}{t^2} - \bar{V}^2) = 1\}. \tag{4.1}$$

In particular, when $s = 1$, we have $\ker(\Phi) = S$.

Proof. Let T denote of set on the right-hand side of Equation (4.1). Clearly, T is subgroup of S. Since every element in S maps to 0 by Equation (3.8), we conclude that $T \subset \ker(\Phi)$. To show the reverse inclusion $\ker(\Phi) \subset T$, it is sufficient to show that if D maps to a principal divisor $\mathrm{div}(r_1(x)y + r_2(x)) \in J(C')$, then $D \in T$. Let

$$D = \sum_{j=1}^{n} [(x_j, y_j)] - [\infty].$$

Then,

$$\Phi(D) = \sum_{j=1}^{n} ([(x_j, \frac{y_j}{(h/s)(x_j)})] - [\infty]) = \mathrm{div}(r_1(x)y + r_2(x)).$$

This means that $\{(x_j, \frac{y_j}{(h/s)(x_j)}) | 1 \leq j \leq n\}$ are precisely the roots of

$$\begin{cases} r_1(x)y + r_2(x) = 0, \\ y^2 = f'(x). \end{cases}$$

Equivalently, points $\{(x_j, y_j\} | 1 \leq j \leq n\}$ are precisely the roots of

$$\begin{cases} r_1(x) \cdot \frac{y}{h/s(x)} + r_2(x) = 0, \\ (\frac{y}{h/s(x)})^2 = f'(x). \end{cases} \tag{4.2}$$

Define $d = \gcd(h/s, r_1)$ and set $t = \frac{h/s}{d}$ such that $\gcd(t, \frac{r_1}{d}) = 1$. Choose $\bar{V} \equiv \frac{r_2}{r_1/d} \pmod{t}$ with $\deg(\bar{V}) < \deg(t)$. We claim that $(t^2, t\bar{V}) \in T$ and that D lies in the divisor class represented by $(t^2, t\bar{V})$. By construction, $(t^2, t\bar{V})$ satisfies all conditions but $\gcd(t, \frac{f}{t^2} - \bar{V}^2) = 1$. To check this, consider any singular point $(c, 0) \in C$. Since none of x_j are equal to c, $r_1(x)y + r_2(x)$ does not vanish at $(c, y_c) \in C'$. Hence,

$$(r_1^2 f' - r_2^2)|_{x=c} \neq 0. \tag{4.3}$$

In particular, if $(x - c) \mid t$, then because $\gcd(t, \frac{r_1}{d}) = 1$, it follows that $\frac{r_1}{d}|_{x=c} \neq 0$. Thus,

$$\frac{f}{t^2} - \bar{V}^2 \equiv \frac{f}{t^2} - \frac{r_2^2}{r_1^2/d^2} \equiv \frac{1}{r_1^2/d^2}(r_1^2 f' - r_2^2) \not\equiv 0 \pmod{x - c}, \tag{4.4}$$

which confirms $\gcd(t, \frac{f}{t^2} - \bar{V}^2) = 1$. Therefore, $(t^2, t\bar{V}) \in T$.

Take w satisfying condition $\star$ so that the corresponding pair (U, V) with

$$U = \frac{f}{t^2} - (tw - \bar{V})^2, \ V = t^2 w - t\bar{V} \tag{4.5}$$

is a representative of $(t^2, t\bar{V})$. Define

$$H(x, y) := (y \cdot \frac{r_1/d}{t} + r_2)(y \cdot \frac{1}{t} + (tw - \bar{V})).$$

We claim that H does not vanish at any singular points and satisfies $\mathrm{div}(H) = D - (U, V)$. Expanding $H(x, y)$, we obtain

$$H = \underbrace{f \cdot \frac{r_1/d}{t^2}}_{①} + \underbrace{r_2(tw - \bar{V})}_{②} + \frac{y}{t} \underbrace{(r_2 + \frac{r_1}{d}(tw - \bar{V}))}_{③}.$$

By our choice of $\bar{V}$,

$$③ \equiv r_2 - \frac{r_1}{d}\bar{V} \equiv 0 \pmod t,$$

ensuring that

$$\frac{y}{t} \times ③ = y(\cdots) \implies (\frac{y}{t} \times ③)|_{(c,0)} = 0,$$

for any singular point $(c, 0)$.

Fix a singular point $(c, 0)$. When $(x - c) \nmid t$, we observe that $①|_{(c,0)} = 0$. Moreover, by the choice of w, we have $(tw - \bar{V})|_{(c,0)} \neq 0$. Since $r_1^2 f' = r_1^2 \frac{f}{h^2/s^2} = \frac{r_1^2}{d^2} \cdot \frac{f}{t^2}$, it follows that

$$r_1^2 f'(c) = 0 \underset{Eq(4.3)}{\implies} r_2(c) \neq 0.$$

Thus, we obtain

$$(① + ②)|_{(c,0)} = r_2(tw - \bar{V})|_{(c,0)} \neq 0.$$

Now, consider the case $(x - c) \mid t$. Using the same argument as in Equation (4.4), we deduce

$$① + ② \equiv f \cdot \frac{r_1/d}{t^2} - r_2\bar{V} \equiv \frac{1}{r_1/d}(f' \cdot r_1^2 - r_2^2) \not\equiv 0. \pmod{x - c}$$

In both case, we conclude that

$$H(c, 0) = (① + ② + ③)|_{(c,0)} = (① + ②)|_{(c,0)} \neq 0.$$

Hence $H(x, y)$ does not vanish at any singular point.

To find the roots of the two factors of $H(x, y)$, we solve

$$\left\{ \begin{array}{c} y \cdot \frac{r_1/d}{t} + r_2 = 0, \\ y^2 = f. \end{array} \right. \iff \left\{ \begin{array}{c} f \cdot \frac{r_1^2/d^2}{t^2} - r_2^2 = f' \cdot r_1^2 - r_2^2 = 0, \\ \frac{y}{h/s} \cdot r_1 + r_2 = 0. \end{array} \right. \iff \left\{ \begin{array}{c} r_1 \cdot \frac{y}{h/s} + r_2 = 0, \\ (\frac{y}{h/s})^2 = f'. \end{array} \right. \tag{4.6}$$

$$\left\{ \begin{array}{c} y \cdot \frac{1}{t} + tw - \bar{V} = 0, \\ y^2 = f. \end{array} \right. \iff \left\{ \begin{array}{c} f \cdot \frac{1}{t^2} - (tw - \bar{V})^2 = 0, \\ y = -t^2 w + t\bar{V}. \end{array} \right. \underset{Eq(4.5)}{\iff} \left\{ \begin{array}{c} U = 0, \\ y = -V. \end{array} \right. \tag{4.7}$$

Equation (4.6) coincides with Equation (4.5), whose roots are exactly (x_j, y_j) $(1 \le j \le n)$. Similarly, the roots of Equation (4.7) correspond to the points in the Weil divisor of $(U, -V)$. Therefore,

$$\operatorname{div}(H) = D - (U, V).$$

Since $H(x, y)$ does not vanish at any singular points and satisfies $\operatorname{div}(H) = D - (U, V)$, it follows that D lies in the divisor class of $(t^2, t\bar{V}) \in T$. Thus, we conclude that $\ker(\Phi) \subset T$. This completes the proof. □

Lemma 4.1.2. *Let C, C' and $\Phi : J(C) \to J(C')$ be as defined in Theorem 4.1.1. Assume $\frac{h}{s} = \prod_{i=1}^{k}(x - c_i)^{n_i}$, where $c_1, \cdots, c_k$ are pairwise distinct. For any element $(t^2, t\bar{V}) \in \ker(\Phi)$ with*

$$t = \prod_{i=1}^{k}(x - c_i)^{m_i},\ 0 \le m_i \le n_i, \forall 1 \le i \le k,$$

there exists a unique decomposition:

$$(t^2, t\bar{V}) = \sum_{i=1}^{k}((x - c_i)^{2m_i}, (x - c_i)^{m_i}\bar{V}_i), \tag{4.8}$$

where $\bar{V}_i \equiv \prod_{j \ne i}(x - c_j)^{m_j}\bar{V} \pmod{(x - c_i)^{m_i}}$ with $\deg(\bar{V}_i) < m_i, \forall 1 \le i \le k$.

Proof. Fix any $1 \le l \le k$, we claim that

$$\sum_{i=1}^{l}((x - c_i)^{2m_i}, (x - c_i)^{m_i}\bar{V}_i) = (\prod_{i=1}^{l}(x - c_i)^{2m_i}, \prod_{i=1}^{l}(x - c_i)^{m_i}\bar{V}), \tag{4.9}$$

where $\bar{V} \equiv \frac{\bar{V}_i}{\prod_{j \ne i}(x - c_j)^{m_j}} \pmod{(x - c_i)^{m_i}}, \forall 1 \le i \le l$ and $\deg(\bar{V}) < \sum_{i=1}^{l} m_i$. Then Equation (4.8) is a special case of Equation (4.9) when $l = k$. It is sufficient to prove Equation (4.9), which can be done by induction on l.

When $l = 1$, Equation (4.9) holds true trivially. Assume it holds for $l - 1$, i.e,

$$\sum_{i=1}^{l-1}((x - c_i)^{2m_i}, (x - c_i)^{m_i}\bar{V}_i) = (\prod_{i=1}^{l-1}(x - c_i)^{2m_i}, \prod_{i=1}^{l-1}(x - c_i)^{m_i}\bar{V}'),$$

where $\bar{V}' \equiv \frac{\bar{V}_i}{\prod_{j \ne i, 1 \le j \le l-1}(x - c_j)^{m_j}} \pmod{(x - c_i)^{m_i}}, \forall 1 \le i \le l - 1$. By Theorem 3.1.16, addition of any two elements in S is closed and can be implemented via Cantor Composition. Since

$$((x - c_i)^{2m_i}, (x - c_i)^{m_i}\bar{V}_i) \in \ker(\Phi) \subset S,\ 1 \le i \le k,$$

we have

$$(\prod_{i=1}^{l-1}(x - c_i)^{2m_i}, \prod_{i=1}^{l-1}(x - c_i)^{m_i}\bar{V}') \in S.$$

Thus by Cantor composition,

$$\begin{aligned}\sum_{i=1}^{l}((x - c_i)^{2m_i}, (x - c_i)^{m_i}\bar{V}_i) =& (\prod_{i=1}^{l-1}(x - c_i)^{2m_i}, \prod_{i=1}^{l-1}(x - c_i)^{m_i}\bar{V}') + ((x - c_l)^{2m_l}, (x - c_l)^{m_l}\bar{V}_l) \\ =& (\prod_{i=1}^{l}(x - c_i)^{2m_i}, \prod_{i=1}^{l}(x - c_i)^{m_i}\bar{V}),\end{aligned}$$

where $\bar{V} \equiv h_1 \prod_{i=1}^{l-1}(x-c_i)^{m_i}\bar{V}_l + h_2(x-c_l)^{m_l}\bar{V}' \pmod{\prod_{i=1}^{l}(x-c_i)^{m_i}}$, $\deg(\bar{V}) < \sum_{i=1}^{l} m_i$ and $h_1 \prod_{i=1}^{l-1}(x-c_i)^{2m_i} + h_2(x-c_l)^{2m_l} = 1$.

Thus we have

$$\begin{aligned}\bar{V} &\equiv h_2(x-c_l)^{m_l}\bar{V}' \equiv \frac{1}{(x-c_l)^{m_l}} \cdot \frac{\bar{V}_i}{\prod_{j\neq i, 1\leq j\leq l-1}(x-c_j)^{m_j}} \\ &\equiv \frac{\bar{V}_i}{\prod_{j\neq i, 1\leq j\leq l}(x-c_j)^{m_j}} \pmod{(x-c_i)^{m_i}},\ \forall 1 \leq i \leq l-1. \\ \text{and } \bar{V} &\equiv h_1 \prod_{i=1}^{l-1}(x-c_i)^{m_i}\bar{V}_l \equiv \frac{\bar{V}_l}{\prod_{i=1}^{l-1}(x-c_i)^{m_i}} \pmod{(x-c_l)^{m_l}}.\end{aligned}$$

This proves Equation (4.9).

Suppose

$$(t^2, t\bar{V}) = \sum_{i=1}^{k}((x-c_i)^{2m_i'}, (x-c_i)^{m_i'}\bar{V}_i'),$$

where $((x-c_i)^{2m_i'}, (x-c_i)^{m_i'}\bar{V}_i') \in \ker(\Phi)$, $\forall 1 \leq i \leq k$. Then using Equation (4.9), we obtain $m_i = m_i'$, $\forall 1 \leq i \leq k$ and

$$\bar{V} \equiv \frac{\bar{V}_i'}{\prod_{j\neq i}(x-c_j)^{m_j}} \implies \bar{V}_i \underset{Eq(4.8)}{\equiv} \prod_{j\neq i}(x-c_j)^{m_j}\bar{V} \equiv \bar{V}_i' \pmod{(x-c_i)^{m_i}},\ 1 \leq i \leq k.$$

Since $\deg(\bar{V}_i) < m_i$ and $\deg(\bar{V}_i') < m_i$, it follows that $\bar{V}_i = \bar{V}_i'$, $1 \leq i \leq k$, proving the uniqueness.

Thus, the decomposition in Equation (4.8) is both valid and unqiue, completing the proof. □

Corollary 4.1.3. *Let C, C' and $\Phi : J(C) \to J(C')$ be as defined in Theorem 4.1.1. Assume $\frac{h}{s} = \prod_{i=1}^{k}(x-c_i)^{n_i}$, where $c_1, \cdots, c_k$ are pairwise distinct. Then, the kernel of Φ decomposes as*

$$\ker(\Phi) \cong \mathbf{C}^{p-r} \times (\mathbf{C}^*)^r,$$

where $r = |\{1 \leq i \leq k \mid (x-c_i) \nmid f'\}|$ and $p = \sum_{i=1}^{k} n_i$.

Proof. For any $1 \leq i \leq k$, we define a constant

$$d_i := (x - \frac{f}{(x-c_i)^{2n_i}})|_{x=c_i}$$

and a curve

$$C_i : y^2 = (x-c_i)^{2n_i}(x-d_i).$$

By Theorem 3.1.16, the Jacobian group of C_i is given by

$$\begin{aligned}J(C_i) =\{&((x-c_i)^{2m_i}, (x-c_i)^{m_i}\bar{V}_i) \mid 0 \leq m_i \leq n_i, \deg(\bar{V}_i) < m_i, \\ &\gcd((x-c_i)^{m_i}, (x-c_i)^{2n_i-2m_i}(x-d_i) - \bar{V}_i^2) = 1.\}\end{aligned}$$

For $m_i = 0$, we must have $\bar{V}_i = 0$. For $0 < m_i \leq n_i$, the gcd condition simplifies as follows:

$$\begin{aligned}
&\gcd((x-c_i)^{m_i}, (x-c_i)^{2n_i-2m_i}(x-d_i) - \bar{V}_i^2) = 1 \\
\Longleftrightarrow\ &((x-c_i)^{2n_i-2m_i}(x-d_i) - \bar{V}_i^2)|_{x=c_i} \neq 0 \\
\Longleftrightarrow\ &((x-c_i)^{2n_i-2m_i} \cdot \frac{f}{(x-c_i)^{2n_i}} - \bar{V}_i^2)|_{x-c_i} = (\frac{f}{(x-c_i)^{2m_i}} - \bar{V}_i^2)|_{x-c_i} \neq 0 \\
\Longleftrightarrow\ &\gcd((x-c_i)^{m_i}, \frac{f}{(x-c_i)^{2m_i}} - \bar{V}_i^2) = 1.
\end{aligned}$$

Thus, each $J(C_i)$ embeds naturally into $\ker(\Phi)$. Define a homomorphism

$$\psi : \prod_{i=1}^{k} J(C_i) \longrightarrow \ker(\Phi),$$

$$(((x-c_1)^{2m_1}, (x-c_1)^{m_1}\bar{V}_1), \cdots, ((x-c_k)^{2m_k}, (x-c_k)^{m_k}\bar{V}_k)) \mapsto \sum_{i=1}^{k}((x-c_i)^{2m_i}, (x-c_i)^{m_i}\bar{V}_i).$$

By Lemma 4.1.2, ψ is a bijection, which gives

$$\ker(\Phi) \cong \prod_{i=1}^{k} J(C_i).$$

For each $1 \leq i \leq k$, Theorem 3.3.4 and Theorem 3.3.6 yield

$$J(C_i) \cong \begin{cases} \mathbb{C}^{n_i}, & \text{if } d_i = c_i, \\ \mathbb{C}^{n_i-1} \times \mathbb{C}^*, & \text{if } d_i \neq c_i. \end{cases}$$

By the construction of d_i, we have

$$d_i \neq c_i \Longleftrightarrow \frac{f}{(x-c_i)^{2n_i}}|_{x=c_i} \neq 0 \Longleftrightarrow (x-c_i) \nmid \frac{f}{(x-c_i)^{2n_i}} \Longleftrightarrow (x-c_i) \nmid f'.$$

Let r be the number of indices $i = 1, \cdots, k$ satisfying $(x-c_i) \nmid f'$ and $p = \sum_{i=1}^{k} n_i$. Summing over all i, we obtain

$$\prod_{i=1}^{k} J(C_i) \cong \mathbb{C}^{p-r} \times (\mathbb{C}^*)^r.$$

Thus, combining this with $\ker(\Phi) \cong \prod_{i=1}^{k} J(C_i)$, we conclude

$$\ker(\Phi) \cong \mathbb{C}^{p-r} \times (\mathbb{C}^*)^r.$$

□

Theorem 4.1.4. *Let C, C' and $\Phi : J(C) \longrightarrow J(C')$ be as defined in Theorem 4.1.1. Suppose $\frac{h}{s} = \prod_{l=1}^{p}(x-c_l)$, where $c_1, \cdots, c_p$ may not be pairwise distinct. Define the intermediate curves*

$$C_l : y^2 = \frac{f(x)}{\prod_{t=1}^{l}(x-c_t)^2}, \ \forall 1 \leq l \leq p,$$

and set $C_0 = C$, $C_p = C'$. Let Φ_l denote the (partial) normalization map from $J(C_{l-1})$ to $J(C_l)$, for each $1 \le l \le p$. Then $\Phi = \Phi_p \circ \cdots \circ \Phi_1$ and the kernel of Φ decomposes as

$$\ker(\Phi) \cong \prod_{l=1}^{p} \ker(\Phi_l).$$

Proof. It is evident to see that $\Phi = \Phi_p \circ \cdots \circ \Phi_1$. To show $\ker(\Phi) \cong \prod_{l=1}^{p} \ker(\Phi_l)$, it suffices to establish that

$$\prod_{l=1}^{p} \ker(\Phi_l) \cong \mathbb{C}^{p-r} \times (\mathbb{C}^*)^r$$

by Lemma 4.1.3, where r is as defined in Lemma 4.1.3.

For any fixed $1 \le l \le p$, Theorem 4.1.1 gives

$$\ker(\Phi_l) = \{(1,0)\} \cup \{((x-c_l)^2, \alpha(x-c_l)) \mid \alpha \in \mathbb{C}, (\frac{f(x)}{\prod_{t=1}^{l}(x-c_t)^2} - \alpha^2)|_{x=c_l} \neq 0\}.$$

Define

$$d_l := (x - \frac{f(x)}{\prod_{t=1}^{l}(x-c_t)^2})|_{x=c_l},$$

so that the condition $(\frac{f(x)}{\prod_{t=1}^{l}(x-c_t)^2} - \alpha^2)|_{x=c_l} \neq 0$ is equivalent to $((x-d_l) - \alpha^2)|_{x=c_l} \neq 0$. Thus,

$$\ker(\Phi_l) = \{(1,0)\} \cup \{((x-c_l)^2, \alpha(x-c_l)) \mid \alpha \in \mathbb{C}, ((x-d_l) - \alpha^2)|_{x=c_l} \neq 0\}.$$

By Theorem 3.1.11, this corresponds to the Jacobian of the curve

$$C_l : y^2 = (x-c_l)^2(x-d_l).$$

If $(x-c_l) \mid \frac{f}{\prod_{t=1}^{l}(x-c_t)^2}$, then $d_l = c_l$, and by Theorem 3.3.4,

$$\ker(\Phi_l) \cong J(y^2 = (x-c_l)^3) \cong \mathbb{C}.$$

If $(x-c_l) \nmid \frac{f}{\prod_{t=1}^{l}(x-c_t)^2}$, then $d_l \neq c_l$, and by Theorem 3.3.6,

$$\ker(\Phi_l) \cong J(y^2 = (x-c_l)^2(x-d_l)) \cong \mathbb{C}^*.$$

Thus,

$$\ker(\Phi_l) \cong \begin{cases} \mathbb{C}, & \text{if } (x-c_l) \mid \frac{f}{\prod_{t=1}^{l}(x-c_t)^2}, \\ \mathbb{C}^*, & \text{if } (x-c_l) \nmid \frac{f}{\prod_{t=1}^{l}(x-c_t)^2}. \end{cases}$$

This implies

$$\prod_{l=1}^{p} \ker(\Phi_l) \cong \mathbb{C}^{p-a} \times (\mathbb{C}^*)^a,$$

where

$$a = |\{1 \leq l \leq p \mid (x - c_l) \nmid \frac{f}{\prod_{t=1}^{l}(x - c_t)^2}\}|.$$

What is left is to show $a = r$. Choose $b_1, \cdots, b_k \in \{1, \cdots, p\}$ such that $c_{b_1}, c_{b_2}, \cdots, c_{b_k}$ are pairwise distinct and $\frac{h}{s} = \prod_{i=1}^{k}(x - c_{b_i})^{n_i}$ for some $n_i \in \mathbb{N}_+$. Then,

$$r = |\{1 \leq i \leq k \mid (x - c_{b_i}) \nmid f'\}|.$$

For each fixed $1 \leq i \leq k$,

$$|\{1 \leq l \leq p \mid c_l = c_{b_i}, (x - c_l) \nmid \frac{f}{\prod_{t=1}^{l}(x - c_t)^2}\}| = \begin{cases} 0, & \text{if } (x - c_{b_i}) \mid f', \\ 1, & \text{if } (x - c_{b_i}) \nmid f'. \end{cases}$$

Summing over all i,

$$r = \sum_{i=1}^{k} |\{1 \leq l \leq p \mid c_l = c_{b_i}, (x - c_l) \nmid \frac{f}{\prod_{t=1}^{l}(x - c_t)^2}\}| = a.$$

Thus $a = r$, which completes the proof. □

4.2 Splitting property of the exact sequence associated with partial normalization

Let $C : y^2 = f(x) = h^2(x)e(x)$ be a singular hyperelliptic curve and $C' : y^2 = f'(x) = s^2(x)e(x)$, where $s \mid h$ be a (partial) normalization of C. There exists a (partial) normalization map $\Phi : J(C) \to J(C')$ as defined in Definition 3.2.1. Since Φ is surjective, we obtain the exact sequence:

$$0 \to \ker(\Phi) \xrightarrow{i} J(C) \xrightarrow{\Phi} J(C') \to 0. \tag{4.10}$$

Let C_l, Φ_l $(1 \leq l \leq p)$ be as defined in Theorem 4.1.4. According to Theorem 4.1.4, we have the factorization $\Phi = \Phi_p \circ \cdots \circ \Phi_1$ and the decomposition $\ker(\Phi) \cong \prod_{l=1}^{p} \ker(\Phi_l)$. Using this, we establish that sequence (4.10) splits if and only if

$$0 \to \ker(\Phi_l) \to J(C_{l-1}) \xrightarrow{\Phi_l} J(C_l) \to 0$$

splits for each $l = 1, \cdots, p$. Therefore, it suffices to study the splitting property of sequence (4.10) in the case when $\deg(\frac{h}{s}) = 1$.

Sequence (4.10) is in fact an exact sequence of group schemes. We show that the exact sequence (4.10) splits when C has geometric genus 0. However, for the normalization map of certain families of curves of positive geometric genus, the corresponding exact sequence does not split.

Proposition 4.2.1. *We choose the same setting and notation as in Theorem 4.1.4, the sequence* (4.10) *splits if and only if*

$$0 \to \ker(\Phi_l) \to J(C_{l-1}) \xrightarrow{\Phi_l} J(C_l) \to 0$$

splits for each $l = 1, \cdots, p$.

Proof. The statement is equivalent to showing that

$$J(C) \cong J(C') \times \ker(\Phi) \text{ if and only if } J(C_{l-1}) \cong J(C_l) \times \ker(\Phi_l),\ \forall 1 \leq l \leq p.$$

Assume $J(C) \cong J(C') \times \ker(\Phi)$. Then, for C_{p-1}, we have

$$\begin{aligned} J(C_{p-1}) &\cong J(C)/\ker(\Phi : C \to C_{p-1}) \underset{Thm\ 4.1.4}{\cong} J(C)/\prod_{k=1}^{p-1} \ker(\Phi_k) \\ &\cong J(C') \times \ker(\Phi)/\prod_{k=1}^{p-1} \ker(\Phi_k) \underset{Thm\ 4.1.4}{\cong} J(C') \times \ker(\Phi_p). \end{aligned}$$

Now, fix any $l < p$ and assume by induction that

$$J(C_{k-1}) \cong J(C_k) \times \ker(\Phi_k),\ \forall l < k \leq p.$$

Then, by using this isomorphism iteratively, we obtain

$$J(C_l) \cong J(C') \times \prod_{k=l+1}^{p} \ker(\Phi_k).$$

Thus,

$$\begin{aligned} J(C_{l-1}) &\cong J(C)/\ker(\Phi : C \to C_{l-1}) \underset{Thm4.1.4}{\cong} J(C)/\prod_{k=1}^{l-1} \ker(\Phi_k) \\ &\cong J(C') \times \ker(\Phi)/\prod_{k=1}^{l-1} \ker(\Phi_k) \underset{Thm4.1.4}{\cong} J(C') \times \prod_{k=l}^{p} \ker(\Phi_k) \cong J(C_l) \times \ker(\Phi_l). \end{aligned}$$

By induction, we conclude that

$$J(C_{l-1}) \cong J(C_l) \times \ker(\Phi_l),\ \forall 1 \leq l \leq p.$$

Conversely, assume that

$$J(C_{l-1}) \cong J(C_l) \times \ker(\Phi_l),\ \forall 1 \leq l \leq p.$$

Applying this iteratively, we obtain

$$J(C) \cong J(C_1) \times \ker(\Phi_1) \cong \cdots \cong J(C') \times \prod_{k=1}^{p} \ker(\Phi_k) \underset{Thm4.1.4}{\cong} J(C') \times \ker(\Phi).$$

Since both direction hold, the proof is complete. □

Theorem 4.2.2. *Let $C : y^2 = f(x) = h^2(x)x$ and $C' : y^2 = f'(x) = s^2(x)x$ with $s \mid h$. Then, the exact sequence associated with the partial normalization map from $J(C)$ to $J(C')$ splits:*

$$0 \to \ker(\Phi) \to J(C) \xrightarrow{\Phi} J(C') \to 0.$$

Proof. By Proposition 4.2.1, it suffices to prove the statement in the case when $\deg(h/s) = 1$. Assume $\frac{h}{s} = x - c$. Then, by Corollary 4.1.3, we have

$$\ker(\Phi) \cong \begin{cases} \mathbf{C}, & \text{if } (x-c) \mid f', \\ \mathbf{C}^*, & \text{if } (x-c) \nmid f'. \end{cases}$$

Now, assume $s(x) = \prod_{i=1}^{k}(x-c_i)^{m_i}$, where $c_1, \cdots, c_k$ are pairwise distinct. By Theorem 3.3.10, we obtain

$$J(C') \cong \mathbf{C}^{\sum_{i=1}^{k} m_i - l'} \times (\mathbf{C}^*)^{l'}, \text{ and } J(C) \cong \mathbf{C}^{\sum_{i=1}^{k} m_i + 1 - l} \times (\mathbf{C}^*)^{l}$$

where l' is the number of nonzero c_i $(1 \le i \le k)$ and l is the number of nonzero elements in the set $\{c, c_1, \cdots, c_k\}$.

If $(x-c) \nmid f'$, then $c \neq 0, c_1, \cdots, c_k$, which implies $l = l' + 1$. Hence,

$$J(C) \cong J(C') \times \mathbf{C}^*.$$

If $(x-c) \mid f'$, there are two cases: either $c = 0$ or $c = c_i$ for some nonzero c_i. In both case, $l = l'$, so

$$J(C) \cong J(C') \times \mathbf{C}.$$

In both cases, we conclude that $J(C) \cong J(C') \times \ker(\Phi)$, meaning that the exact sequence splits. □

In general, the exact sequence associated with the normalization map does not split. The above theorem shows that singular curves of geometric genus 0 provide a special case where the sequence does split. In the rest of this section, we will present certain families of singular curves of positive geometric genus as counterexamples, for which the exact sequence (4.10) does not split.

Theorem 4.2.3. *Let $C : y^2 = x^2 e(x)$ be a singular hyperelliptic curve, where $e(x)$ has no repeated roots and $\deg(e(x)) = 2g - 1 \geq 3$. Let $C' : y^2 = e(x)$ be the normalization of C, and let Φ denote the normalization map from $J(C)$ to $J(C')$. If $x \mid e(x)$, then the following exact sequence does not split as a sequence of group schemes:*

$$0 \to \ker(\Phi) \xrightarrow{i} J(C) \xrightarrow{\Phi} J(C') \to 0.$$

Proof. By Theorem 4.1.1 and Corollary 4.1.3, we obtain

$$\ker(\Phi) = \{(x^2, \alpha x) | \alpha \in \mathbf{C}^*\} \cup \{(1, 0)\} \cong \mathbf{C}.$$

Applying Cantor composition, we find that

$$(x^2, \alpha_1 x) + (x^2, \alpha_2 x) = (x^2, \frac{\alpha_1 \alpha_2}{\alpha_1 + \alpha_2} x), \ \forall \alpha_1 \neq -\alpha_2.$$

From this addition law, we can define an isomorphism between $\ker(\Phi)$ and $\mathbf{C}$:

$$\theta : \ker(\Phi) \to \mathbf{C}, (x^2, \alpha x) \mapsto \frac{1}{\alpha}, (1, 0) \mapsto 0.$$

Suppose the exact sequence splits, then there exists $\phi : J(C) \to \ker(\Phi)$ such that $\phi \circ i = id_{\ker(\Phi)}$. Composing ϕ with θ, we obtain

$$\psi : J(C) \to \mathbf{C}, \text{ where } (x^2, \alpha x) \mapsto \frac{1}{\alpha}, \ \forall \alpha \in \mathbf{C}^* \text{ and } (1, 0) \mapsto 0.$$

Consider $(U, V) = \sum_{j=1}^{2g-1}([(x_j, y_j)] - [\infty])$, where

$$U = e(x) - \alpha^2 (x^{g-1} - 1)^2, \text{ and } V = \alpha(x^g - x). \tag{4.11}$$

It is clear that (U, V) is a representative of $(x^2, \alpha x)$ in $J(C)$, so the image of $(x^2, \alpha x)$ should be the sum of the image of $[(x_j, y_j)] - [\infty]$ $(1 \le j \le 2g - 1)$. Restricting ψ to divisors of the form $[(x, y)] - [\infty]$, ψ is a bivariate function in x and y. And $\psi \in \mathbb{C}[x, y, \frac{1}{x}]/(y^2 = f(x))$ as it is a regular function between affine varieties. Since $\psi(x, y) = -\psi(x, -y)$, we can write

$$\psi(x, y) = \frac{r(x)y}{x^k} \tag{4.12}$$

for some $k \in \mathbb{N}$ and $r(x) \in \mathbb{C}[x]$. Writing

$$\frac{r(x) \cdot \alpha(x^g - x)}{x^k} = a_n x^n + \cdots + a_0 + \cdots + a_{-m} x^{-m}, \tag{4.13}$$

with $a_i \in \mathbb{C}, \forall -m \leq i \leq n$, and $p_k = \sum_{j=1}^{2g-1} x_j^k, q_k = \sum_{j=1}^{2g-1} \frac{1}{x_j^k}$. We obtain

$$\frac{1}{\alpha} = \psi((x^2, \alpha x)) = \sum_{j=1}^{2g-1} \psi(x_j, y_j) \underset{Eq(4.11),(4.12),(4.13)}{=} \alpha(a_n p_n + \cdots + a_0(2g-1) + \cdots a_{-m} q_m), \ \forall \alpha \in \mathbb{C}^*.$$

Applying the result of Lemma 4.2.4, we conclude that

$$a_n = \cdots a_1 = a_{-2} = \cdots = a_{-m} = 0.$$

Thus, we simplify Equation (4.13) to

$$\frac{r(x) \cdot \alpha(x^g - x)}{x^k} = a_0 + a_{-1}\frac{1}{x},$$

which implies $(x^{g-1} - 1) \mid (a_0 x + a_{-1})$. So that we must have $g = 2$ and $a_0 = -a_{-1}$. While in this case, we compute

$$\psi((x^2, \alpha x)) = \alpha(a_0 \cdot 3 - a_0 q_1) \underset{Eq(4.15)}{=} a_0 \alpha(3 - \frac{s + 2\alpha^2}{\alpha^2}) = \frac{a_0}{\alpha}(\alpha^2 - s) \neq \frac{1}{\alpha},$$

where $s := \frac{e(x)}{x}|_{x=0} \neq 0$. This contradiction implies that ϕ cannot exist, so the exact sequence does not split as a sequence of group schemes. □

Lemma 4.2.4. *Let $e(x) \in \mathbb{C}[x]$ be a polynomial satisfying $x \mid e(x), x^2 \nmid e(x)$ and $\deg(e(x)) = 2g - 1 \geq 3$. Define*

$$U := e(x) - \alpha^2(x^{g-1} - 1)^2, \tag{4.14}$$

where $\alpha \in \mathbb{C}^*$, and let x_j $(1 \leq j \leq 2g-1)$ be the roots of $U(x) = 0$. Define

$$p_k = \sum_{j=1}^{2g-1} x_j^k, \ q_k = \sum_{j=1}^{2g-1} \frac{1}{x_j^k}, \ k \in \mathbb{N}_+.$$

By varying α, p_k, q_k can be considered as functions of α. For each k, we have $p_k \in \mathbb{C}[\alpha]$ and $q_k \in \mathbb{C}(\alpha)$. Moreover, $\deg(p_k) = 2k$ and $2k$ is the smallest number n such that $\alpha^n q_k \in \mathbb{C}[\alpha]$ for each k.

Proof. Let $w_i (1 \leq i \leq 2g-1)$ denote the elementary functions of $x_j (1 \leq j \leq 2g-1)$. By Equation (4.14) and Vieta's Formula, w_i can be considered as a polynomial in α when we vary α for any i. Moreover, it is easy to see that

$$\deg(w_i) \leq 2, \forall i, \text{ and } \deg(w_1) = 2.$$

Fix any $k \in \mathbb{N}_+$, p_k is a symmetric function of $x_j (1 \leq j \leq 2g-1)$, so it can be expressed as a polynomial in $w_i (1 \leq i \leq 2g-1)$. It turns out that $p_k \in \mathbb{C}[\alpha], \ \forall k$.

Applying Newton's Identities [Mea92], we obtain the recurrence relations:

$$(-1)^k p_k = \sum_{i=1}^{k-1} (-1)^{i-1} w_{k-i} p_i - k w_k, \forall 1 \le k \le 2g-1,$$
$$(-1)^k p_k = \sum_{i=k-(2g-1)}^{k-1} (-1)^{i-1} w_{k-i} p_i, \forall k > 2g-1.$$

When $k=1$, we have $\deg(p_1) = \deg(w_1) = 2$. Assume by induction that $\deg(p_d) = 2d$ for each $d \le k$, then $\deg(w_1 p_k) = 2(k+1)$ and $\deg(w_{k+1-i} p_i) \le 2(i+1) < 2(k+1)$ for each $i < k$. Thus, it follows that $\deg(p_{k+1}) = 2(k+1)$. This proves $\deg(p_k) = 2k$ for any k by induction.

Similarly, $q_k (k \in \mathbb{N}_+)$ are symmetric functions of $\frac{1}{x_j}(1 \le j \le 2g-1)$, which are the roots of $x^{2g-1}U(\frac{1}{x}) = 0$. Let v_i $(1 \le i \le 2g-1)$ denote the elementary functions of $\frac{1}{x_j}(1 \le j \le 2g-1)$. By Vieta's formula, we obtain

$$\alpha^2 v_i = w_{2g-1-i}, \ \forall 1 \le i \le 2g-1.$$

For any i, $w_i \in \mathbb{C}[\alpha]$, it follows that $v_i \in \mathbb{C}(\alpha)$, and the smallest n for which $\alpha^n v_i \in \mathbb{C}[\alpha]$ is at most 2. Applying Newton's Identities gives:

$$(-1)^k q_k = \sum_{i=1}^{k-1} (-1)^{i-1} v_{k-i} q_i - k v_k, \forall 1 \le k \le 2g-1,$$
$$(-1)^k q_k = \sum_{i=k-(2g-1)}^{k-1} (-1)^{i-1} v_{k-i} q_i, \forall k > 2g-1.$$

When $k=1$, we have

$$q_1 = v_1 = \frac{1}{\alpha^2} w_{2g-2} = \begin{cases} \frac{s}{\alpha^2}, & \text{if } g \ge 3 \\ \frac{s+2\alpha^2}{\alpha^2}, & \text{if } g = 2. \end{cases} \tag{4.15}$$

where s is the coefficient of the linear term in $e(x)$. By assumption $x^2 \nmid e(x)$, we have $s \ne 0$, implying that the statement holds for $k=1$.

Suppose the statement is true for all $d \le k$. Then by the recurrence relations, $q_{k+1} \in \mathbb{C}(\alpha)$. And the smallest number n such that $\alpha^n v_1 q_k \in \mathbb{C}[\alpha]$ is $2(k+1)$, while the smallest n for $\alpha^n v_{k-i} q_i \in \mathbb{C}[\alpha]$ is at most $2(i+1)$, which is less than $2(k+1)$ for all $i < k$. Therefore, the smallest number n such that $\alpha^n q_{k+1} \in \mathbb{C}[\alpha]$ is $2(k+1)$. By induction on k, the statement follows. □

Theorem 4.2.3 implies that the exact sequence (4.10) does not split when C contains a (higher) cusp and C' is its normalization. Next, we consider the case when C has only nodal singularities and show that a similar non-splitting phenomenon occurs for a certain family of these curves. Our approach follows the same general strategy as before. Instead of working with the image of $(x^2, \alpha x)$, we first construct divisor classes lying outside of S that admit a generalized Mumford representation, and then use the images of these divisors to derive a contradiction.

Proposition 4.2.5. *Let $C : y^2 = f(x) = h^2(x)e(x)$, where $e(x)$ has no repeated roots and $\deg(f) = 2g+1$. Suppose $(x-c) \mid f(x)$, and the exponent of $(x-c)$ in $h(x)$ is $k \ge 1$. Then the pair $((x-c)^{2k+1}, (x-c)^k \bar{V})$ represents a divisor class in $J(C)$, where $\bar{V}$ satisfies following conditions:*

(1) $\deg(\bar{V}) < k+1$.

(2) $(x-c) \mid \frac{f}{(x-c)^{2k}} - \bar{V}^2$.

(3) $(x-c)^2 \nmid \frac{f}{(x-c)^{2k}} - \bar{V}^2$.

Proof. We apply the same approach as in the proof of Theorem 3.1.12 to show that $((x-c)^{2k+1}, (x-c)^k\bar{V})$ represents a divisor class. We define

$$V(x) = (x-c)^{2k+1}w(x) - (x-c)^k\bar{V}, \text{ and } U(x) = \frac{f(x) - V(x)^2}{(x-c)^{2k+1}},$$

where $w(x)$ is chosen to satisfy

$$\deg(V) > max\{g, 2k+1\}, \text{ and } \gcd(h, U) = 1.$$

Under these conditions, (U, V) represents a divisor in $J(C)$ and can be reduced to $((x-c)^{2k+1}, (x-c)^k\bar{V})$.

Assume both (U_1, V_1) and (U_2, V_2) can be reduced to $((x-c)^{2k+1}, (x-c)^k\bar{V})$. This implies that

$$U_i = \frac{f - V_i^2}{(x-c)^{2k+1}},\ i = 1, 2, \tag{4.16}$$

$$\text{and } -V_i \equiv (x-c)^k\bar{V} \pmod{(x-c)^{2k+1}},\ i = 1, 2. \tag{4.17}$$

Define

$$H(x,y) := \frac{1}{x-c}\Big(\frac{y}{(x-c)^k} - \frac{V_1}{(x-c)^k}\Big)\Big(\frac{y}{(x-c)^k} + \frac{V_2}{(x-c)^k}\Big).$$

We claim that H does not vanish at any singular points and $\operatorname{div}(H) = (U_1, V_1) - (U_2, V_2)$. Consider any singular point $(c', 0)$, there are two cases: $c' = c$ or $c' \neq c$.

Case 1. $c' = c$

Expanding H, we obtain

$$H = \underbrace{\frac{f - V_1V_2}{(x-c)^{2k+1}}}_{\textcircled{1}} + y\underbrace{\frac{(V_2 - V_1)}{(x-c)^{2k+1}}}_{\textcircled{2}}.$$

From Equation (4.17), we have$\bar{V}_2 - \bar{V}_1 \equiv 0 \pmod{(x-c)^{2k+1}}$, which implies that $\textcircled{2}|_{(c,0)} = y(\cdots)|_{(c,0)} = 0$. Furthermore,

$$\textcircled{1} \underset{Eq(4.17)}{\equiv} \frac{f - (x-c)^{2k}\bar{V}^2}{(x-c)^{2k+1}} \underset{Condition(3)}{\not\equiv} 0 \pmod{(x-c)}.$$

Thus, $H|_{(c,0)} = (\textcircled{1} + \textcircled{2})|_{(c,0)} \neq 0$.

Case 2. $c' \neq c$

In this case,

$$\frac{y}{(x-c)^k}|_{(c',0)} = 0.$$

Additionally,

$$U_i|_{(c',0)} = -\frac{V_i^2}{(x-c)^{2k+1}}|_{(c',0)} \neq 0, \implies V_i|_{(c',0)} \neq 0,\ i = 1, 2.$$

Thus,

$$H|_{(c',0)} = \frac{1}{x-c}\Big(-\frac{V_1}{(x-c)^k}\Big)\Big(-\frac{V_2}{(x-c)^k}\Big)|_{(c',0)} \neq 0.$$

In both case, we conclude that $H|_{(c',0)} \neq 0$, meaning that H does not vanish at any singular points.

Moreover,

$$\frac{y}{(x-c)^k} - \frac{V_1}{(x-c)^k} = 0 \Longleftrightarrow \begin{cases} y = V_1(x), \\ \frac{y^2}{(x-c)^{2k}} - \frac{V_1^2}{(x-c)^{2k}} \underset{Eq(4.16)}{=} U_1 \cdot (x-c) = 0. \end{cases}$$

Similarly,

$$\frac{y}{(x-c)^k} + \frac{V_2}{(x-c)^k} = 0 \Longleftrightarrow \begin{cases} y = -V_2(x), \\ \frac{y^2}{(x-c)^{2k}} - \frac{V_2}{(x-c)^{2k}} \underset{Eq(4.16)}{=} U_2 \cdot (x-c) = 0. \end{cases}$$

Since H is nonzero at $(c, 0)$, its zeros correspond exactly to the points occur in the divisor $(U_1, V_1)+(U_2, -V_2)$. Consequently,

$$\operatorname{div}(H) = (U_1, V_1) - (U_2, V_2).$$

This implies (U_1, V_1) and (U_2, V_2) are equivalent. Since there are infinitely choice for w satisfying the given conditions, there exist infinitely many divisors that can be reduced to $((x-c)^{2k+1}, (x-c)^k\bar{V})$. The argument above shows that any two such divisors are equivalent. Thus, $((x-c)^{2k+1}, (x-c)^k\bar{V})$ can represent the divisor class of divisors that can be reduced to it. □

Remark 4.2.6. *For any divisor class represented by $((x-c)^{2k+1}, (x-c)^k\bar{V})$, choose (U, V) as one of its representative, i.e., (U, V) can be reduced to $((x-c)^{2k+1}, (x-c)^k\bar{V})$. Then it is evident that $(U, -V)$ is a representative of $((x-c)^{2k+1}, -(x-c)^k\bar{V})$. Consequently, we have*

$$((x-c)^{2k+1}, (x-c)^k\bar{V}) + ((x-c)^{2k+1}, -(x-c)^k\bar{V}) = (1, 0).$$

Remark 4.2.7. *Let $(\widetilde{U}, \widetilde{V})$ be the reduction result of $((x-c)^{2k+1}, (x-c)^k\bar{V})$. If $(\widetilde{U}, \widetilde{V})$ represents a divisor, i.e.,* $\gcd(h, \widetilde{U}) = 1$, *then $(\widetilde{U}, \widetilde{V})$ is a representative of $((x-c)^{2k+1}, (x-c)^k\bar{V})$. This can be shown using the same approach as in Proposition 3.1.14.*

Remark 4.2.8. *In Proposition 4.2.5, the range of k can be extended to* $\mathbb{N}$. *When $k = 0$, the only pair of polynomials satisfying the given conditions is $((x-c), 0)$, which corresponds to the divisor $[(c, 0)] - [\infty]$.*

Remark 4.2.9. *In Proposition 4.2.5, if the geometric genus of C is positive, then the divisor class $((x-c)^{2k+1}, (x-c)^k\bar{V})$ does not lie in S. When $(x-c) \nmid e(x)$, there exist additional divisor classes represented by $((x-c)^{2k+t}, (x-c)^k\bar{V})$, where*

- $1 \le t \le \frac{\deg(e(x))-1}{2}$, *and* $\deg(\bar{V}) < k + t$,
- $(x-c)^t \mid \frac{f}{(x-c)^{2k}} - \bar{V}^2$, *and* $(x-c)^{t+1} \nmid \frac{f}{(x-c)^{2k}} - \bar{V}^2$.

These divisor classes, together with $((x-c)^{2l}, (x-c)^l\bar{V})$ for each $0 \le l \le k$ in S, form a subgroup of $J(C)$, where addition can be performed using Cantor composition.

When $(x-c) \mid e(x)$, the same statement holds, except that the range for t is restricted to $t = 1$.

These results extend beyond the scope of this section, we only prove part of them here.

Proposition 4.2.10. *Choose the same setting as in Proposition 4.2.5. Let $((x-c)^{2l}, (x-c)^l\bar{V}') \in S$, then the addition*

$$((x-c)^{2k+1}, (x-c)^k\bar{V}) + ((x-c)^{2l}, (x-c)^l\bar{V}')$$

can be performed using Cantor Composition.

Proof. When $k = 0$ or $l = 0$, the statement is trivial. We assume $k \ge 1$ and $0 < l \le k$. We proceed in three steps:

(1) We apply Cantor composition to the sum

$$((x-c)^{2k+1}, (x-c)^k\bar{V}) + ((x-c)^{2l}, (x-c)^l\bar{V}'),$$

obtaining the result $((x-c)^{2k+1}, (x-c)^k\bar{V}_3)$.

(2) We show that $((x-c)^{2k+1}, (x-c)^k\bar{V}_3)$ is a valid representation.

(3) We demonstrate that $((x-c)^{2l}, (x-c)^l\bar{V}') + ((x-c)^{2k+1}, (x-c)^k\bar{V}) = ((x-c)^{2k+1}, (x-c)^k\bar{V}_3)$.

Step 1. Apply Cantor composition to $((x-c)^{2k+1}, (x-c)^k\bar{V}) + ((x-c)^{2l}, (x-c)^l\bar{V}')$.

By Theorem 3.1.12, we have

$$(x-c) \nmid \frac{f}{(x-c)^{2l}} - \bar{V}'^2. \tag{4.18}$$

Furthermore, from the construction of divisor classes in Proposition 4.2.5, we obtain:

$$(x-c) \mid \frac{f}{(x-c)^{2k}} - \bar{V}^2, \text{ and } (x-c)^2 \nmid \frac{f}{(x-c)^{2k}} - \bar{V}^2. \tag{4.19}$$

We first show that the power of $(x-c)$ in $(x-c)^l\bar{V}' + (x-c)^k\bar{V}$ is precisely l. If $0 < l < k$, the claim is evident. When $l = k$, Equation (4.18) and 4.19 imply that

$$\begin{aligned} &(x-c) \nmid \frac{f}{(x-c)^{2k}} - \bar{V}^2 - (\frac{f}{(x-c)^{2k}} - \bar{V}'^2) = (\bar{V}' - \bar{V})(\bar{V}' + \bar{V}) \\ \Longrightarrow\ &(x-c) \nmid (\bar{V}' + \bar{V}), \text{ and } (x-c) \nmid (\bar{V}' - \bar{V}). \end{aligned} \tag{4.20}$$

Thus, the power of $(x-c)$ in $(x-c)^k\bar{V}' + (x-c)^k\bar{V}$ is exactly k, proving the claim.

Since l is less than both $2l$ and $2k+1$, we compute

$$d = \gcd((x-c)^{2l}, (x-c)^{2k+1}, (x-c)^l\bar{V}' + (x-c)^k\bar{V}) = (x-c)^l.$$

Thus, there exists h_1, h_3 such that

$$\begin{aligned} (x-c)^l &= (x-c)^{2l}h_1 + ((x-c)^l\bar{V}' + (x-c)^k\bar{V})h_3, \\ \text{or equivalently, } 1 &= (x-c)^l h_1 + (\bar{V}' + (x-c)^{k-l}\bar{V})h_3. \end{aligned} \tag{4.21}$$

We now compute:

$$\begin{aligned} U &= \frac{(x-c)^{2l}(x-c)^{2k+1}}{(x-c)^{2l}} = (x-c)^{2k+1}, \\ V &\equiv [h_1(x-c)^{2l}(x-c)^k\bar{V} + h_3(f + (x-c)^l\bar{V}'(x-c)^k\bar{V})]/d \\ &\equiv h_1(x-c)^{l+k}\bar{V} + h_3(\frac{f}{(x-c)^l} + (x-c)^k\bar{V}'\bar{V}) \\ &\underset{Eq(4.21)}{\equiv} (x-c)^k[\bar{V} + (x-c)^{k-l}h_3(\frac{f}{(x-c)^{2k}} - \bar{V}^2)] \pmod{(x-c)^{2k+1}}. \end{aligned}$$

Define

$$\bar{V}_3 \equiv \bar{V} + (x-c)^{k-l}h_3(\frac{f}{(x-c)^{2k}} - \bar{V}^2) \pmod{(x-c)^{k+1}} \tag{4.22}$$

with $\deg(\bar{V}_3) < k+1$.

Thus, the result of applying Cantor composition to $((x-c)^{2l},(x-c)^l\bar{V}')+((x-c)^{2k+1},(x-c)^k\bar{V})$ is given by $((x-c)^{2k+1},(x-c)^k\bar{V}_3)$.

Step 2. Show $((x-c)^{2k+1},(x-c)^k\bar{V}_3)$ is a valid representation.

It is evident that $((x-c)^{2k+1},(x-c)^k\bar{V}_3)$ satisfies condition (1) in Proposition 4.2.5. To verify it satisfies the remaining two conditions, consider

$$\begin{aligned}\frac{f}{(x-c)^{2k}}-\bar{V}_3^2 &\underset{Eq(4.22)}{\equiv} \frac{f}{(x-c)^{2k}}-(\bar{V}+(x-c)^{k-l}h_3(\frac{f}{(x-c)^{2k}}-\bar{V}^2))^2\\ &\equiv (\frac{f}{(x-c)^{2k}}-\bar{V}^2)\underbrace{[1-2(x-c)^{k-l}h_3\bar{V}-(x-c)^{2k-2l}h_3^2(\frac{f}{(x-c)^{2k}}-\bar{V}^2)]}_{①}. \pmod{(x-c)^{k+1}}\end{aligned}$$

For $l<k$, the term ① satisfies

$$① \equiv 1 \pmod{(x-c)}.$$

For $l=k$, we obtain

$$① \underset{Eq(4.19)}{\equiv} 1-2h_3\bar{V} \underset{Eq(4.21)}{\equiv} (\bar{V}'-\bar{V})h_3 \underset{Eq(4.21),(4.20)}{\not\equiv} 0 \pmod{(x-c)}.$$

Thus, the power of $(x-c)$ in $\frac{f}{(x-c)^{2k}}-\bar{V}_3^2$ is the same as in $\frac{f}{(x-c)^{2k}}-\bar{V}^2$. From Equation (4.19), we conclude that

$$(x-c)\mid\frac{f}{(x-c)^{2k}}-\bar{V}_3^2,\text{ and }(x-c)^2\nmid\frac{f}{(x-c)^{2k}}-\bar{V}_3^2.$$

Since $\bar{V}_3$ satisfies all three necessary conditions in Proposition 4.2.5, $((x-c)^{2k+1},(x-c)^k\bar{V}_3)$ represents a divisor class.

Step 3. Show $((x-c)^{2l},(x-c)^l\bar{V}')+((x-c)^{2k+1},(x-c)^k\bar{V})=((x-c)^{2k+1},(x-c)^k\bar{V}_3)$.

We choose representatives $(U_1,V_1),(U_2,V_2)$ and (U_3,V_3) for the divisor classes $((x-c)^{2l},(x-c)^l\bar{V}')$, $((x-c)^{2k+1},(x-c)^k\bar{V})$ and $((x-c)^{2k+1},(x-c)^k\bar{V}_3)$, respectively, where

$$\begin{aligned}V_1&=w_1(x-c)^{2l}-(x-c)^l\bar{V}',\ U_1=\frac{f-V_1^2}{(x-c)^{2l}},\\ V_2&=w_2(x-c)^{2k+1}-(x-c)^k\bar{V},\ U_2=\frac{f-V_2^2}{(x-c)^{2k+1}},\\ V_3&=w_3(x-c)^{2k+1}-(x-c)^k\bar{V}_3,\ U_3=\frac{f-V_3^2}{(x-c)^{2k+1}},\end{aligned}$$

for some $w_1,w_2,w_3\in\mathbf{C}[x]$. Moreover, $w_i,(i=1,2,3)$ are chosen appropriately such that $\gcd(U_i,h)=1,\ (i=1,2,3)$. This ensures that

$$V_i|_{x=c'}\neq 0,\ i=1,2,3. \tag{4.23}$$

for any singular points $(c',0)$ where $c'\neq c$. Next, we define the function

$$H:=\frac{1}{x-c}(\frac{y}{(x-c)^l}-\frac{V_1}{(x-c)^l})(\frac{y}{(x-c)^k}-\frac{V_2}{(x-c)^k})(\frac{y}{(x-c)^k}+\frac{V_3}{(x-c)^k}).$$

We claim that $\operatorname{div}(H) = (U_1, V_1) + (U_2, V_2) - (U_3, V_3)$. To prove this, we first show that H does not vanish at any singular points. For any singular points $(c', 0)$ where $c' \neq c$, we note that

$$\frac{y}{(x-c)^l}|_{(c',0)} = \frac{y}{(x-c)^k}|_{(c',0)} = 0.$$

Thus,

$$H|_{(c',0)} = \frac{1}{x-c}(-\frac{V_1}{(x-c)^l})(-\frac{V_2}{(x-c)^k})(\frac{V_3}{(x-c)^k})|_{(c',0)} \underset{Eq(4.23)}{\neq} 0.$$

To evaluate H at the singular point $(c, 0)$, we expand H as follows:

$$\begin{aligned} H &= \frac{1}{x-c}(\frac{y}{(x-c)^l} - \frac{V_1}{(x-c)^l})(\frac{f}{(x-c)^{2k}} - \frac{V_2V_3}{(x-c)^{2k}} + \frac{y}{(x-c)^{2k}}(V_3 - V_2)) \\ &= \frac{1}{(x-c)^{2k+l+1}} \underbrace{(f(V_3 - V_2) - V_1(f - V_2V_3))}_{①} + \frac{y}{(x-c)^{2k+l+1}} \underbrace{(f - V_2V_3 - V_1(V_3 - V_2))}_{②}. \end{aligned}$$

By construction of V_1, V_2 and V_3, we compute

$$\begin{aligned} ① &\equiv f(-(x-c)^k(\bar{V}_3 - \bar{V})) - (w_1(x-c)^{2l} - (x-c)^l\bar{V}')(f - (x-c)^{2k}\bar{V}\bar{V}_3) \\ &\underset{Eq(4.22),(4.21),(4.19)}{\equiv} -(x-c)^{2k+l}(\frac{f}{(x-c)^{2k}} - \bar{V}^2)(\frac{f}{(x-c)^{2l}} - \bar{V}'^2))h_3. \quad (\mathrm{mod}\ (x-c)^{2k+l+2}) \end{aligned}$$

Hence, we get

$$\frac{①}{(x-c)^{2k+l+1}}|_{(c,0)} = -\frac{1}{x-c}(\frac{f}{(x-c)^{2k}} - \bar{V}^2)(\frac{f}{(x-c)^{2l}} - \bar{V}'^2))h_3|_{(c,0)} \underset{Eq(4.18),(4.19),(4.21)}{\neq} 0.$$

Additionally, using the definition of V_1, V_2 and V_3, we obtain

$$\begin{aligned} ② &\equiv f - (x-c)^{2k}\bar{V}\bar{V}_3 + (w_1(x-c)^{2l} - (x-c)^l\bar{V}')(x-c)^k(\bar{V}_3 - \bar{V}) \\ &\underset{Eq(4.22),(4.19)}{\equiv} (x-c)^{2k}(\frac{f}{(x-c)^{2k}} - \bar{V}^2)[1 - (\bar{V}' + (x-c)^{k-l}\bar{V})h_3] \\ &\underset{Eq(4.21)}{\equiv} (x-c)^{2k}(\frac{f}{(x-c)^{2k}} - \bar{V}^2)(x-c)^l h_1 \\ &\underset{Eq(4.19)}{\equiv} 0. \quad (\mathrm{mod}\ (x-c)^{2k+l+1}) \end{aligned}$$

Therefore, $y \cdot \frac{②}{(x-c)^{2k+l+1}}|_{(c,0)} = y(\cdots)|_{(c,0)} = 0$, implying $H(c, 0) = \frac{①}{(x-c)^{2k+l+1}}|_{(c,0)} \neq 0$.

Furthermore, we observe that

$$\frac{y}{(x-c)^l} - \frac{V_1}{(x-c)^l} = 0 \Longleftrightarrow \begin{cases} y = V_1(x), \\ \frac{y^2}{(x-c)^{2l}} - \frac{V_1^2}{(x-c)^{2l}} = U_1 = 0. \end{cases}$$

$$\frac{y}{(x-c)^k} - \frac{V_2}{(x-c)^k} = 0 \Longleftrightarrow \begin{cases} y = V_2(x), \\ \frac{y^2}{(x-c)^{2k}} - \frac{V_2^2}{(x-c)^{2k}} = U_2 \cdot (x-c) = 0. \end{cases}$$

$$\frac{y}{(x-c)^k} + \frac{V_3}{(x-c)^k} = 0 \Longleftrightarrow \begin{cases} y = -V_3(x), \\ \frac{y^2}{(x-c)^{2k}} - \frac{V_3^2}{(x-c)^{2k}} = U_3 \cdot (x-c) = 0. \end{cases}$$

Since H does not vanish at singular points, the zeros of H are precisely the points in $(U_1, V_1) + (U_2, V_2) - (U_3, V_3)$. It follows that

$$\operatorname{div}(H) = (U_1, V_1) + (U_2, V_2) - (U_3, V_3).$$

Thus, $(U_1, V_1) + (U_2, V_2) = (U_3, V_3)$, proving that the addition of (U_1, V_1) and (U_2, V_2) can be done via Cantor composition. □

We now obtain additional divisor classes with a generalized Mumford representation in $J(C)$. Suppose the exact sequence (4.10) splits, so that there exists a morphism from $J(C)$ to $\ker(\Phi) \cong \mathbf{C}^*$. In the following two lemmas, we derive the images of these divisor classes. This will lead to a contradiction regarding the existence of such a morphism in Theorem 4.2.13.

Lemma 4.2.11. *Let $C : y^2 = x^2 e(x)$ be a singular hyperelliptic curve, where $x \nmid e(x)$ and $e(x)$ has no repeated roots. Then, for any $\beta_1 \neq \beta_2$, we have*

$$(x^3, \beta_1 x^2 - \gamma x) + (x^3, -\beta_2 x^2 + \gamma x) = (x^2, \frac{(\beta_1 + \beta_2)\gamma + s}{\beta_1 - \beta_2} x),$$

where γ is a square root of $e(0)$, and s is the coefficient of the linear term in $e(x)$.

Proof. By Proposition 4.2.10, applying Cantor composition yields

$$(x^3, \beta_1 x^2 - \gamma x) + (x^2, \alpha x) = (x^3, \frac{s + (\alpha + \gamma)\beta_1}{\alpha - \gamma} x^2 - \gamma x). \tag{4.24}$$

We set

$$\beta_2 = \frac{s + (\alpha + \gamma)\beta_1}{\alpha - \gamma} \Longleftrightarrow \alpha = \frac{s + (\beta_1 + \beta_2)\gamma}{\beta_2 - \beta_1}.$$

Substituting these relations into Equation (4.24), the statement follows. □

Lemma 4.2.12. *Let $C : y^2 = x^2 e(x)$ be a singular hyperelliptic curve, where $x \nmid e(x)$ and $e(x)$ has no repeated roots. Let γ be a square root of $e(0)$, and let s be the coefficient of the linear term in $e(x)$. Suppose there exists a group homomorphism $\phi : J(C) \longrightarrow \mathbf{C}^*$ satisfying*

$$\phi((x^2, \alpha x)) = \frac{\alpha + \gamma}{\alpha - \gamma}, \quad \forall \alpha \neq \pm\gamma.$$

Then we also have:

$$\phi((x^3, \beta x^2 - \gamma x)) = K(s + 2\gamma\beta), \quad \forall \beta \neq \frac{-s}{2\gamma}$$
$$\phi((x^3, \beta x^2 + \gamma x)) = \frac{1}{K(s - 2\gamma\beta)}, \quad \forall \beta \neq \frac{s}{2\gamma}$$

for some $K \in \mathbf{C}^*$.

Proof. By Theorem 4.2.5, the divisor classes $(x^3, \beta x^2 \pm \gamma x)$ $(s \mp 2\beta\gamma \neq 0)$ exist $J(C)$. Applying Lemma 4.2.11, we obtain

$$(x^3, \beta_1 x^2 - \gamma x) + (x^3, -\beta_2 x^2 + \gamma x) = (x^2, \frac{(\beta_1 + \beta_2)\gamma + s}{\beta_1 - \beta_2} x), \forall \beta_1 \neq \beta_2.$$

Define $\phi_\pm(\beta) := \phi((x^3, \beta x^2 \pm \gamma x))$. Then

$$\phi_-(\beta_1) \cdot \phi_+(-\beta_2) = \frac{s + 2\gamma\beta_1}{s + 2\gamma\beta_2}, \forall \beta_1 \neq \beta_2.$$

Fix any value of β_1 (resp. β_2), it follows that ϕ_+ (resp. ϕ_-) must have the form

$$\phi_+(\beta) = \frac{1}{K(s - 2\gamma\beta)}, \ \phi_-(\beta) = K(s + 2\gamma\beta), \tag{4.25}$$

for some $K \in \mathbf{C}^*$, completing the proof. □

Theorem 4.2.13. *Let $C : y^2 = x^2e(x)$ be a singular hyperelliptic curve, where $e(x)$ has no repeated roots and $\deg(e(x)) = 2g - 1 \geq 3$. Let $C' : y^2 = e(x)$ be its normalization, and let Φ denote the normalization map from $J(C)$ to $J(C')$. If $e(x)$ satisfies*

$$x \nmid e(x), \ \textit{and} \gcd(e(x), sx + 2e(0)) = 1,$$

where s is the coefficient of the linear term in $e(x)$, then the following exact sequence does not split as a sequence of group schemes:

$$0 \longrightarrow \ker(\Phi) \xrightarrow{i} J(C) \xrightarrow{\Phi} J(C') \longrightarrow 0.$$

Proof. Let γ be a square root of $e(0)$. According to Theorem 4.1.1 and Corollary 4.1.3, we have

$$\ker(\Phi) = \{(x^2, \alpha x) | \alpha \neq \pm\gamma\} \cup \{(1, 0)\} \cong \mathbf{C}^*.$$

Applying Cantor composition, we get

$$(x^2, \alpha_1 x) + (x^2, \alpha_2 x) = (x^2, \frac{\gamma^2 + \alpha_1\alpha_2}{\alpha_1 + \alpha_2}x), \forall \alpha_1 \neq -\alpha_2.$$

Given the addition above, it is obvious that the map

$$\theta : \ker(\Phi) \longrightarrow \mathbf{C}^*, (x^2, \alpha x) \mapsto \frac{\alpha + \gamma}{\alpha - \gamma}, (1, 0) \mapsto 1.$$

is an isomorphism between $\ker(\Phi)$ and $\mathbf{C}^*$.

Assume the exact sequence splits, then there exists $\phi : J(C) \longrightarrow \ker(\Phi)$ with $\phi \circ i = id_{\ker(\Phi)}$. Composing θ with ϕ, there exists:

$$\psi : J(C) \longrightarrow \mathbf{C}^*, \text{ where } (x^2, \alpha x) \mapsto \frac{\alpha + \gamma}{\alpha - \gamma}, \forall \alpha \neq \pm\gamma.$$

By Lemma 4.2.12, we also have

$$\psi((x^3, \beta x^2 + \gamma x)) = \frac{1}{K(s - 2\gamma\beta)}, \ \forall \beta \neq \frac{s}{2\gamma} \tag{4.26}$$

for some $K \in \mathbf{C}^*$.

We choose a representative (U, V) of $(x^3, \beta x^2 + \gamma x)$ (see Remark 4.2.7), where

$$U = \frac{e(x) - (\beta x + \gamma)^2}{x} = \sum_{j=1}^{2g-2}(x - x_j), \ V = -\beta x^2 - \gamma x.$$

Then, for any $\beta \neq \frac{s}{2\gamma}$, the product of the images of $[(x_j, V(x_j))] - [\infty]$ $(1 \leq j \leq 2g - 2)$ should be equal to the image of $(x^3, \beta x^2 + \gamma x)$. Restricting ψ to divisors of the form $[(x, y)] - [\infty]$, ψ is a bivariate function in x and y. And $\psi \in \mathbb{C}[x, y, \frac{1}{x}]/(y^2 = f(x))$ as it is a regular function between affine varieties. Since $\psi(x, y) \cdot \psi(x, -y) = 1$ and $\psi \in \mathbb{C}(x, y)$, we have

$$\psi(x, y) = \frac{g_1(x)y + g_2(x)}{g_1(x)y - g_2(x)},$$

for some polynomial $g_1, g_2 \in \mathbb{C}[x]$ with $\gcd(g_1, g_2) = 1$. Under this condition, $g_1(x)y + g_2(x) = g_1(x)y - g_2(x) = 0$ if and only if $y = g_2(x) = 0$. Thus, for any nonsingular point (x, y) with $y \neq 0$, we must have $g_1(x)y + g_2(x) \neq 0$ and $g_1(x)y - g_2(x) \neq 0$, otherwise $\psi(x, y)$ could be 0 or ∞. This implies that $g_1(x)y + g_2(x)$ and $g_1(x)y - g_2(x)$ only vanish at points where the y-coordinate is zero, leading to

$$(g_1(x)y + g_2(x))(g_1(x)y - g_2(x)) = g_1^2(x)x^2e(x) - g_2^2(x) = x^{k_0} \prod_l (x - c_l)^{k_l}, \tag{4.27}$$

for some $k_0, k_l \in \mathbb{N}$, where $(x - c_l) \mid e(x)$, $\forall l$. Let

$$z_1 := \prod_{j=1}^{2g-2} (g_1(x_j)(-\beta x_j^2 - \gamma x_j) + g_2(x_j)),$$
$$z_2 := \prod_{j=1}^{2g-2} (g_1(x_j)(-\beta x_j^2 - \gamma x_j) - g_2(x_j)).$$

Since both z_1 and z_2 are symmetric functions of x_j, $(1 \leq j \leq 2g - 2)$, whose elementary functions are functions of β, z_1, z_2 are functions of β. Then,

$$\psi((x^3, \beta x^2 + \gamma x)) = \prod_{j=1}^{2g-2} \psi(x_j, V(x_j)) = \frac{z_1(\beta)}{z_2(\beta)}. \tag{4.28}$$

Multiplying the numerator and denominator by $z_1(\beta)$ and substituting Equation (4.27), we obtain

$$\psi((x^3, \beta x^2 + \gamma x)) = \frac{z_1(\beta)^2}{\prod_{j=1}^{2g-2} x_j^{k_0} \cdot \prod_l \prod_{j=1}^{2g-2} (x_j - c_l)^{k_l}} = \frac{z_1(\beta)^2}{(s - 2\gamma\beta)^{k_0} \cdot \prod_l U(c_l)^{k_l}}.$$

Using Equation (4.26), 4.28 and $e(x)|_{x=c_l} = 0$, we derive

$$z_1(\beta) = K'(s - 2\gamma\beta)^{\frac{k_0-1}{2}} \prod_l (c_l\beta + \gamma)^{k_l}, \tag{4.29}$$
$$z_2(\beta) = KK'(s - 2\gamma\beta)^{\frac{k_0+1}{2}} \prod_l (c_l\beta + \gamma)^{k_l}, \tag{4.30}$$

for some $K' \in \mathbb{C}^*$. The above equations require k_0 to be odd. Considering Equation (4.27), k_0 being odd implies $x \mid g_2(x)$, $x^2 \nmid g_2(x)$ and $g_1(0)^2\gamma^2 - g'(0)^2 = 0$, where $g'(x) = \frac{g_2(x)}{x}$.

Suppose $g_1(0)\gamma + g_2'(0) = 0$. We claim that $(s - 2\gamma\beta) \mid z_1(\beta)$, $(s - 2\gamma\beta)^2 \nmid z_1(\beta)$ and $(s - 2\gamma\beta)^2 \mid z_2(\beta)$. Define

$$r_1(x) := g_1(x)(-\beta x^2 - \gamma x) + g_2(x),$$
$$r_2(x) := g_1(x)(-\beta x^2 - \gamma x) - g_2(x).$$

In this case, $x^2 \mid r_2$. Thus,

$$(s - 2\gamma\beta)^2 = (\prod_{j=1}^{2g-2} x_j)^2 \mid \prod_{j=1}^{2g-2} r_2(x_j) = z_2(\beta).$$

Similarly, as $x \mid r_1$, we conclude that $(s-2\gamma\beta) \mid r_1$. Rewriting

$$\frac{r_1(x)}{x} = g_1(x)(\frac{s}{2\gamma} - \beta)x - ((\frac{s}{2\gamma}x + \gamma)g_1(x) - g_2'(x)).$$

And write

$$(\frac{s}{2\gamma}x + \gamma)g_1(x) - g_2'(x) = \prod_{i=1}^{n}(x - a_i), \text{ for some } a_i \in \mathbf{C}^*, \ \forall i. \tag{4.31}$$

As $g_1(0)\gamma - g_2'(0) \neq 0$, none of a_i equals to 0. Additionally, $g_1(a_i) \neq 0, \forall i$. Otherwise, there exists $g'(a_i) = 0$, contradicts with $\gcd(g_1, g_2) = 1$.

Using this, we compute

$$\begin{aligned}\prod_{j=1}^{2g-2}\frac{r_1(x_j)}{x_j} &= \prod_{j=1}^{2g-2}(g_1(x_j)(\frac{s}{2\gamma} - \beta)x_j - ((\frac{s}{2\gamma}x_j + \gamma)g_1(x_j) - g_2'(x_j))) \\ &= (\frac{s}{2\gamma} - \beta)(\cdots) + \prod_{j=1}^{2g-2}((\frac{s}{2\gamma}x_j + \gamma)g_1(x_j) - g_2'(x_j)) \\ &= (\frac{s}{2\gamma} - \beta)(\cdots) + \prod_{j=1}^{2g-2}\prod_{i=1}^{n}(x_j - a_i) \\ &= (\frac{s}{2\gamma} - \beta)(\cdots) + \prod_{i=1}^{n}U(a_i).\end{aligned}$$

As $z_1(\beta) = \prod_{j=1}^{2g-2}x_j \cdot \prod_{j=1}^{2g-2}\frac{r_1(x_j)}{x_j} = (\frac{s}{2\gamma} - \beta)^2(\cdots) + (\frac{s}{2\gamma} - \beta)\prod_{i=1}^{n}U(a_i)$, to show $(s-2\gamma\beta)^2 \nmid z_1(\beta)$ is equivalent to show $(s-2\gamma\beta) \nmid \prod_{i=1}^{n}U(a_i)$, i.e., $(s-\gamma\beta) \nmid U(a_i)$, $\forall 1 \leq i \leq n$. Note that

$$(s-2\gamma\beta) \mid U(a_i) = e(a_i) - (a_i\beta + \gamma)^2. \Longleftrightarrow e(a_i) - (a_i\frac{s}{2\gamma} + \gamma)^2 = 0.$$

$$\underset{Eq(4.31)}{\Longleftrightarrow} e(a_i) - (\frac{g_2'(a_i)}{g_1(a_i)})^2 = 0. \underset{g_1(a_i)\neq 0}{\Longleftrightarrow} g_1(a_i)^2 e(a_i) - g_2'(a_i)^2 = 0.$$

$$\underset{Eq(4.27), a_i \neq 0}{\Longleftrightarrow} a_i = c_l, \text{ for some } l, \text{ where } (x - c_l) \mid e(x), g_2'(x).$$

This means that if there exists $1 \leq i \leq n$ such that $(s-2\gamma\beta) \mid U(a_i)$, we have $g_2'(a_i) = e(a_i) = 0$. While from $\gcd(g_1(x), g_2(x)) = 1$, we know $g_1(a_i) \neq 0$. Then considering Equation (4.31), we must have $\frac{s}{2\gamma}a_i + \gamma = 0$. However, our assumption $\gcd(e(x), sx + 2\gamma^2) = 1$ contradicts with the existence of such a_i. Therefore, $(s-2\gamma\beta)^2 \nmid z_1(\beta)$. Our claim holds.

For another case where $g_1(0)\gamma - g_2'(0) = 0$. Using the same approach as above, we obtain $(s-2\gamma\beta)^2 \mid z_1(\beta)$, $(s-2\gamma\beta) \mid z_2(\beta)$ and $(s-2\gamma\beta)^2 \nmid z_2(\beta)$.

Combining these results with Equation (4.29) and 4.30, we must have $g_1(0)\gamma + g_2'(0) = 0$, and accordingly, $1 = \frac{k_0 - 1}{2}$, i.e., $k_0 = 3$.

Moreover, take $(c_l, 0)$ with $(x - c_l) \mid e(x)$, it is easy to calculate

$$\psi(c_l, 0) = \begin{cases} 1, & \text{if } (x - c_l) \mid g_2(x), \\ -1, & \text{if } (x - c_l) \nmid g_2(x). \end{cases}$$

Write $e(x) = \prod_{d=1}^{2g-1}(x - c_d)$, as $\sum_{d=1}^{2g-1}([(c_d, 0)] - [\infty])$ is a representative of $((x-c)^2, 0)$, whose image under ψ is -1. This implies that the number of indices l for which $(x - c_l) \mid g_2(x), e(x)$ must be even, denoted by $2t$. Furthermore, we observe that $k_l = 1, \forall l$, since the power of $(x - c_l)$ in $g_1(x)e(x)$ is 1, while in $g_2(x)^2$, it is at least 2. Hence the degree of right-hand side of Equation (4.27) is odd, combining these:

$$3 + 2t = 2\deg(g_1) + 2g + 1 > 2\deg(g_2) \geq 2(2t + 1).$$

This leads to $t = 0$, which further implies $g = 1$. However, this contradicts with our assumption that the geometric genus of C is positive. Therefore, there does not exist $\phi : J(C) \to \ker(\Phi)$ such that $\phi \circ i = id_{\ker(\Phi)}$, implying that the exact sequence does not split as group schemes. □

Remark 4.2.14. *If we allow $g = 1$ in Proposition 4.2.13, then the condition $\gcd(e(x), sx + 2e(0)) = 1$ holds automatically. In this case, we obtain $\deg(g_1) = 0$, $\deg(g_2) = 1$, and furthermore, $g_2 = -\gamma x$. This coincides with the map given in Theorem 3.3.2. Our proof thus shows that, for an elliptic nodal curve, the map described in Theorem 3.3.2 is the unique isomorphism of group schemes between its Jacobian and $\mathbf{C}^*$.*

Remark 4.2.15. *Let $e(x) = \prod_{j=1}^{n}(x - x_j) \in \mathbf{C}[x]$ with $e(0) \neq 0$. Denote by s the coefficient of the linear term in $e(x)$. Then, the following equivalence holds:*

$$\gcd(e(x), sx + 2e(0)) \neq 1. \iff \exists j : 2\frac{1}{x_j} = \sum_{j=1}^{n} \frac{1}{x_j}.$$

This provides an alternative way to verify the condition.

Using Proposition 4.2.1, we can extend the results of Theorem 4.2.3 and Theorem 4.2.13 to a broader class of curves, as stated in the following theorem.

Theorem 4.2.16. *Let $C : y^2 = f(x) = h^2(x)e(x)$ be a singular hyperelliptic curve, where $e(x)$ has no repeated roots and $\deg(f(x)) = 2g + 1 > deg(e(x)) \geq 3$. Let $C' : y^2 = e(x)$ be its normalization, and let Φ denote the normalization map. If $h(x)$ and $e(x)$ satisfy one of the following conditions:*
(1) $\gcd(h(x), e(x)) \neq 1$, or
(2) $\gcd(h(x), e(x)) = 1$, and there exists $(x - c) \mid h(x)$ such that

$$\gcd(e(x), s(x - c) + 2e(c)) = 1,$$

where $s := \left.\frac{e(x)-e(c)}{x-c}\right|_{x=c}$, then the following exact sequence does not split as a sequence of group schemes:

$$0 \to \ker(\Phi) \xrightarrow{i} J(C) \xrightarrow{\Phi} J(C') \to 0.$$

Proof. If $\gcd(h(x), e(x)) \neq 1$, we choose a factor $(x - c)$ such that $(x - c)$ divides both $h(x)$ and $e(x)$. In either cases, we can assume without loss of generality that $c = 0$ through a linear transformation. Consequently, the gcd condition in the second case simplifies to $\gcd(e(x), sx + 2e(0)) = 1$. We define C'' as the singular curve given by

$$y^2 = x^2 e(x),$$

and let $\Phi' : J(C'') \to J(C')$ denote the partial normalization map (defined in Definition 3.2.1). Then Φ can be factored as the composition of Φ' and the partial normalization map from $J(C)$ to $J(C'')$.

According to Theorem 4.2.3 and Theorem 4.2.13, the exact sequence associated with Φ' doe not split in both cases. Thus, by Proposition 4.2.1, the exact sequence associated with Φ does not split either. □

Bibliography

[BLR12] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron Models*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer Berlin Heidelberg, 2012. ISBN: 9783642514388.

[CNO22] S. Caglar, K. Nari, and E. Ozdemir. "An Application of Nodal Curves". In: *arXiv preprint arXiv:2206.06261* (2022).

[Can87] D. G. Cantor. "Computing in the Jacobian of a hyperelliptic curve". In: *Mathematics of Computation* 48 (1987), pp. 95–101.

[Gal12] S. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. ISBN: 9781107013926.

[Koh12] D. R. Kohel. "Constructive and destructive facets of torus-based cryptography". In: 2012.

[Mea92] D. G. Mead. "Newton's Identities". In: *The American Mathematical Monthly* 99.8 (1992), pp. 749–751. ISSN: 00029890, 19300972.

[Mum82] D. B. Mumford. *Tata Lectures on Theta II, Birhauser.* 1982.

[Ozd09] E. Ozdemir. *Curves and their applications to factoring polynomials.* University of Maryland, College Park, 2009.

[Sil09] J. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946.

[Was08] L. C. Washington. *Elliptic curves: number theory and cryptography.* Chapman and Hall/CRC, 2008.