博 士 論 文

# Torsion points on Jacobian varieties and $p$-adic Sato theory

(ヤコビ多様体のねじれ元と $p$-進佐藤理論)

宮坂 宥憲

平成 23 年

# Torsion points on Jacobian varieties and $p$-adic Sato theory

A thesis presented

by

Yuken MIYASAKA

to

The Mathematical Institute

for the degree of

Doctor of Science

Tohoku University

Sendai, Japan

March 2012

# Acknowledgements

I would like to express my sincere gratitude to my advisor, Professor Takao Yamazaki for his invaluable advice and continuous encouragement. Without them, this thesis would never have been completed.

I would like to thank Professor Akihiko Yukie and Professor Nobuo Tsuzuki for their important suggestions and helpful comments on this thesis.

A part of this thesis consists of a joint work with Professor Takao Yamazaki. I would like to express my appreciation to him for fruitful discussions and encouragement through the joint work.

I am thankful to Noriyuki Otsubo for his insightful comments. In particular, the remark in §3.1.8 is suggested by him. I am also deeply grateful to Takeshi Ikeda for stimulating discussion. I learned the importance of the equation of the form (3.2.1) from him.

I am greatly indebted to my collaborator Kensaku Kinjo for his helpful discussions and useful comments. I am very glad for writing two papers with him through my doctoral course.

I wish to express my thanks to Doctors Toru Kan and Ryo Takada for their friendships and various supports throughout our undergraduate, master's and doctoral courses. My appreciation also goes to all members of the Number Theory Seminar at Tohoku University for their constant encouragement.

This work was partly supported by JSPS Research Fellowships for Young Scientists.

Finally I would like to express my heartily thanks to my parents and family for their constant support and warm encouragement throughout my study.

# Contents

# Chapter 1

# Introduction

The aim of the present thesis is to apply the $p$-*adic Sato theory* to arithmetic geometry. Classically, the Sato theory describes solutions of complete integrable equations including the KP equation and hierarchy in the complex analytic setting by using *Sato tau-functions*. Anderson developed a $p$-adic analogous theory of Sato tau-function, and proved that torsion points of certain prime orders are not on a theta divisor in the Jacobian variety of a cyclic quotient of a Fermat curve of prime degree. In this thesis, we apply Anderson's $p$-adic theory of Sato tau-function to a hyperelliptic curve given by the equation:

$$y^2 = x^{2g+1} + x$$

with $g \geq 2$, and prove analogous results.

## 1. Torsion points on Jacobian varieties

The problem of finding torsion points on a subvariety of a Jacobian variety comes from the following celebrated result of Raynaud [26]:

> Let $K$ be a field of characteristic zero, $A$ an abelian variety over $K$ and $Z$ a closed subvariety of $A$. Then the Zariski closure of the intersection of $Z$ with the set of torsion points $A_{\mathrm{tor}}$ on $A$ is contained in a finite union of translates of subabelian varieties of $A$ by torsion points.

In particular, Raynaud's theorem implies that the intersection of $Z$ $(\neq A)$ with $A_{\mathrm{tor}}$ is a finite set, if either $Z$ is a curve of genus at least two, or if $A$ is absolutely simple. However, it is usually not easy to determine this finite set $Z \cap A_{\mathrm{tor}}$ explicitly for given $A$ and $Z$.

Now let us assume $A = J$ is the Jacobian variety of a smooth projective geometrically connected curve $X$ of genus $g \geq 2$. Of particular interest is the case where $Z = X$ is the Abel-Jacobi embedded image of $X$ with respect to some base point. (Raynaud's theorem in this case was proved by himself a little earlier.) Since Coleman [7] started a research on determining the set $X \cap J_{\mathrm{tor}}$ explicitly when $X$ is some Fermat curve, many works have been done in this direction. Let us state some results about these works:

- Poonen [25] described an algorithm for determining the set $X \cap J_{\mathrm{tor}}$ explicitly when $X/\mathbb{Q}$ is the Abel-Jacobi embedded image of a genus 2 curve $X$ with respect to a Weierstrass point as a base point.

- Coleman-Tamagawa-Tzermias [8] studied the Fermat curve $X : x^n + y^n + z^n = 0$ with $n \geq 4$. Let $T$ be the set of closed points satisfying $xyz = 0$. Fix $c \in T$ and the Abel-Jacobi embedding of $X$ with respect to $c$. Then they proved that the finite set $X \cap J_{\mathrm{tor}}$ is precisely the set $T$.

- Let $p$ be a prime number $\geq 23$ and $X := X_0(p)$ be the modular curve. Let $H$ be the set of hyperelliptic branch points on $X$ when $X$ is hyperelliptic and $p \neq 37$, and otherwise let $H$ the empty set. Then Coleman-Kaskel-Ribet [9] conjectured that if $X$ is the Abel-Jacobi embedded image with respect to the cusp $\infty \in X$, then the finite set $X \cap J_{\mathrm{tor}}$ coincides with the set $\{0, \infty\} \cup H$. Baker [4] and Tamagawa [32] independently gave a proof of this conjecture.

See [33] for a lucid survey on this subject, and also see [5] on Coleman-Kaskel-Ribet's conjecture.

Anderson [2] considered the case where $Z = \Theta$ is the theta divisor of $J$. He proved that torsion points of certain prime orders are not on $\Theta$ when $X$ is a cyclic quotient of a Fermat curve of prime degree. For details of this result and its generalization by Grant [11], see Remark 1.0.3 below. In order to prove his result, Anderson developed a $p$-adic analogue of the theory of *tau-function*, which was originally introduced by Sato [27, 28] (see also [29]) in his study of soliton equations (in the complex analytic setting). In this thesis, we apply Anderson's theory to other curves and prove analogous results.

## 2. Main theorems

Let us state our main results. Fix an integer $g \geq 2$. Let $K$ be a field of characteristic zero that contains a primitive $4g$-th root $\zeta$ of unity. We consider a hyperelliptic curve $X$ of genus $g$ over $K$ defined by the equation

$$y^2 = x^{2g+1} + x. \tag{1.0.1}$$

Let $\infty$ be the $K$-rational point at which the functions $x$ and $y$ have poles. There is an automorphism $r$ of $X$ defined by $r(x, y) = (\zeta^2 x, \zeta y)$. Let $G := \langle r \rangle$ be the subgroup of $\mathrm{Aut}(X)$ generated by $r$, which is a cyclic group of order $4g$. The Jacobian variety $J$ of $X$ will be considered as a $\mathbb{Z}[G]$-module by the induced action of $G$. (We will see in §3.1.8 that $J$ is absolutely simple when $g > 45$.) We define the theta divisor $\Theta$ to be the set of $\mathscr{L} \in J$ such that $H^0(X, \mathscr{L}((g-1)\infty)) \neq \{0\}$.

Let $p$ be a prime number such that $p \equiv 1 \mod 4g$, and choose a prime ideal $\wp \subset \mathbb{Z}[\zeta]$ lying above $p$. We write $\chi$ for the composition of

$$G \to \mathbb{Z}[\zeta]^* \twoheadrightarrow (\mathbb{Z}[\zeta]/\wp)^* = \mathbb{F}_p^*$$

where the first map is defined by $r \mapsto \zeta$. We will show in Lemma 3.2.1 below that, for $i = 0, 1, \cdots, 4g-1$, we have

$$\dim_{\mathbb{F}_p} J[p]^{\chi^i} = \begin{cases} 0 & (i: \text{ even}) \\ 1 & (i: \text{ odd}), \end{cases}$$

where $J[p]^{\chi^i} = \{\mathscr{L} \in J[p] \mid r^*\mathscr{L} = \chi^i(r)\mathscr{L}\}$. Our main results are the following, which was obtained in a joint work with Professor Takao Yamazaki (Tohoku University) [20]:

**Theorem 1.0.1.** *If $i \in \{1, 3, \cdots, 4g-1\}$ is relatively prime to $4g$, then we have*

$$(J[p]^{\chi^i} + J[2]) \cap \Theta \subseteq J[2].$$

**Theorem 1.0.2.** *Assume that $K$ is a finite extension of $\mathbb{Q}_p$. Let $Q \in X(K)$ and put $\mathscr{L}_Q := \mathscr{O}_X(Q - \infty)$. Assume that the coordinates $x(Q)$ and $y(Q)$ of $Q$ belong to the integer ring of $K$. If $i \in \{1, 3, \cdots, 4g-1\}$ is relatively prime to $4g$, then we have*

$$(J[p]^{\chi^i} + \mathscr{L}_Q) \cap \Theta = \{\mathscr{L}_Q\}.$$

Note that the set $\Theta \cap J_{\mathrm{tor}}$ is explicitly determined when $g = 2$ by Boxall-Grant [6]. It consists of twenty-two points (over an algebraically closed field).

**Remark 1.0.3.** For the sake of comparison, we state Anderson's result. Fix an odd prime number $l$, integers $a \geq b > 1$ such that $l + 1 = a + b$, and a primitive $l$-th root $\zeta_l$ of unity. Let $X$ be the smooth projective curve defined by

$$y^l = x^a(1-x)^b, \tag{1.0.2}$$

and define $J$ and $\Theta$ similarly as above. (By Koblitz-Rohrlich [15], $J$ is absolutely simple.) There is an automorphism $\gamma$ of $X$ defined by $\gamma(x, y) = (x, \zeta_l y)$, which induces a $\mathbb{Z}[\zeta_l]$-module structure on $J$. For an ideal $\mathfrak{a}$ of $\mathbb{Z}[\zeta_l]$, we write $J[\mathfrak{a}]$ for the $\mathfrak{a}$-torsion subgroup of $J$. Let $p$ be a prime number such that $p \equiv 1 \mod l$ and take a prime ideal $\wp$ over $p$. Anderson's result is the following:

**Theorem 1.0.4** (Anderson)**.**

$$(J[\wp] + J[(1-\zeta_l)]) \cap \Theta \subseteq J[(1-\zeta_l)].$$

Grant [11] improved Anderson's result by showing for all $n \geq 1$

$$(J[\wp^n] + J[(1-\zeta_l)]) \cap \Theta \subseteq J[(1-\zeta_l)]$$

under the assumption that $X$ is hyperelliptic (that happens if and only if $a \in \{2, (l+1)/2, l-1\}$).

## 3. Tau-function as solutions of KP hierarchy

The Korteweg-de Vries (KdV) equation is a non-linear partial differential equation defined by

$$4u_t - 12uu_x - u_{xxx} = 0,$$

where $u = u(t, x)$ (which models a water wave of shallow canals), and the Kadomtsev-Petviashvili (KP) equation is the two-dimensional KdV equation defined by

$$(4u_t - 12uu_x - u_{xxx})_x - 3u_{yy} = 0$$

where $u = u(t, x, y)$. In 1970's, Lax [17, 18] provided that the KdV and KP equations are obtained by the first equation of the KdV and KP hierarchies which are certain compatible systems of non-linear partial differential equations. In Hirota's method ([12, 13]), these equations are translated to bilinear forms. For example, the KP equation is

$$(4D_xD_t - D_x^4 - 3D_y^2)\tau \cdot \tau = 0$$

by translating $u = (\log \tau)_{xx}$ and using Hirota's differential operators $D_\bullet$. The function $\tau$ is called the *Sato tau-function*, which is the master function expressing solutions of the KP hierarchy.

The KdV and KP equations have a strong connection with algebraic curves. For example, there is a classical fact that the Weierstrass $\wp$-function of an elliptic curve over $\mathbb{C}$ gives rise to a solution of the KdV equation. In general, the theta-functions of a compact Riemann surface over $\mathbb{C}$ have a relation with the Sato tau-functions (see, §2.3). These equations are also related with the Schottky problem. The Novikov conjecture is to characterize Jacobian varieties among principal polarized complex abelian varieties in terms of the KP equation and theta functions, which was solved by Shiota [31]. Recently, a non-archimedean version of the Novikov conjecture is formalized and proved in terms of $p$-adic theta-functions of Mumford curves by Ichikawa [14].

For more details, we refer the readers to [1] for a historical survey on the KdV and KP hierarchies, [24] for an elementary introduction on Sato theory, and also see Sato's original papers [27, 28].

## 4. Organization

The present thesis is organized as follows. Chapter 2 is devoted to study mainly the *Sato Grassmannian* and *tau-functions*. The Jacobian variety of a smooth projective curve over a field are translated in terms of the Sato Grassmannian by using *Krichever pairs*. There are the analytic part of the Sato Grassmannian on which a certain huge group (*loop group*) acts. The tau-function is defined by using this action of the loop group on the Sato Grassmannian. Points on the theta divisor of the Jacobian variety correspond to points of the Sato Grassmannian on the zero locus of the tau-function by the Krichever pair. In Section 2 of this chapter, we consider the $p$-adic analytic part of the Sato Grassmannian, which is introduced by Anderson. We are going to analyze the $p$-adic tau-functions by the use of its expansion theorem that the tau-function can be written as an infinite linear combination of Schur functions and Plücker coordinates, and prove the key property that a certain special loop (*Dwork loop*) gives a non-vanishing point on the $p$-adic tau-function under some assumptions. These results, which were proved by An-

derson, are also crucial in the proof of our main theorems. In Section 3 of this chapter, we deal with the complex analytic part of the Sato Grassmannian. In this case, the tau-functions have a close relation with the *theta-functions* of a compact Riemann surface over the complex number field. The observation of such a property of the tau-functions does not relate with our proof of the main theorems in this thesis. However a $p$-adic analogue of this theory leaves as a problem to be considered.

In Chapter 3, the main theorems and Anderson's result are proved. In Section 1 of this chapter, we study geometry of the hyperelliptic curve (1.0.1). The proof of Theorems 1.0.1 and 1.0.2 is completed in Section 2. The important fact for the proof is that the Dwork loop has a non-vanishing property on the $p$-adic tau-function, and that points of the Sato Grassmannian corresponding to non-trivial torsion points of a certain order on the Jacobian variety can be constructed by using the Dwork loop. For the sake of comparison, we study geometry of the Fermat quotient (1.0.2) in Section 3, and give a proof of Theorem 1.0.4 in Section 4.

# Chapter 2

# Sato Grassmannian and tau-functions

## 2.1 Sato Grassmannian and Krichever pairs

### 2.1.1 Definition of Sato Grassmannian

Let $K$ be a field. Let $K[[T^{-1}]]$ be the ring of power series in $T^{-1}$ with coefficients in $K$ and $K((T^{-1}))$ the fraction field of $K[[T^{-1}]]$. The *Sato Grassmannian* $\mathrm{Gr}^{alg}(K)$ is the set of all $K$-subspace $W \subset K((T^{-1}))$ such that the $K$-dimensions of the kernel and cokernel of the map

$$f_W : W \to K((T^{-1}))/K[[T^{-1}]], \quad w \mapsto w + K[[T^{-1}]]$$

are finite. The *index* of $W \in \mathrm{Gr}^{alg}(K)$ is defined by

$$i(W) := \mathrm{Ker}(f_W) - \mathrm{Coker}(f_W).$$

By definition of the Sato Grassmannian, a $K$-subspace $W \subset K((T^{-1}))$ belongs to $\mathrm{Gr}^{alg}(K)$ if and only if there exists some integer $i_0$ such that

$$\dim_K W \cap T^n K[[T^{-1}]] = \begin{cases} n + i_0 & (n \gg 0) \\ \{0\} & (n \ll 0). \end{cases} \tag{2.1.1}$$

(Here the integer $i_0$ equals to the index $i(W)$ of $W$ defined above.) For each $n \in \mathbb{Z}$ we define $\mathrm{Gr}^{alg,n}(K) := \{W \in \mathrm{Gr}^{alg}(K) \mid i(W) = n\}$.

### 2.1.2 Admissible basis

Let $W \in \mathrm{Gr}^{alg}(K)$ and put $i_0 := i(W)$. From the property (2.1.1), $W$ has a $K$-basis $\{w_i\}_{i=1}^{\infty}$ such that

(1) $\{\deg w_i\}_{i=1}^{\infty}$ is a strictly increasing sequence,

(2) $w_i$ is monic for all $i$, and

(3) $\deg(w_i - T^{i-i_0})$ is a bounded function of $i$.

(Here $\deg : K((T^{-1}))^* \to \mathbb{Z}$ is the sign inversion of the normalized valuation, and $w \in K((T^{-1}))$ is called monic if and only if $\deg(w - T^{\deg w}) < \deg(w)$.) Such a $K$-basis $\{w_i\}_{i=1}^{\infty}$ of $W$ will be called *admissible*. Conversely, if a $K$-subspace $V$ of $K((T^{-1}))$ has a $K$-basis satisfying the properties (1), (2) and (3) above for some integer $i_0$, then $V$ belongs to $\mathrm{Gr}^{alg}(K)$.

### 2.1.3 Partition, Plücker coordinate and Ferrer's diagram

Let $\lambda := (\lambda_i)_{i=1}^{\infty}$ be a sequence consisting of non-negative integers. The sequence $\lambda$ will be called the *partition* if $\lambda$ is a non-increasing sequence and $\lambda_i = 0$ for sufficiently large $i$. If $\lambda$ is a partition, the integer $\ell(\lambda) := \max\{i \mid \lambda_i \neq 0\}$ will be called the *length* of $\lambda$.

Let $W$ be an element of $\mathrm{Gr}^{alg}(K)$. For an admissible basis $\{w_i\}_{i=1}^{\infty}$ of $W$, we take the non-increasing sequence $\kappa := (\kappa_i)$ as

$$\kappa_i := i - i(W) - \deg(w_i).$$

The sequence $\kappa$ consists of non-negative integers and by definition $\kappa_i = 0$ for sufficiently large $i$. Hence $\kappa$ is a partition. We call $\kappa$ the *partition of* $W$. The partition $\kappa$ does not depend on a choice of an admissible basis of $W$. Note that if the partition $\kappa$ is a zero partition (i.e. $\kappa_i = 0$ for all $i \geq 1$), then the equation (2.1.1) implies that

$$W \cap T^{-i(W)} K[[T^{-1}]] \neq \{0\}.$$

Let $i_0 := i(W)$ be the index of $W$. We take an admissible basis $\{w_i\}_{i=1}^{\infty}$ of $W$ and write $w_i = \sum_j w_{ij}T^j$ $(w_{ij} \in K)$. Let $\lambda := (\lambda_i)_{i=1}^{\infty}$ be an arbitrary partition. Then for sufficiently large $j$, we have

$$w_{i,j-\lambda_j-i_0} = \begin{cases} 1 & (i = j) \\ 0 & (i \neq j), \end{cases}$$

since $\{w_i\}_{i=1}^{\infty}$ is admissible. Hence the determinant

$$\det_{i,j=1}^{n} w_{i,j-\lambda_j-i_0} \tag{2.1.2}$$

is independent of sufficiently large $n$. The determinant (2.1.2) will be called the *$\lambda$-th Plücker coordinate*, denoted by $P_\lambda(W)$. The Plücker coordinate does not depend on a choice of an admissible basis.

For a partition $\lambda$, the *Ferrer's diagram* of $\lambda$ is defined by

$$\Phi(\lambda) := \{(i, j) \in \mathbb{N} \mid j \leq \lambda_i,\ i = 1, 2, \ldots\}.$$

**Proposition 2.1.1.** *Let $\lambda$ be a partition and $\kappa$ the partition of $W \in \mathrm{Gr}^{alg}(K)$. Assume that $\Phi(\lambda) \not\supseteq \Phi(\kappa)$. Then we have $P_\lambda(W) = 0$.*

*Proof.* Let $\{w_i\}_{i=1}^{\infty}$ be an admissible basis of $W$ and $i_0$ the index of $W$. To prove that the determinant (2.1.2) is vanishing, it suffices to show that there exists an integer $i_1$ such that $w_{i_1,j-\lambda_j-i_0} = 0$ for all $j \geq i_1$, because $w_i$ is admissible. Since $\deg(w_i) = i - \kappa_i - i_0$, we have $w_{i,j} = 0$ for all $j > i - \kappa_i - i_0$. We also have some integer $i_1$ such that $\kappa_{i_1} > \lambda_{i_1}$ because of the assumption $\Phi(\lambda) \not\supseteq \Phi(\kappa)$. Hence we get $i_1 - \lambda_{i_1} - i_0 > i_1 - \kappa_{i_1} - i_0$, which means that elements $w_{i_1,j-\lambda_j-i_0}$ with all $j \geq i_1$ are zero. The claim is proved. □

Let $\lambda$ be a partition and $\Phi(\lambda)$ the Ferrer's diagram of $\lambda$. For each $(i, j) \in \Phi(\lambda)$, we define the corresponding *hook* at $(i, j)$ by the set

$$\{(k, l) \in \Phi(\lambda) \mid (k = i \text{ and } l \geq j) \text{ or } (k \geq i \text{ and } l = j)\}.$$

### 2.1.4 Krichever pairs

Let $X$ be a smooth projective geometrically irreducible curve over a field $K$ equipped with a $K$-rational point $\infty$. We fix an isomorphism $N_0 : \hat{\mathscr{O}}_{X,\infty} \cong K[[T^{-1}]]$, and write $N$ for the composition map

$$N : \operatorname{Spec} K((T^{-1})) \to \operatorname{Spec} K[[T^{-1}]] \xrightarrow{N_0} X.$$

An $N$-trivialization of a line bundle $\mathscr{L}$ on $X$ is an isomorphism $\sigma : N^*\mathscr{L} \cong K((T^{-1}))$ of $K((T^{-1}))$-vector spaces induced by an isomorphism $\sigma_0 : N_0^*\mathscr{L} \cong$

$K[[T^{-1}]]$ of $K[[T^{-1}]]$-modules. A pair $(\mathscr{L}, \sigma)$ of a line bundle $\mathscr{L}$ on $X$ and a $N$-trivialization $\sigma$ of $\mathscr{L}$ is called a ***Krichever pair***. Two Krichever pairs are said to be isomorphic if there exists an isomorphism of line bundles compatible with $N$-trivializations. We write $\mathrm{Kr}(X, N)$ for the set of isomorphism classes of Krichever pairs. We have a canonical surjective map

$$[\cdot] : \mathrm{Kr}(X, N) \to \mathrm{Pic}(X), \qquad [(\mathscr{L}, \sigma)] = \mathscr{L}.$$

For each $n \in \mathbb{Z}$ we define $\mathrm{Kr}^n(X, N) := \{(\mathscr{L}, \sigma) \in \mathrm{Kr}(X, N) \mid \deg(\mathscr{L}) = n\}$ to be the inverse image of $\mathrm{Pic}^n(X)$ by $[\cdot]$.

### 2.1.5 A Krichever pair associated to a Weil divisor

Let $D = \sum_{P \in X} n_P P$ be a Weil divisor on $X$. The associated line bundle $\mathscr{O}_X(D)$ admits a $N$-trivialization $\sigma(D)$ induced by the composition

$$\sigma(D) : \mathscr{O}_X(D) \hookrightarrow K(X) \overset{N}{\to} K((T^{-1})) \overset{T^{-n_\infty}}{\to} K((T^{-1})).$$

(Here $n_\infty$ is the coefficient of $\infty$ in $D$.) Therefore we obtain a Krichever pair $(\mathscr{O}_X(D), \sigma(D))$.

### 2.1.6 Vector space associated to a Krichever pair

For $(\mathscr{L}, \sigma) \in \mathrm{Kr}(X, N)$, we define a $K$-subspace $W(\mathscr{L}, \sigma)$ of $K((T^{-1}))$ by

$$W(\mathscr{L}, \sigma) := \{\sigma N^* f \in K((T^{-1})) \mid f \in H^0(X \setminus \{\infty\}, \mathscr{L})\}.$$

It follows from Riemann-Roch theorem that there exists a $K$-basis $\{w\}_{i=1}^{\infty}$ of $W(\mathscr{L}, \sigma)$ satisfying the property (1), (2) and (3) of §2.1.2 for $i_0 = \deg(\mathscr{L}) + 1 - g$, that is, $W(\mathscr{L}, \sigma) \in \mathrm{Gr}^{alg}(K)$. Note that $A := W(\mathscr{O}_X, N)$ is a $K$-subalgebra of $K((T^{-1}))$ such that $\mathrm{Spec}\, A \cong X \setminus \{\infty\}$, and that $W(\mathscr{L}, \sigma)$ is a $A$-submodule of $K((T^{-1}))$ for any $(\mathscr{L}, \sigma) \in \mathrm{Kr}(X, N)$.

The following fact is fundamental to us. (See Proposition 2.1.3 for details.)

**Proposition 2.1.2.** *Let $(\mathscr{L}, \sigma), (\mathscr{L}', \sigma') \in \mathrm{Kr}(X, N)$. If $W(\mathscr{L}, \sigma) = W(\mathscr{L}', \sigma')$, then we have $(\mathscr{L}, \sigma) = (\mathscr{L}', \sigma')$.*

### 2.1.7 Group structure

We regard $\mathrm{Kr}(X, N)$ as an abelian group by the tensor product, so that the identity element is given by $(\mathscr{O}_X, N)$. Note that $[\cdot] : \mathrm{Kr}(X, N) \to \mathrm{Pic}(X)$ is a group homomorphism. Take $(\mathscr{L}, \sigma), (\mathscr{L}', \sigma) \in \mathrm{Kr}(X, N)$ and let $(\mathscr{L}'', \sigma'') = (\mathscr{L} \otimes$

$\mathscr{L}', \sigma \otimes \sigma')$ be their product. Then $W(\mathscr{L}'', \sigma'')$ coincides with the $K$-subspace of $K((T^{-1}))$ spanned by $\{ww' \in K((T^{-1})) \mid w \in W(\mathscr{L}, \sigma), w' \in W(\mathscr{L}', \sigma')\}$.

For $V \in \mathrm{Gr}^{alg}(K)$, we set $A_V := \{f \in K((T^{-1})) \mid fV \subset V\}$, which is a $K$-subalgebra of $K((T^{-1}))$. We define

$$\mathrm{Gr}_A^{alg}(K) := \{V \in \mathrm{Gr}^{alg}(K) \mid A_V = A\}.$$

For $V, V' \in \mathrm{Gr}_A^{alg}(K)$, we define their product to be $V \cdot V' = \langle ww' \mid w \in V, w' \in V' \rangle_K$, under which $\mathrm{Gr}_A^{alg}(K)$ becomes an abelian group.

**Proposition 2.1.3** ([2, §2.3]; see also [22])**.** *The construction of §2.1.6 defines an isomorphism of abelian groups*

$$W : \mathrm{Kr}(X, N) \to \mathrm{Gr}_A^{alg}(K), \qquad (\mathscr{L}, \sigma) \mapsto W(\mathscr{L}, \sigma)$$

*which satisfies the following properties:*

1. *We have $i(W(\mathscr{L}, \sigma)) = \deg(\mathscr{L}) + 1 - g$ for any $(\mathscr{L}, \sigma) \in \mathrm{Kr}(X, N)$.*
2. *For $V, V' \in \mathrm{Gr}_A^{alg}(K)$, one has $[W^{-1}(V)] = [W^{-1}(V')]$ if and only if $V = uV'$ for some $u \in K[[T^{-1}]]^*$.*

*Moreover, the restriction of the map $W$ to $\mathrm{Kr}^0(X, N)$ defines an isomorphism of abelian groups*

$$W : \mathrm{Kr}^0(X, N) \to \mathrm{Gr}_A^{alg,1-g}(K).$$

### 2.1.8 Homothety class

For $W, W' \in \mathrm{Gr}^{alg}(K)$, we write $W \sim W'$ if $W = uW'$ for some $u \in K[[T^{-1}]]^\times$. This equivalent relation is called *homothety*. Note that $\mathrm{Gr}_A^{alg}(K)$ is stable under homothety, and also that $\mathrm{Gr}_A^{alg}(K)/\sim$ is well-defined as a group under the structure in the sense of §2.1.7. We write, by abuse of notation, $[W]$ for the homothety class of $W \in \mathrm{Gr}_A^{alg}(K)$. By Proposition 2.1.3, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Kr}(X, N) & \xrightarrow{[\cdot]} & \mathrm{Pic}(X) \\ {\scriptstyle W}\downarrow\wr & & \downarrow\wr \\ \mathrm{Gr}_A^{alg}(K) & \xrightarrow{[\cdot]} & \mathrm{Gr}_A^{alg}(K)/\sim . \end{array} \tag{2.1.3}$$

### 2.1.9 Theta divisor

Let us write $J := \mathrm{Pic}^0(X)$ for the *Jacobian variety* of $X$. Let us also write $\Theta \subset J$ for the *theta divisor*, which is defined to be the set of $\mathscr{L} \in J$ such that $H^0(C, \mathscr{L}((g-1)\infty)) \neq \{0\}$. (Here $\mathscr{L}((g-1)\infty) = \mathscr{L} \otimes \mathscr{O}_X((g-1)\infty)$.) Observe that $(\mathscr{L}, \sigma) \in \mathrm{Kr}^0(X, N)$ satisfies $\mathscr{L} \in \Theta$ if and only if

$$(*) \qquad W(\mathscr{L}, \sigma) \cap T^{g-1}K[[T^{-1}]] \neq \{0\},$$

because there is an isomorphism $W(\mathscr{L}, \sigma) \cap T^{g-1}K[[T^{-1}]] \cong H^0(X, \mathscr{L}((g-1)\infty))$. Let $\mathrm{Gr}_A^{\Theta}(K)$ be the set of elements of $\mathrm{Gr}^{alg,1-g}(K)$ satisfying the condition $(*)$. Then we have the following description of the Jacobian variety and the theta divisor:

$$\begin{array}{ccccc} \mathrm{Kr}^0(X,N) & \twoheadrightarrow & J & \supset & \Theta \\ \downarrow \wr & & \downarrow \wr & & \downarrow \wr \\ \mathrm{Gr}_A^{alg,1-g}(K) & \twoheadrightarrow & \mathrm{Gr}_A^{alg,1-g}(K)/\sim & \supset & \mathrm{Gr}_A^{\Theta}(K)/\sim . \end{array}$$

### 2.1.10 Automorphism of a curve

Suppose we are given two endomorphisms $r$ and $\bar{r}$ of $K$-schemes which fit in the commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}\, K((T^{-1})) & \xrightarrow{N} & X \\ {\scriptstyle \bar{r}}\downarrow & & \downarrow{\scriptstyle r} \\ \mathrm{Spec}\, K((T^{-1})) & \xrightarrow{N} & X. \end{array}$$

Assume further that $r(\infty) = \infty$. Then, for $(\mathscr{L}, \sigma) \in \mathrm{Kr}(X, N)$, the composition

$$(r, \bar{r})^*\sigma : N^*r^*\mathscr{L} \cong \bar{r}^*N^*\mathscr{L} \overset{\bar{r}^*\sigma}{\cong} \bar{r}^*K((T^{-1})) \cong K((T^{-1}))$$

is an $N$-trivialization of $r^*\mathscr{L}$. Therefore we get an induced homomorphism

$$\mathrm{Kr}(X, N) \to \mathrm{Kr}(X, N), \qquad (\mathscr{L}, \sigma) \mapsto (r^*\mathscr{L}, (r, \bar{r})^*\sigma),$$

which, by abuse of notation, will be denoted by $r^*$. This homomorphism is compatible with $[\cdot]$ in the sense that $[r^*(\mathscr{L}, \sigma)] = r^*\mathscr{L}$.

## 2.2 $p$-adic analytic Grassmannian — Anderson's theory —

Throughout this section, we assume that $p$ is a prime number and $K$ is a finite extension of the field $\mathbb{Q}_p$ of $p$-adic numbers equipped with the absolute value $|\cdot|$ such that $|p| = p^{-1}$.

### 2.2.1 $p$-adic Sato Grassmannian

Let $H(K)$ be the ring defined by

$$H(K) := \left\{ \sum_{i=-\infty}^{\infty} a_i T^i \;\middle|\; a_i \in K,\ \sup_{i=-\infty}^{\infty} |a_i| < \infty,\ \lim_{i\to\infty} |a_i| = 0 \right\}.$$

Note that $H(K)$ is equipped with the norm

$$\left\| \sum_i a_i T^i \right\| := \sup_i |a_i|,$$

and $(H(K), \|\cdot\|)$ is a $p$-adic Banach algebra over $K$ . Let $H_+(K)$ and $H_-(K)$ be the closed $K$-subspaces of $H(K)$ defined by

$$H_+(K) := \left\{ \sum_i a_i T^i \in H(K) \;\middle|\; a_i = 0 \text{ (for all } i \le 0) \right\},$$
$$H_-(K) := \left\{ \sum_i a_i T^i \in H(K) \;\middle|\; a_i = 0 \text{ (for all } i > 0) \right\}.$$

The *p-adic Grassmannian* $\mathrm{Gr}^{\mathrm{an}}(K)$ is the set of all $K$-subspaces $\bar{V} \subset H(K)$ such that $\bar{V}$ is the image of a $K$-linear injective map $w : H_+(K) \to H(K)$ satisfying the following conditions: there exist an integer $i_0$, a $K$-linear operator $v : H_+(K) \to H_-(K)$ with $\|v\| \le 1$, and a $K$-linear endomorphism $u$ on $H_+(K)$ with $\|u\| \le 1$ that is a uniform limit of bounded $K$-linear operators of finite rank (i.e. *completely continuous*), such that the map $T^{i_0} w$ has the form

$$T^{i_0} w = \begin{bmatrix} 1+u \\ v \end{bmatrix} : H_+(K) \to \begin{bmatrix} H_+(K) \\ H_-(K) \end{bmatrix}.$$

The *index* of $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$, denoted by $i(\bar{V})$, is defined by the difference of the dimensions of the kernel and cokernel of the projection map $\bar{V} \to H_+(K)$.

**Proposition 2.2.1** ([2, §3.2])**.** *There is an injective map*

$$\mathrm{Gr}^{\mathrm{an}}(K) \hookrightarrow \mathrm{Gr}^{alg}(K), \qquad \bar{V} \mapsto \bar{V}^{alg} := \bar{V} \cap K((T^{-1})).$$

*For any $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$, one has $i(\bar{V}) = i(\bar{V}^{alg})$. For $V \in \mathrm{Gr}^{alg}(K)$, there exists $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$ such that $\bar{V}^{alg} = V$ if and only if $V$ has an admissible basis $\{w_i\}$ such that $w_i \in H(K)$ for all $i$ and $\|w_i\| = 1$ for almost all $i$.*

*Proof.* We only show the "if" part of the last statement. Let $\{w_i\}$ be an admissible basis of $V$ such that $w_i \in H(K)$ for all $i$ and $\|w_i\| = 1$ for almost all $i$. Take non-zero constants $c_1, c_2, \ldots \in K$ such that $c_i = 1$ for almost all $i$ and $\|c_i w_i\| = 1$ for all $i$. Let $w$ be a $K$-linear map

$$w : TK[T] \to H(K), \quad T^i \mapsto c_i w_i.$$

This map extends to $H_+(K) \to H(K)$ since $\|w\| \leq 1$. If we write $w = T^{i_0}[1 + u, v]$, then $\|u\| \leq 1$, $\|v\| \leq 1$ and $u$ is a finite rank operator (hence completely continuous). Therefore $w$ is an admissible presentation of the closure $\bar{V}$ of $V$ in $H(K)$ and we have $\bar{V}^{alg} = V$. □

### 2.2.2 The $p$-adic loop group

We define the *$p$-adic loop group* $\Gamma(K)$ to be the subgroup of $H(K)^\times$ consisting of all $\sum_i h_i T^i \in H(K)^\times$ such that $|h_0| = 1$, $|h_i| \leq 1$ for all $i \leq 0$, and there exists a real number $0 < \rho < 1$ such that

$$|h_i| \leq \rho^i \quad \text{for all } i \geq 1.$$

Define the subgroups $\Gamma_+(K)$ and $\Gamma_-(K)$ of $\Gamma(K)$ by

$$\begin{aligned} \Gamma_+(K) &:= \left\{ \sum_i h_i T^i \in \Gamma(K) \;\middle|\; h_0 = 1, h_i = 0 \ (i < 0) \right\}, \\ \Gamma_-(K) &:= \left\{ \sum_i h_i T^i \in \Gamma(K) \;\middle|\; h_i = 0 \ (i > 0) \right\}. \end{aligned}$$

**Lemma 2.2.2.** *The $p$-adic loop group $\Gamma(K)$ acts on $\mathrm{Gr}^{\mathrm{an}}(K)$ as*

$$\Gamma(K) \times \mathrm{Gr}^{\mathrm{an}}(K) \to \mathrm{Gr}^{\mathrm{an}}(K), \qquad (h, \bar{V}) \mapsto h\bar{V} := \{hv \mid v \in \bar{V}\}.$$

*Moreover we have*

*(1) the action of $\Gamma_+(K)$ on $\mathrm{Gr}^{\mathrm{an}}(K)$ preserves index,*

(2) *the action of* $\Gamma_-(K)$ *on* $\mathrm{Gr}^{\mathrm{an}}(K)$ *preserves the homothety class in* $\mathrm{Gr}^{alg}(K)$*, that is, we have* $\bar{V}^{alg} \sim (h\bar{V})^{alg}$ *for* $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$ *and* $h \in \Gamma_-(K)$.

*Proof.* Let $w$ be an admissible presentation of $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$. Then by definition $T^{i(\bar{V})}w$ has the form

$$T^{i(\bar{V})}w = \begin{bmatrix} 1+u \\ v \end{bmatrix} : H_+(K) \to \begin{bmatrix} H_+(K) \\ H_-(K) \end{bmatrix},$$

where the operators $u$ and $v$ are of norm $\leq 1$ and $v$ is completely continuous. Now let $h \in \Gamma_+(K)$. We regard $h$ as a multiplicative operator $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on $H(K) = H_+(K) \oplus H_-(K)$. Then the operators $a, d$ are invertible and isometric of norm $\leq 1$, the operator $b$ is completely continuous of norm $< 1$, and the operator $c$ is $0$. Note that $hw$ does not give an admissible presentation of $h\bar{V}$ in general, however the operator $hwa^{-1}$ on $H_+(K)$ has the form

$$hwa^{-1} = T^{i(\bar{V})} \begin{bmatrix} 1 + aua^{-1} + bva^{-1} \\ dva^{-1} \end{bmatrix},$$

which gives an admissible presentation of $h\bar{V}$. Hence it follows $h\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$ and $i(W) = i(h\bar{V})$, and the claim (1) is proved. The claim (2) is immediately followed from Proposition 2.1.3 since $\Gamma_-(K) \subset K[[T^{-1}]]^\times$ □

### 2.2.3 $p$-adic tau-functions

Let $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$ and $h \in \Gamma_+(K)$. We define the *tau-function* by

$$\tau_w(h) := \det[H_+ \overset{T^{i(\bar{V})}w}{\to} H \overset{h}{\to} H \overset{\text{proj.}}{\to} H_+], \tag{2.2.1}$$

where the operator $w$ is an admissible presentation of $\bar{V}$. (Here the right hand side of (2.2.1) is an infinite dimensional determinant which is defined by Serre in [30].) The following proposition is a crucial property of the tau-function.

**Proposition 2.2.3.** *Let* $w$ *be an admissible presentation of a given* $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$. *A necessary and sufficient condition for* $h \in \Gamma_+(K)$ *to be* $\tau_w(h) = 0$ *is that*

$$h\bar{V} \cap T^{-i(\bar{V})}K[[T^{-1}]] = \{0\}.$$

*Proof.* In general the determinant of a $K$-linear map on a Banach space over $K$ is vanishing if and only if the kernel of the $K$-linear map is non-trivial. Hence we have

$$\tau_w(h) = 0 \Leftrightarrow \mathrm{Ker}[H_+ \overset{T^{i(\bar{V})}w}{\to} H \overset{h}{\to} H \overset{\text{proj.}}{\to} H_+] \neq \{0\}$$

$$\Leftrightarrow T^{i(\bar{V})}\bar{V} \cap h^{-1}H_- \neq \{0\}$$
$$\Leftrightarrow h\bar{V} \cap T^{-i(\bar{V})}H_- \neq \{0\}$$
$$\Leftrightarrow h\bar{V} \cap T^{-i(\bar{V})}K[[T^{-1}]] \neq \{0\}.$$

□

### 2.2.4 Schur functions

Let $h := \sum_{i=0}^{\infty} h_i T^i$ be a loop in $\Gamma_+(K)$ such that

$$|h_i| \leq \rho^i \qquad (i = 0, 1, 2, \ldots)$$

for some real number $0 < \rho < 1$. For a partition $\lambda = (\lambda_i)_{i=1}^{\infty}$, the *Schur function* $S_\lambda(h)$ is defined by

$$S_\lambda(h) := \det_{i,j=1}^{\ell(\lambda)} h_{\lambda_i - i + j},$$

where $\ell(\lambda)$ is the length of the partition $\lambda$. The tau-function has an expression in terms of Schur functions and Plcker coordinates (§2.1.3) as follows.

**Theorem 2.2.4** (see [27, 28], or [29])**.** *Let $w$ be an admissible presentation of an arbitrary $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$. Assume that an admissible basis of $\bar{V}^{alg}$ is given by $\{w(T^i)\}_{i=1}^{\infty}$. Then*

$$\tau_w(h) = \sum_{\lambda} P_\lambda(\bar{V}^{alg}) S_\lambda(h), \tag{2.2.2}$$

*where the suffix $\lambda$ runs all partitions.*

The assumption for $\bar{V}^{alg}$ in Theorem 2.2.4 means that there exists an admissible basis $\{w_i\}_{i=1}^{\infty}$ of $\bar{V}^{alg}$ such that $\|w_i\| = 1$ for all $i \geq 1$. Hence one sees that the right hand side of (2.2.2) converges for any partition $\lambda$ because we have

$$|P_\lambda(\bar{V}^{alg})| \leq 1 \qquad \text{and} \qquad |S_\lambda(h)| \leq \rho^{|\lambda|} \tag{2.2.3}$$

where $|\lambda| := \sum_i \lambda_i$ (the *weight* of $\lambda$). From Proposition 2.1.1, $P_\lambda(\bar{V}^{alg}) = 0$ if the Ferrer's diagram $\Phi(\lambda)$ does not contain the Ferrer's diagram $\Phi(\kappa)$ where $\kappa$ is the partition of $\bar{V}^{alg}$. Hence it follows that the sum on the right hand side of (2.2.2) is restricted to the sum only on the partition $\lambda$ such that $\Phi(\lambda) \supseteq \Phi(\kappa)$. The following proposition gives a non-vanishing property of the $p$-adic tau-function.

**Proposition 2.2.5.** *We use the same assumption in Theorem 2.2.4. Let $\kappa$ be the partition of $\bar{V}^{alg}$. Assume further that there exists a loop $h \in \Gamma_+(K)$ satisfying*

$$|S_\lambda(h)| < |S_\kappa(h)|$$

*for all partitions $\lambda$ such that $\Phi(\lambda) \supseteq \Phi(\kappa)$ and $\lambda \neq \kappa$. Then we have*

$$\tau_w(h) \neq 0.$$

*Proof.* Note that $P_\kappa(\bar{V}^{alg}) = 1$. By (2.2.3), we have

$$|\tau_w(h) - S_\kappa(h)| < |\tau_w(h)|.$$

This inequality implies that $\tau_w(h) \neq 0$ because $|S_\kappa(h)| \geq 0$. □

### 2.2.5 Dwork loops and Anderson's theorem

In his study of the $p$-adic properties of zeta functions of hypersurfaces over finite fields (see, for example, [10]), Dwork constructed a special element of $\Gamma(K)$ (which we call a Dwork loop). We shall exploit his construction. Assume that $K$ contains a $(p-1)$-st root $\pi$ of $-p$. Let $u$ be a unit of the integer ring of $K$. A *Dwork loop* is defined by

$$h(T) := \exp(\pi((uT) - (uT)^p)).$$

For all $i \geq 0$, we have (see, for example [16, Chapter I])

$$|h_i| \leq |p|^{i(p-1)/p^2} \tag{2.2.4}$$

where $h(T) = \sum_i h_i T^i$. Therefore $h(T) \in \Gamma_+(K)$.

The following theorem is technically crucial in Anderson [2].

**Theorem 2.2.6** ([2, Lemma 3.5.1])**.** *Assume that $p \geq 7$. Let $h$ be a Dwork loop and $w$ be an admissible presentation of a given $\bar{V} \in \mathrm{Gr}^{\mathrm{an}}(K)$. We write $\kappa = (\kappa_i)_{i=1}^\infty$ and $\ell(\kappa)$ for the partition of $\bar{V}^{alg}$ and the length of $\kappa$. Assume further that $\bar{V}^{alg}$ satisfies that*

*(A1) there exists an admissible basis $\{w_i\}_{i=1}^\infty$ such that $\|w_i\| = 1$ for all $i \geq 1$,*

*(A2) the partition $\kappa$ satisfies $\max\{\kappa_1, \ell(\kappa)\} < p/4$.*

*Then, we have $\tau_w(h) \neq 0$. Equivalently, we have*

$$h\bar{V} \cap T^{-i(\bar{V})} K[[T^{-1}]] = \{0\}.$$

*Proof.* From the assumption (A1) and Proposition 2.2.5, it suffices to show that

$$|S_\lambda(h)| < |S_\kappa(h)|$$

for all partitions $\lambda$ such that $\Phi(\lambda) \supseteq \Phi(\kappa)$ and $\lambda \neq \kappa$. By (2.2.4) and definition of Schur functions in §2.2.4, we have

$$|S_\lambda(h)| \leq |p|^{|\lambda|(p-1)/p^2}. \tag{2.2.5}$$

for each partition $\lambda$. Since $h_i = (u\pi)^i/i!$ for $0 \le i < p$, we have

$$S_\lambda(h) = \frac{(u\pi)^{|\lambda|} C_\lambda}{|\lambda|!}$$

for each partition $\lambda$ such that $\ell(\lambda) + \lambda_1 \le p$, where

$$C_\lambda := |\lambda|! \left( \prod_{(i,j)\in\Phi(\lambda)} C_\lambda(i,j) \right)^{-1}$$

and $C_\lambda(i,j)$ is the cordiality of the hook at $(i,j) \in \Phi(\lambda)$. (Here the *hook* is defined in §2.1.3). Note that $C_\lambda(i,j) \le \ell(\lambda) + \lambda_1 - 1 < p$ for any $(i,j) \in \Phi(\lambda)$, thus $C_\lambda(i,j)$ is a $p$-adic unit. Hence we have

$$|S_\lambda(h)| = |(u\pi)^{|\lambda|}| = |p|^{|\lambda|/(p-1)} \tag{2.2.6}$$

for each partition $\lambda$ such that $\ell(\lambda) + \lambda_1 \le p$. By the assumption (A2), $\kappa$ satisfies $\ell(\kappa) + \kappa_1 \le p$, hence it follows from (2.2.6) that

$$|S_\kappa(h)| = |p|^{|\kappa|/(p-1)}. \tag{2.2.7}$$

Hence the claim holds if $\lambda$ satisfies $\ell(\lambda) + \lambda_1 \le p$, because $|\lambda| > |\kappa|$.

By (2.2.5) and (2.2.7), we need to show

$$\frac{|\kappa|}{p-1} < \frac{|\lambda|(p-1)}{p^2}$$

for each partition $\lambda$ such that $\ell(\lambda) + \lambda_1 > p$. Now we have $C_\lambda(1,1) \ge p$ because $\ell(\lambda) + \lambda_1 > p$, and also have $C_\kappa(1,1) < p/2 - 1$ because the assumption (A1). Therefore we have

$$|\lambda| \ge |\kappa| + \frac{p}{2} + 1.$$

We also have $|\kappa| < p^2/4$ from (A1). Hence it follows that

$$\begin{aligned}
|\lambda| \left(\frac{p-1}{p^2}\right) - |\kappa| \left(\frac{1}{p-1}\right) &\ge \left(|\kappa| + \frac{p}{2} + 1\right) \left(\frac{p-1}{p^2}\right) - |\kappa| \left(\frac{1}{p-1}\right) \\
&= \left(1 + \frac{p}{2}\right) \left(\frac{p-1}{p^2}\right) - |\kappa| \left(\frac{p-1}{p^2} + \frac{1}{p-1}\right) \\
&> \left(1 + \frac{p}{2}\right) \left(\frac{p-1}{p^2}\right) - \frac{p^2}{4} \left(\frac{p-1}{p^2} + \frac{1}{p-1}\right) \\
&\ge 0
\end{aligned}$$

if $p \ge 3 + \sqrt{5}$, and we are done.

□

### 2.2.6 $p$-adic analytic part of Krichever pairs

In this subsection, we translate all results in §2.2.1–§2.2.5 into the language of Krichever pairs. Therefore all results in this subsection can be explained by the results in §2.2.1–§2.2.5.

We use the notation of §2.1.4. Let $\mathrm{Kr}_{\mathrm{an}}(X, N)$ be the subset of $\mathrm{Kr}(X, N)$ consisting of all Krichever pairs $(\mathscr{L}, \sigma)$ such that $W(\mathscr{L}, \sigma)$ admits an admissible basis $\{w_i\}$ satisfying

1. $w_i \in H(K)$ for all $i$, and
2. $\|w_i\| = 1$ for almost all $i$.

For each $n \in \mathbb{Z}$, we put $\mathrm{Kr}^n_{\mathrm{an}}(X, N) = \mathrm{Kr}_{\mathrm{an}}(X, N) \cap \mathrm{Kr}^n(X, N)$.

For $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we write $\bar{W}(\mathscr{L}, \sigma)$ for the closure of $W(\mathscr{L}, \sigma)$ in $H(K)$. One recovers $W(\mathscr{L}, \sigma)$ from $\bar{W}(\mathscr{L}, \sigma)$ by $W(\mathscr{L}, \sigma) = \bar{W}(\mathscr{L}, \sigma) \cap K((T^{-1}))$. (Here we regard both $H(K)$ and $K((T^{-1}))$ as $K$-vector subspaces of $\prod_{i\in\mathbb{Z}} KT^i$.) It follows that

$$\mathrm{Kr}_{\mathrm{an}}(X, N) = \{(\mathscr{L}, \sigma) \in \mathrm{Kr}(X, N) \mid \bar{W}(\mathscr{L}, \sigma) \in \mathrm{Gr}^{\mathrm{an}}(K)\}.$$

Hence the following propositions are the reformulation of Proposition 2.1.2 and Lemma 2.2.2 respectively.

**Proposition 2.2.7.** *Let $(\mathscr{L}, \sigma), (\mathscr{L}', \sigma')$ be Krichever pairs in $\mathrm{Kr}_{\mathrm{an}}(X, N)$. If $\bar{W}(\mathscr{L}, \sigma) = \bar{W}(\mathscr{L}', \sigma')$, then we have $(\mathscr{L}, \sigma) = (\mathscr{L}', \sigma')$.*

**Proposition 2.2.8** ([2, §3.3])**.** *There is an action of $\Gamma(K)$ on $\mathrm{Kr}_{\mathrm{an}}(X, N)$ characterized by the following property: for any $h \in \Gamma(K)$ and $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $\bar{W}(h(\mathscr{L}, \sigma)) = h\bar{W}(\mathscr{L}, \sigma)$. (Here the right hand side means $\{hw \mid w \in \bar{W}(\mathscr{L}, \sigma)\}$.) Moreover, this action satisfies the following properties:*

1. *For any $h \in \Gamma(K)$ and $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $\deg[h(\mathscr{L}, \sigma)] = \deg[(\mathscr{L}, \sigma)]$.*
2. *For any $h \in \Gamma_-(K)$ and $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $[h(\mathscr{L}, \sigma)] = [(\mathscr{L}, \sigma)]$.*
3. *Suppose $(\mathscr{O}_X, N) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$. For any $h \in \bar{W}(\mathscr{O}_X, N) \cap \Gamma(K)$ and $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $[h(\mathscr{L}, \sigma)] = [(\mathscr{L}, \sigma)]$.*

Finally, the following theorem is a reformulation of Theorem 2.2.9 ([2, Lemma 3.5.1]).

**Theorem 2.2.9** ([2, Lemma 3.5.1])**.** *Assume that $p \geq 7$. Let $h$ be a Dwork loop and $(\mathscr{L}, \sigma) \in \mathrm{Kr}^0_{\mathrm{an}}(X, N)$. We write $\kappa = (\kappa_i)_{i=1}^{\infty}$ and $\ell(\kappa)$ for the partition of $W(\mathscr{L}, \sigma)$ and the length of $\kappa$. Assume further that $W(\mathscr{L}, \sigma)$ satisfies that*

*(A1) there exists an admissible basis $\{w_i\}_{i=1}^{\infty}$ such that $\|w_i\| = 1$ for all $i \geq 1$,*

*(A2) the partition $\kappa$ satisfies $\max\{\kappa_1, \ell(\kappa)\} < p/4$.*

*Then, we have $W(h(\mathscr{L}, \sigma)) \cap T^{g-1}K[[T^{-1}]] = \{0\}$. Equivalently, we have*

$$[h(\mathscr{L}, \sigma)] \notin \Theta.$$

## 2.3 Complex analytic Grassmannian — theta and tau functions —

In this section, we study a relation between the theta-function and the tau-function, which is summarized in Segal-Wilson's paper [29]. The theta-function is a holomorphic function on a $g$-dimensional complex vector space $U := H^1(X, \mathscr{O}_X)$ and characterized by functional equations with respect to the lattice $\Lambda := H^1(X, \mathbb{Z})$ in $U$, where $X/\mathbb{C}$ is a compact Riemann surface of genus $g$. On the other hand, the tau-function is a holomorphic function on the loop group which is an infinite dimensional vector space. Our Goal in this section is, roughly speaking, to show under some translations of domains of these functions that

**Claim 2.3.1.** (tau-function) = (exponential factor) $\cdot$ (theta-function).

We first give a review of the Mumford theta-function in subsection 1, study the Čech cohomology of Riemann surfaces in subsection 2, and give definitions of the complex analytic Grassmannian and the loop group in subsections 3, 4, and 5. In subsection 6,7, and 8, we deal with the complex analytic tau-function whose definition is given in a different manner to the definition in §2.2.3, but they are essentially the same. The proof of Claim 2.3.1 is given in the final subsection.

**Remark 2.3.2.** Claim 2.3.1 is independent of the main results in this thesis, but it interests because we have hopes that there exists a $p$-adic analogous theory of this claim.

### 2.3.1 Mumford theta-functions

Let $X/\mathbb{C}$ be a compact Riemann surface of genus $g$ and $\mathscr{O}_X$ the sheaf of holomorphic functions on $X$. The exponential map $f \to e^f$ induces an exact sequence of sheaves:

$$0 \to 2\pi i\mathbb{Z} \to \mathscr{O}_X \overset{f \to e^f}{\to} \mathscr{O}_X^{\times} \to 0.$$

If we identify $2\pi i\mathbb{Z}$ with $\mathbb{Z}$, we obtain the exact

$$\begin{aligned} 0 \to & H^0(X, \mathbb{Z}) \to H^0(X, \mathscr{O}_X) \to H^0(X, \mathscr{O}_X^{\times}) \\ \to & H^1(X, \mathbb{Z}) \to H^1(X, \mathscr{O}_X) \to H^1(X, \mathscr{O}_X^{\times}) \to H^2(X, \mathbb{Z}). \end{aligned}$$

Note that the map $H^0(X, \mathscr{O}_X) \to H^0(X, \mathscr{O}_X^{\times})$ is surjective and that the map $\mathrm{Pic}(X) = H^1(X, \mathscr{O}_X^{\times}) \to H^2(X, \mathbb{Z}) = \mathbb{Z}$ is the degree map. Put $\Lambda := H^1(X, \mathbb{Z})$, $U := H^1(X, \mathscr{O}_X)$, and define $J$ to be the subgroup of $\mathrm{Pic}(X)$ of degree $0$. Then we get an exact sequence

$$0 \to \Lambda \to U \to J \to 0.$$

Note that $U$ is a complex vector space of dimension $g$ and $\Lambda$ is a lattice in $U$ and that the Jacobian $J$ of $X$ is isomorphic to $U/\Lambda$, which becomes a complex torus.

Let $\Lambda \times \Lambda \to \mathbb{Z}$ be the intersection pairing of $\Lambda$. Let us denote $\lambda \cdot \lambda'$ by the image of $\lambda, \lambda' \in \Lambda$ in this pairing map and fix a quadratic form $s : \Lambda \to \mathbb{Z}/2\mathbb{Z}$ such that

$$s(\lambda + \lambda') - s(\lambda) - s(\lambda') \equiv \lambda \cdot \lambda' \bmod 2.$$

The *theta-function* $\theta(u)$ of $X$ is defined by a holomorphic function on $U$:

$$\theta(u) := \sum_{\lambda \in \Lambda} (-1)^{s(\lambda)} e^{-\frac{\pi}{2} H(\lambda, \lambda + 2u)},$$

where $H : U \times U \to \mathbb{C}$ is a unique Hermitian form over $U$ such that the imaginary part of this form is the $\mathbb{R}$-bilinear extension of the intersection pairing of $\Lambda$. For $u \in U$, $\lambda \in \Lambda$, one can easily check that the theta-function satisfies the following equation

$$\theta(u) = (-1)^{s(\lambda)} e^{-\frac{\pi}{2} H(\lambda, \lambda + 2u)} \theta(u + \lambda). \tag{2.3.1}$$

The functional equation (2.3.1) gives a characterization of the theta-function up to a constant factor (see, for example [21]). If we write $C := \theta(0)^{-1}$, then the equation (2.3.1) is written by

$$\theta(u + \lambda) = C\theta(u)\theta(\lambda) e^{\pi H(\lambda, u)}. \tag{2.3.2}$$

The relation (2.3.2) also gives a characterization of the theta function up to a certain transformation, namely

**Lemma 2.3.3.** *Let $f$ be a holomorphic function on $U$ such that*

$$f(u + \lambda) = C' f(u) f(\lambda) e^{\pi H(\lambda, u)}$$

*for all $u \in U$, $\lambda \in \Lambda$, and for some constant $C' \in \mathbb{C}^\times$. Then*

$$f(u) = C_f e^{\alpha(u)} \theta(u - \beta),$$

*for some constant $C_f \in \mathbb{C}^\times$, a $\mathbb{C}$-linear map $\alpha : U \to \mathbb{C}$, and some point $\beta \in U$.*

*Proof.* We claim that a certain translation of the function $f$ satisfies the functional equation (2.3.1) up to a constant. Put $g(u) := C' f(u)/(C\theta(u))$. Then for $u \in U, \lambda \in \Lambda$,

$$g(u + \lambda) = \frac{(C')^2 f(u) f(\lambda) e^{\pi H(\lambda, u)}}{C^2 \theta(u)\theta(\lambda) e^{\pi H(\lambda, u)}} = g(u) g(\lambda).$$

In particular the function $g$ is a homomorphism on $\Lambda$. We choose a $\mathbb{R}$-linear map $a : U \to \mathbb{C}$ such that $g(\lambda) = e^{a(\lambda)}$ for $\lambda \in \Lambda$. Write $a = \alpha + \gamma$, where $\alpha$ is

$\mathbb{C}$-linear and $\gamma$ is antilinear. Since the Hermitian form $H$ is non-degenerate, there exists $\beta \in U$ such that $\gamma(\lambda) = -\pi H(\lambda, \beta)$. Hence we have $g(\lambda) = e^{\alpha(\lambda) - \pi H(\lambda,\beta)}$ for $\lambda \in \Lambda$. Here we put

$$G(u) := \frac{e^{-\alpha(u)} f(u+\beta)}{\theta(u)}.$$

Then a direct computation gives

$$G(u+\lambda) = G(u) e^{-\alpha(\lambda) + \pi B(\lambda,\beta)} g(\lambda) = G(u)$$

for $u \in U$ and $\lambda \in \Lambda$. Hence $e^{-\alpha(u)} f(u+\beta)$ satisfies the functional equation (2.3.1). □

### 2.3.2 Čech cohomology

We fix a point $x_\infty \in X$ and choose a local parameter $T^{-1}$ at $x_\infty$. Let $D_0 := \{|T| \leq 1\}$ and $D_\infty := \{|T| \geq 1\}$ be discs in the Riemann sphere. We choose a holomorphic embedding $N$ from a neighborhood of $D_\infty$ to underlying $X$ such that $N(x_\infty) = \infty$. Set $X_\infty = N(D_\infty)$. Let $X_0$ denote the complement of the interior of $X_\infty$ in $X$. One can regard the intersection $X_0 \cap X_\infty$ as the unit circle $S^1$ by $N$. Let $V_0$ be the set of holomorphic functions $f : D_0 \to \mathbb{C}$ with $f(0) = 0$. Then we claim that there exists a surjective map $V_0 \twoheadrightarrow U$. (Recall that $U := H^1(X, \mathscr{O}_X)$ is a $g$-dimensional vector space over $\mathbb{C}$.)

Let $\{\mathcal{U}_0, \mathcal{U}_\infty\}$ be an open covering of $X$ to be $X_0 \subset \mathcal{U}_0 \subset X$ and $X_\infty \subset \mathcal{U}_\infty \subset X$. Taking the Čech complex of $X$ with respect to the open covering $\{\mathcal{U}_0, \mathcal{U}_\infty\}$, we have the exact sequence

$$0 \to \mathbb{C} \to \mathscr{O}_X(\mathcal{U}_0) \oplus \mathscr{O}_X(\mathcal{U}_\infty) \to \mathscr{O}_X(\mathcal{U}_0 \cap \mathcal{U}_\infty) \to U \to 0.$$

If we take the direct limit of the above sequence with respect to $\mathcal{U}_0$ and $\mathcal{U}_\infty$ by approximating to $X_0$ and $X_\infty$, we have the exact sequence

$$0 \to \mathbb{C} \to \mathscr{O}_X(X_0) \oplus \mathscr{O}_X(X_\infty) \to \mathscr{O}_X(X_0 \cap X_\infty) \to U \to 0.$$

Let $V_\infty$ be the set of holomorphic functions $g : D_\infty \to \mathbb{C}$ with $f(\infty) = 0$. Then we have

$$0 \to \mathscr{O}_X(X_0) \oplus V_\infty \to \mathscr{O}(S^1) \to U \to 0$$

under the identification $X_\infty \cong D_\infty$. Similarly, giving the same procedure for $\mathbb{P}^1(\mathbb{C})$, we have the exact sequence

$$0 \to \mathscr{O}(D_0) \oplus V_\infty \to \mathscr{O}(S^1) \to 0,$$

hence we have

$$0 \to \mathscr{O}_X(X_0) \to \mathscr{O}(D_0) \to U \to 0.$$

As a conclusion, we get a surjective map $V_0 \twoheadrightarrow U$.

### 2.3.3 Complex analytic part of Sato Grassmannian

Let $H$ be the set of square integrable $\mathbb{C}$-valued functions on the unit circle $S^1$ and $T^i$ $(i \in \mathbb{Z})$ the orthonormal basis on $H$. Define $H_+$ and $H_-$ by the closed subspace of $H$ to be spanned by the basis $\{T^i\}$ with $i \geq 1$ and $i \leq 0$, respectively. Then we have a decomposition $H = H_+ \oplus H_-$.

The (*complex analytic*) *Sato Grassmannian* $\mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}$ is the set of consisting of closed $\mathbb{C}$-subspaces $W \subset H$ such that the kernel and cokernel of the projection map

$$pr : W \to H_+$$

are finite dimensional over $\mathbb{C}$. Equivalently, the the $K$-subspace $W \subset H$ belongs to $\mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}$ if and only if there exists an injective map

$$w : H_+ \to H$$

such that $W$ is the image of $w$ and that for some integer $i$ the map $T^i w$ has the form

$$T^i w = \begin{bmatrix} w_+ \\ w_- \end{bmatrix},$$

where $w_+ - 1$ is a trace class and $w_-$ is a compact operator. We call an *admissible presentation* the injective map $w$. The *index* of $W$ is the integer $i := i(W)$. Note that $\{T^{i(W)} w(T^j)\}_{j=1}^{\infty}$ gives a $\mathbb{C}$-basis of $W$, which is called an *admissible basis* with respect to the admissible presentation $w$.

**Remark 2.3.4.** For $W \in \mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}$, the intersection

$$W^{alg} := W \cap \mathbb{C}((T^{-1}))$$

gives an element of $\mathrm{Gr}^{alg}(\mathbb{C})$ and $i(W) = i(W^{alg})$. (Here $\mathrm{Gr}^{alg}(\mathbb{C})$ is defined in the sense of §2.1.1.) Since $W^{alg}$ is dense in $W$, we have an embedding

$$\mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}} \hookrightarrow \mathrm{Gr}^{alg}(\mathbb{C}); \quad W \mapsto W^{alg}.$$

Hence we can regard $\mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}$ as a subset of $\mathrm{Gr}^{alg}(\mathbb{C})$. One recovers $W$ from $W^{alg}$ by taking the closure of $W^{alg}$ in $H$.

### 2.3.4 Complex analytic part of Krichever pairs

We use the same notation in §2.3.2. The *complex Krichever pair* $(\mathscr{L}, \sigma)$ is a pair of a line bundle $\mathscr{L}$ on $X$ and an $N$-trivialization $\sigma$ of $\mathscr{L}$, where the $N$-trivialization is a trivialization of $\mathscr{L}$ over $X_\infty$. Let us write $\mathrm{Kr}_{\mathbb{C}}(X, N)$ to be the set of complex Krichever pairs $(\mathscr{L}, \sigma)$.

**Theorem 2.3.5** (cf. [29, Proposition 6.1] or [22]). *For $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathbb{C}}(X, N)$, let $W(\mathscr{L}, \sigma)$ be the closure in $H$ of the set of functions $f \in H$ such that $f$ has the form $f = \sigma \tilde{f}|_{S^1}$ for some open subset $X_0 \subset \mathcal{U} \subset X$ and some section $\tilde{f} \in \Gamma(\mathcal{U}, \mathscr{L})$. (Here $\tilde{f}|_{S^1}$ is the section $\tilde{f}$ restricted to $X_0 \cap X_\infty \cong S^1$.) Then $W(\mathscr{L}, \sigma) \in \mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}$ and $i(W(\mathscr{L}, \sigma)) = 1 - g + \deg(\mathscr{L})$.*

We write $A := W(\mathscr{O}_X, N)$. Note that $i(A) = 1 - g$ and that $AW(\mathscr{L}, \sigma) \subseteq W(\mathscr{L}.\sigma)$ for all $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathbb{C}}(X, N)$. We put $\mathrm{Kr}_{\mathbb{C}}^n := \{(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathbb{C}}(X, N) \mid \deg(\mathscr{L}) = n\}$.

### 2.3.5 Complex analytic loop group

The *loop group* $\Gamma$ is defined by

$$\Gamma := \{h : S^1 \to \mathbb{C}^\times \mid \text{real analytic function}\}.$$

The loop group $\Gamma$ acts on $\mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}$ as

$$\Gamma \times \mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}} \to \mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}, \qquad (h, W) \mapsto hW := \{hw \mid w \in W\}.$$

Let $\Gamma_+$ (resp. $\Gamma_-$) be the subgroup of $\Gamma$ to be the set consisting of elements $h \in \Gamma$ such that $h$ has the form $h = \tilde{h}|_{S^1}$ for some holomorphic $\tilde{h} : D_0 \to \mathbb{C}^\times$ with $\tilde{h}(0) = 1$ (resp. $\tilde{h} : D_\infty \to \mathbb{C}^\times$ with $\tilde{h}(\infty) = 1$ ). These groups also act on $\mathrm{Gr}_{\mathbb{C}}^{\mathrm{an}}$.

### 2.3.6 Determinant bundle and tau-functions

In this subsection, we define the tau-function in a different manner to §2.2.3. Namely, we construct a holomorphic line bundle (determinant bundle) over the Grassmannian on which the loop group acts, and define the tau-functions by the use of these objects.

We first start with an example of finite dimensional determinant bundle. For $V \in \mathrm{Gr}(n, m)$ $(1 \leq n \leq m < \infty)$, we write $\bigwedge^n V$ for the set $\{\lambda v_1 \wedge v_2 \wedge \cdots \wedge v_n \mid \lambda \in \mathbb{C}\}$, where $(v_1, v_2, \ldots, v_n)$ is a $\mathbb{C}$-basis of $V$. If we choose another basis $(v_1', v_2', \ldots, v_n')$ of $V$, then there exists $t \in \mathrm{GL}_n(\mathbb{C})$ such that

$$(v_1, v_2, \ldots, v_n) = (v_1', v_2', \ldots, v_n')t^{-1}.$$

For $\lambda v_1 \wedge v_2 \wedge \cdots \wedge v_n \in \bigwedge^n V$, we have a computation

$$\begin{aligned} \lambda v_1 \wedge v_2 \wedge \cdots \wedge v_n =& \lambda(v_1' t^{-1}) \wedge (v_2' t^{-1}) \wedge \cdots \wedge (v_n' t^{-1}) \\ =& \lambda \det(t^{-1}) v_1' \wedge v_2' \wedge \cdots \wedge v_n'. \end{aligned}$$

A point of the determinant bundle $\mathrm{Det}^*(n,m)$ over $V$ is defined by a pairs $(v,\lambda)$, where $v$ is a $\mathbb{C}$-basis $v=(v_1,v_2,\ldots,v_n)$ of $V$, $\lambda\in\mathbb{C}$, and $(v,\lambda)$ is identified with $(vt,\lambda\det(t^{-1}))$, which defines a holomorphic line bundle over $\mathrm{Gr}(n,m)$ as

$$\mathrm{Det}^*(n,m)\to\mathrm{Gr}(n,m)\ ;\ (v,\lambda)\mapsto V:=\langle v\rangle_{\mathbb{C}}.$$

We return to the infinite dimensional Grassmannian. From now on, we deal with the subset of index 0 in $\mathrm{Gr}^{\mathrm{an}}_{\mathbb{C}}$, denoted by $\mathrm{Gr}^{an,0}_{\mathbb{C}}$. Let $W$ be an element of $\mathrm{Gr}^{an,0}_{\mathbb{C}}$. A point of $\mathrm{Det}^*$ over $W$ is defined by a pairs $(w,\lambda)$, where $w$ is an admissible basis $w=(w_1,w_2,\ldots)$ of $W$, $\lambda\in\mathbb{C}$, and $(w,\lambda)$ is identified with $(wt,\lambda\det(t^{-1}))$ for some $t\in\mathrm{GL}_{\mathbb{N}}(\mathbb{C})$. (Here $t-1$ is a trace class, hence the determinant of $t$ exists). This construction defines a holomorphic line bundle over $\mathrm{Gr}^{\mathrm{an},0}_{\mathbb{C}}$ as

$$\mathscr{D}:\mathrm{Det}^*\to\mathrm{Gr}^{\mathrm{an},0}_{\mathbb{C}}\ ;\ (w,\lambda)\mapsto W:=\overline{\langle w\rangle}^H,$$

where $\overline{\langle w\rangle}^H$ is the closure of the $\mathbb{C}$-spanned of $(w_1,w_2,\ldots)$ in $H$. We call $\mathrm{Det}^*$ the *determinant bundle* on $\mathrm{Gr}^{\mathrm{an},0}_{\mathbb{C}}$.

The loop groups $\Gamma_\pm$ act on $\mathrm{Det}^*$ as

$$\Gamma_\pm\times\mathrm{Det}^*\to\mathrm{Det}^*,\quad (h,(w,\lambda))\mapsto h(w,\lambda):=(hwa^{-1},\lambda),$$

where $h=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ is regarded as a multiplicative operator on $H=H_+\oplus H_-$. It follows from Lemma 2.2.2 that the action of the loop group on $\mathrm{Gr}^{\mathrm{an},0}_{\mathbb{C}}$ and $\mathrm{Det}^*$ is compatible with the map $\mathscr{D}$. Note that the action of $\Gamma$ on $\mathrm{Det}^*$ is not well-defined, because it is not always true that the operator $a$ is invertible.

The determinant bundle $\mathrm{Det}^*$ has a canonical holomorphic section defined by

$$\rho:\mathrm{Gr}^{\mathrm{an},0}_{\mathbb{C}}\to\mathrm{Det}^*,\quad \rho(W):=(w,\det(w_+)),$$

where $w$ is the admissible basis with respect to an admissible presentation of $W$ and $w_+$ is the plus-part of the admissible presentation. (Here one sees that this section $\rho(W)=(w,\det(w_+))$ does not depend on the choice of admissible presentations. Indeed, if $w'$ is another admissible presentation of $W$, then one has $w'=wt$ for some $t\in\mathrm{GL}_{\mathbb{N}}(\mathbb{C})$. Hence $(wt,\det(w_+t))=(wt,\det(w_+)\det(t))$ is identified with $(w,\det(w_+))$ in $\mathrm{Det}^*$.)

Now we define the tau-function. Let $W\in\mathrm{Gr}^{\mathrm{an},0}_{\mathbb{C}}$ with an admissible presentation $w:H_+\to H$. We assume that $\det(w_+)\neq 0$. Then the *tau-function* of $W$ is the holomorphic function on $\Gamma_+$ defined by

$$\tau_W(h):=\frac{\rho(hW)}{h\rho(W)}. \tag{2.3.3}$$

**Remark 2.3.6.** By definition, we have

$$\rho(hW) = (hwa^{-1}, \det(hwa^{-1})_+), \quad h\rho(W) = (hwa^{-1}, \det(w_+)).$$

Hence $\tau_W(h) = \det(hwa^{-1})_+ / \det(w_+)$. We write $h = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ for a operator $h \in \Gamma_+$ on $H_+ \oplus H_-$. Then we compute

$$\begin{aligned} \det(hwa^{-1})_+ &= \det(w_+ + a^{-1}bw_-) \\ &= \det(H_+ \xrightarrow{w} H \xrightarrow{h} H \xrightarrow{\text{proj}} H_+), \end{aligned}$$

hence the definition of the tau-function in (2.3.3) is the same in §2.2.3 up to a constant. Note that the definition of the tau-function in (2.3.3) is independent of a choice of an admissible presentation of $W$, but the definition in §2.2.3 is depend on the choice.

**Remark 2.3.7.** $\Gamma_-$ acts on the section $\rho$ linearly, hence the tau-function on $\Gamma_-$ is a constant. Indeed, we write $g = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ for $g \in \Gamma_-$. Then we have

$$\det(hwa^{-1})_+ = \det(aw_+a^{-1}) = \det(w_+),$$

hence $\rho(gW) = g\rho(W)$ for $g \in \Gamma_-$.

### 2.3.7 Action of $\Gamma_\pm$ on $\mathrm{Det}^*$

We already define the actions of $\Gamma_+$ and $\Gamma_-$ on $\mathrm{Det}^*$ in the previous subsection, however their actions do not commute. For $h \in \Gamma_+$ and $g \in \Gamma_-$, there exist unique holomorphic functions $\tilde{h} \in V_0$ and $\tilde{g} \in V_\infty$ such that $h = e^{\tilde{h}}$ and $g = e^{\tilde{g}}$, since $D_0$ and $D_\infty$ are simply connected. We define

$$c : \Gamma_- \times \Gamma_+ \to \mathbb{C}, \quad c(g,h) := \det(aa'a^{-1}(a')^{-1}),$$

if we write $h = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_+$ and $g = \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} \in \Gamma_-$. The following lemmas follow from straightforward computations.

**Lemma 2.3.8.** *For $h \in \Gamma_+$ and $g \in \Gamma_-$, we have*

$$gh\rho(W) = c(g,h)hg\rho(W)$$

**Lemma 2.3.9.** *For $h \in \Gamma_+$ and $g \in \Gamma_-$, we have*

$$c(g,h) = e^{S(\tilde{g},\tilde{h})},$$

*where $h = e^{\tilde{h}}$, $g = e^{\tilde{g}}$ as above and*

$$S(\tilde{g},\tilde{h}) := \int_{S^1} \tilde{g}'(T)\tilde{h}(T)dT.$$

### 2.3.8 Transformation formula of tau-functions

We use the same notation in §2.3.4. Let $(\mathscr{L}, \sigma) \in \mathrm{Kr}_{\mathbb{C}}^{g-1}(X, N)$ and set $W := W(\mathscr{L}, \sigma)$. (Note that $W$ also belongs to $\mathrm{Gr}_{\mathbb{C}}^{an,0}$.) Let $w = [w_+, w_-]$ be an admissible presentation of $W$ and assume that $\det(w_+) \neq 0$. Let $\Gamma_+^A$ be a subgroup of $\Gamma_+$ consisting of $k = k_A k_-$ for some $k_A \in A \cap \Gamma$ and $k_- \in \Gamma_-$ with $k_-(0) = 1$. The subgroup $\Gamma_+^A$ has a canonical map

$$a : \Gamma_+^A \to \Gamma_-, \quad k \mapsto k_-.$$

**Proposition 2.3.10.** *For $h \in \Gamma_+$, $k \in \Gamma_+^A$, we have*

$$\tau_W(hk) = \tau_W(h)\tau_W(k)c(a(k), h). \tag{2.3.4}$$

*Proof.* Note that $kW = a(k)k_A W = a(k)W$ because $k_A$ belongs to $A$. Hence we have

$$\tau(k) \cdot k\rho(W) = \rho(kW) = \rho(a(k)W) = a(k)\rho(W), \tag{2.3.5}$$

where the last equality follows from the fact that $\rho$ is $\Gamma_-$-equivariant (see Remark 2.3.7). Similarly one computes

$$\tau(hk) \cdot hk\rho(W) = \rho(hkW) = a(k)\rho(hW). \tag{2.3.6}$$

By $\rho(hW) = \tau(h) \cdot h\rho(W)$, the right hand side of (2.3.6) is $\tau(h) \cdot a(k)h\rho(W)$. If we apply Lemma 2.3.8 for $a(k)h\rho(W)$ and use (2.3.5), we have

$$\tau(h) \cdot a(k)h\rho(W) = \tau(h)\tau(k)c(a(k), h) \cdot hk\rho(W).$$

Canceling the common factor $hk\rho(W)$ in (2.3.6), we get the equation (2.3.4). □

### 2.3.9 Comparison of theta and tau functions

We keep the notation in §2.3.8. Recall that there exist the surjective maps $V_0 \twoheadrightarrow U$ and $U \twoheadrightarrow J$ (see §2.3.1 and §2.3.2). Let $K_0$ and $K$ be the kernels of the map $V_0 \twoheadrightarrow U$ and the composite map $V_0 \twoheadrightarrow U \twoheadrightarrow J$, respectively. Then it follows $K/K_0 \cong \Lambda$. The theta-function $\theta$ is regarded as a holomorphic function on $V_0$ which has functional equations with respect to $K$ in the sense of (2.3.2) and which is $K_0$-invariant. In order to compare the theta-function with the tau-function, we use two isomorphisms $V_0 \overset{f \mapsto e^f}{\to} \Gamma_+$ and $V_\infty \overset{g \mapsto e^g}{\to} \Gamma_-$. The first isomorphism induces the isomorphism $K \cong \Gamma_+^A$. We define the map $K \to V_\infty$ induced by the map $a : \Gamma_+^A \to \Gamma_-$, which, by abuse of notation, will be denoted by $a$. Note that the map $a : K \to V_\infty$ is homomorphic, and that its restriction to $K_0$ is a $\mathbb{C}$-linear mapping. Since $K$ spans $V_0$ over $\mathbb{R}$, the map $a$ is uniquely extended to an $\mathbb{R}$-linear map $a : V_0 \to V_\infty$. We write $a = a_1 + a_2$ where $a_1$ is $\mathbb{C}$-linear and $a_2$ is antilinear.

We shall regard the tau-function $\tau := \tau_W$ as a function on $V_0$ under $V_0 \cong \Gamma_+$. From Lemma 2.3.9 and Proposition 2.3.10, we have

$$\tau(f+k) = \tau(f)\tau(k)e^{S(a(k),f)}, \tag{2.3.7}$$

where $f \in V_0$ and $k \in K$. For all $f, g \in V_0$, the equation (2.3.7) implies that

$$S(a(f), g) - S(a(g), f) \in i\mathbb{R}.$$

Hence it follows $S(a_2(f), g) = \overline{S(a_2(g), f)}$. (Here the right hand side means the complex conjugation of $S(a_2(g), f)$.) We have $a_2(K_0) = 0$ since $a|_{K_0}$ is $\mathbb{C}$-linear and $a_2$ is antilinear. Therefore

$$U \times U \to \mathbb{C}, \quad (f, g) \mapsto S(a_2(f), g)$$

is a well-defined Hermitian form over $V_0/K_0 \cong U$. Moreover Segal-Wilson proved the following crucial result.

**Proposition 2.3.11** (see [29, Proposition 9.10])**.** *For $u, v \in U$, we have*

$$S(a_2(u), v) = \pi H(u, v),$$

*where $H(u, v)$ is the Hermitian form appearing in the definition of the theta-function(§2.3.1).*

Now we prove Claim 2.3.1. First we put

$$\tau_1(f) := \tau(f)e^{-\frac{1}{2}S(a_1(f),f)}$$

for $f \in V_0$. It follows from (2.3.7) that

$$\tau_1(f+k) = \tau_1(f)\tau_1(k)e^{S(a_2(k),f)}, \tag{2.3.8}$$

where $f \in V_0$ and $k \in K$. By $a_2(K_0) = 0$, $\tau_1|_{K_0}$ is a homomorphism from $K_0$ to $\mathbb{C}^*$, hence one can choose a $\mathbb{C}$-linear map $\eta : V_0 \to \mathbb{C}$ such that $\tau_1(k) = e^{\eta(k)}$ for all $k \in K_0$. Second we put

$$\tau_2(f) := \tau_1(f)e^{-\eta(f)}$$

for $f \in V_0$. It follows from (2.3.8) that

$$\tau_2(f+k) = \tau_2(f),$$

where $f \in V_0$ and $k \in K_0$, hence $\tau_2$ is a well-defined function over $V_0/K_0 \cong U$. It also follows from (2.3.8) and Proposition 2.3.11 that

$$\tau_2(u+\lambda) = \tau_2(u)\tau_2(\lambda)e^{\pi B(\lambda,u)}, \tag{2.3.9}$$

where $u \in U$ and $\lambda \in K/K_0 \cong \Lambda$. Applying Lemma 2.3.3 for (2.3.9), we have

$$\tau_2(u) = Ae^{\alpha_W(u)}\theta(u - \beta_W), \quad (u \in U),$$

for a constant $A \in \mathbb{C}$, a linear map $\alpha_W : U \to \mathbb{C}$, and some element $\beta_W \in U$. As a conclusion, we have

$$\tau_W(f) = Ae^{\alpha_W(f)+\frac{1}{2}S(b(f),f)}\theta(\bar{f} - \beta_W),$$

where $\bar{f}$ is the image of $f \in V_0$ in $U = V_0/K_0$, and the claim is proved.

# Chapter 3

# Torsion points on Jacobian varieties via Anderson's $p$-adic Sato theory

## 3.1 Geometry of a hyperelliptic curve

### 3.1.1 A Hyperelliptic Curve

Let $g > 1$ be an integer. Let $K$ be a field of characteristic zero, and assume that $K$ contains a primitive $4g$-th root $\zeta$ of unity. Let $X$ be the hyperelliptic curve given by the equation (1.0.1):

$$y^2 = x^{2g+1} + x.$$

There is an automorphism $r$ of $X$ of order $4g$ given by $r(x, y) = (\zeta^2 x, \zeta y)$. Let $G := \langle r \rangle \cong \mathbb{Z}/4g\mathbb{Z}$ be the subgroup of $\mathrm{Aut}(X)$ generated by $r$. Note that $r(\infty) = \infty$, where $\infty \in X(K)$ is the point at which the functions $x$ and $y$ have poles.

### 3.1.2 Singular Homology

In this subsection we assume $K$ is a subfield of $\mathbb{C}$. The singular homology $H_1(X(\mathbb{C}), \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $2g$ on which $G$ acts linearly. Let $\rho$ :

$G \to \mathrm{Aut}(H_1(X(\mathbb{C}), \mathbb{Z}))$ be the corresponding representation. Let $\chi : G \to \mu_{4g}$ be the character given by $\chi(r) = \zeta$.

**Lemma 3.1.1.** *The representation $\rho \otimes \mathbb{C}$ is equivalent to $\oplus_{i=1,3,\cdots,4g-1}\chi^i$. In particular, the minimal polynomial of $\rho(r)$ is $F(X) := X^{2g} + 1$.*

*Proof.* We consider a $\mathbb{C}[G]$-module $V = H^0(X, \Omega^1_{X/\mathbb{C}}) = \langle w_i = x^{i-1}dx/y \mid i = 1, \cdots, g\rangle_{\mathbb{C}}$. A direct computation shows $r^*(w_i) = \zeta^{2i-1}w_i$. The lemma follows from an isomorphism

$$H_1(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C} \cong V \oplus \mathrm{Hom}(V, \mathbb{C})$$

of $\mathbb{C}[G]$-modules. □

### 3.1.3 Good trivialization

The following is an easy consequence of Hensel's lemma:

**Lemma 3.1.2.** *There exists a unique element $u(T) \in 1 + T^{-1}\mathbb{Z}[[T^{-1}]]$ such that*

$$u(T)^{2g} - u(T)^{2g-1} + (T^{-1})^{4g} = 0. \tag{3.1.1}$$

We define two elements $x(T), y(T) \in \mathbb{Z}[[T^{-1}]][T]$ by

$$x(T) := T^2u(T), \qquad y(T) := -Tx(T)^g.$$

Note that $x(T) \equiv T^2 \mod T$ and $y(T) \equiv -T^{2g+1} \mod T^{2g}$. It follows from Lemma 3.1.2 that

$$(T^{-2}x(T))^{2g} - (T^{-2}x(T))^{2g-1} + (T^{-1})^{4g} = 0.$$

By multiplying $T^{4g}x(T)$, we get

$$y(T)^2 = x(T)^{2g+1} + x(T).$$

Therefore we can define an injection $K(X) \hookrightarrow K((T^{-1}))$ of $K$-algebras by associating $x$ and $y$ with $x(T)$ and $y(T)$ respectively. This induces an isomorphism $N_0 : \hat{\mathscr{O}}_{X,\infty} \cong K[[T^{-1}]]$, and then we can apply the results of §2.1. Note that $A := W(\mathscr{O}_X, N)$ is the $K$-subalgebra of $K((T^{-1}))$ generated by $x(T)$ and $y(T)$.

### 3.1.4 Admissible basis of $A$

We construct a basis $\{w_i\}$ of $A$ such that

1. $w_i \in \mathbb{Z}[[T^{-1}]][T]$ for all $i$,
2. $w_i - T^{2i-2} \in T^{2i-3}\mathbb{Z}[[T^{-1}]]$ for all $i \leq g+1$, and
3. $w_i - T^{i-1+g} \in T^{2g}\mathbb{Z}[[T^{-1}]]$ for all $i \geq g+2$.

In particular, $\{w_i\}$ is admissible in the sense of §2.1.2. First we put

$$u_i = \begin{cases} x(T)^{i-1} & (1 \leq i \leq g), \\ x(T)^{g+(i-g-1)/2} & (i > g,\ i \not\equiv g \mod 2), \\ -y(T)x(T)^{(i-g-2)/2} & (i > g,\ i \equiv g \mod 2). \end{cases}$$

Note that $u_i \in \mathbb{Z}[[T^{-1}]][T]$ for all $i$ and $\{u_i\}$ is a $K$-basis of $A$. We set $w_i = u_i$ for $i \leq g+1$. Suppose we have constructed $w_1, \cdots, w_{i-1}$ for some $i \geq g+2$. There exists $\delta \in \langle w_1, \cdots, w_{i-1}\rangle_{\mathbb{Z}}$ such that $u_i - T^{i-1+g} - \delta \in T^{2g}\mathbb{Z}[[T^{-1}]]$. We then set $w_i := u_i - \delta$. Note that the partition of $A$ is

$$(g, g-1, \cdots, 2, 1, 0, 0, \cdots),$$

and its length is $g$.

### 3.1.5 Two-torsion points

Let $J[2]$ be the two-torsion subgroup in the Jacobian variety $J$ of $X$. For any $\mathscr{L} \in J[2]$, we shall construct an $N$-trivialization $\sigma$ of $\mathscr{L}$ such that $W = W(\mathscr{L}, \sigma)$ admits an admissible basis $\{w_i\}$ satisfying $w_i \in \mathbb{Z}[[T^{-1}]][T]$ for all $i$.

Recall that the Weierstrass points on $X$ are

$$\infty,\ P_0 = (0,0),\ \text{and } P_i = (\zeta^{2i-1}, 0) \quad (1 \leq i \leq 2g).$$

It is proved in [23, Chapter III, §2] that the two-torsion group $J[2]$ of $J$ consists of line bundles associated to Weil divisors

$$D_I := \sum_{i \in I}(P_i - \infty), \quad I \subset \{0, 1, \cdots, 2g\},\ |I| \leq g.$$

For a subset $I \subset \{0, 1, \cdots, 2g\}$ such that $|I| = s \leq g$, we get a Krichever pair $(\mathscr{L}_I, \sigma_I) := (\mathscr{O}_X(D_I), \sigma(D_I))$ by the construction in §2.1.5. We further set $L_I := W(\mathscr{L}_I, \sigma_I)$.

We construct a basis $\{w_{I,i}\}_{i=1}^{\infty}$ of $L_I$ as follows: define an element $f_I$ of $H^0(X \setminus \{\infty\}, \mathscr{L}_I) \subset K(x,y)$ by

$$f_I := y \prod_{j \in I} (x - x(P_j))^{-1}.$$

Note that the divisor of $f_I$ satisfies

$$\mathrm{div}(f_I) = \sum_{j \notin I} P_j - \sum_{j \in I} P_j - (2g - 2s + 1)\infty.$$

Now we define for $1 \leq i \leq g - s$,

$$u_{I,i} := T^s x(T)^{i-1}$$

and for $1 \leq i$,

$$u_{I,g-s+i} = \begin{cases} T^s x(T)^{g-s+(i-1)/2} & (i : \text{odd}) \\ T^s f_I(T) x(T)^{(i-2)/2} & (i : \text{even}), \end{cases}$$

where $f_I(T)$ is the image of $f_I$ by the embedding $N^* : K(x,y) \hookrightarrow K((T^{-1}))$. One sees that

$$\deg(u_{I,i}) = \begin{cases} 2i - 2 + s & (1 \leq i \leq g - s) \\ i + g - 1 & (g - s < i). \end{cases}$$

Therefore $\{u_{I,i}\}_{i=1}^{\infty}$ is a $K$-basis of $L_I$ such that $u_{I,i} \in \mathbb{Z}[[T^{-1}]][T]$ for all $i$. Now we can produce an admissible basis $\{w_{I,i}\}$ of $L_I$ with required properties by the same procedure as §3.1.4. Note that the partition of $L_I$ is

$$(g - s, g - s - 1, \cdots, 2, 1, 0, 0, \cdots),$$

and the length of the partition is $g - s$.

### 3.1.6 Points of degree one

We fix a non-Weierstrass point $Q \in X(K)$. Let $(\mathscr{L}_Q, \sigma_Q)$ be the Krichever pair associated to the Weil divisor $Q - \infty$ under the construction in §2.1.5. We are going to construct an admissible basis $\{w_{Q,i}\}$ of $L_Q := W(\mathscr{L}_Q, \sigma_Q)$ satisfying $w_{Q,i} \in \mathbb{Z}[x(Q), y(Q)][[T^{-1}]][T]$ for all $i$.

We define a function $f_Q \in H^0(X \setminus \{\infty\}, \mathscr{L}_Q) \subset K(x,y)$:

$$f_Q := l_Q \cdot (x - x(Q))^{-1} \qquad l_Q := y - x + y(Q) + x(Q).$$

A straightforward computation shows that $\mathrm{div}(f_Q)+Q+(2g-1)\infty$ is an effective divisor of degree $2g$. We construct a basis $\{u_{Q,i}\}_{i=1}^{\infty}$ of $L_Q$ as follows: for $1 \leq i \leq g$,

$$u_{Q,i} := Tx(T)^{i-1}$$

for $1 \leq i$,

$$u_{Q,g+i} := \begin{cases} Tf_Q(T)x(T)^{(i-1)/2} & (i : \text{odd}) \\ Tx(T)^{g+(i-2)/2} & (i : \text{even}), \end{cases}$$

where $f_Q(T)$ is the image of $f_Q$ in $K((T^{-1}))$ by the embedding $N^*$. One sees that

$$\deg(u_{Q,i}) = \begin{cases} 2i-1 & (1 \leq i \leq g) \\ i+g-1 & (g < i). \end{cases}$$

Therefore $\{u_{Q,i}\}$ is a $K$-basis of $L_Q$ such that $u_{Q,i} \in \mathbb{Z}[x(Q), y(Q)][[T^{-1}]][T]$ for all $i \geq 1$. Now we can produce an admissible basis $\{w_{Q,i}\}$ of $L_Q$ with required properties by the same procedure as §3.1.4. Note that the partition of $L_Q$ is

$$(g-1, g-2, \cdots, 1, 0, 0, \cdots),$$

and its length is $g-1$.

### 3.1.7 Action of $G$ on $\mathrm{Kr}(X, N)$

We define a $K$-algebra automorphism $\bar{r}$ on $K((T^{-1}))$ by

$$\bar{r}\left(\sum_i a_i T^i\right) := \sum_i a_i (\zeta T)^i.$$

Then the diagram

$$\begin{array}{ccc} \mathrm{Spec}\, K((T^{-1})) & \xrightarrow{N} & X \\ \downarrow{\scriptstyle \bar{r}} & & \downarrow{\scriptstyle r} \\ \mathrm{Spec}\, K((T^{-1})) & \xrightarrow{N} & X. \end{array}$$

commutes. By §2.1.10, we get an induced action of $G$ on $\mathrm{Kr}(X, N)$. It holds that $W(r(\mathscr{L}, \sigma)) = \bar{r}(W(\mathscr{L}, \sigma))(:= \{\bar{r}(w) \mid w \in W(\mathscr{L}, \sigma)\})$.

### 3.1.8 Remark on the simplicity of Jacobian

[1] (The result of this subsection will not be used in the sequel.) We suppose $K$ is an algebraically closed field. We deduce from a result of Aoki [3] that the Jacobian

[1] This remark is communicated to us by Noriyuki Otsubo.

variety of $X$ is simple as an abelian variety, at least when $g > 45$. To see this, let $C'$ be the smooth projective curve over $K$ defined by $s^{4g} = t(1-t)$. There exists a degree two map $\pi : C' \to C$ given by $(s,t) \mapsto (c^2t^2, c(2s-1)t)$, where $c = (-4)^{1/4g}$. Aoki's result [3] shows that the Jacobian variety of $C'$ has exactly two simple factors, provided $g > 45$. The existence of $\pi$ shows that the Jacobian variety of $X$ must be one of two simple factors.

## 3.2 Proof of main theorems

We keep the notation and assumption in §3.1. Let $p$ be a prime number such that

$$p \equiv 1 \mod 4g.$$

We further assume that $K$ is a finite extension of $\mathbb{Q}_p$ that contains $(p-1)$-st roots of all integers. Note that $\zeta \in K$.

### 3.2.1 $p$-torsion of the Jacobian

We fix an embedding $\mathbb{Q}(\zeta) \subset \mathbb{Q}_p$, so that we get a prime ideal $\wp := \mathbb{Z}[\zeta] \cap p\mathbb{Z}_p$ of $\mathbb{Z}[\zeta]$ over $p$. Note that $\mathbb{F}_p$ contains all the $4g$-th roots of unity. Put $\bar{\zeta} := \zeta \mod \wp \in \mathbb{F}_p$. Let $J$ be the Jacobian variety of $X$ and $J[p]$ the $p$-torsion subgroup of $J$. Choosing an embedding $K \subset \mathbb{C}$, we get an isomorphism $J[p] \cong H_1(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{F}_p$. The representation $\rho_p : G \to \mathrm{Aut}(J[p])$ is thus equivalent to $\rho \otimes \mathbb{F}_p$. Therefore Lemma 3.1.1 implies the following:

**Lemma 3.2.1.** *The minimal polynomial of $\rho_p(r)$ is*

$$F(X) \mod p = \prod_{i=1,3,\cdots,4g-1} (X - \bar{\zeta}^i).$$

*Consequently, we have*

$$J[p] = \bigoplus_{i=1,3,\cdots,4g-1} J[p]^{\chi^i}, \quad \dim_{\mathbb{F}_p} J[p]^{\chi^i} = 1 \ \ (i = 1, 3, \cdots, 4g-1).$$

*Here, by abuse of notation, we write $\chi^i$ for the composition $G \xrightarrow{\chi^i} \mu_{4g} \hookrightarrow \mathbb{Z}_p^* \overset{\mathrm{mod}\ p}{\twoheadrightarrow} \mathbb{F}_p^*$.*

**Remark 3.2.2.** If we take a different choice for the embedding $\mathbb{Q}(\zeta) \subset \mathbb{Q}_p$, then the characters $\chi^i$ are replaced by $\chi^{ij}$ for some $j \in (\mathbb{Z}/4g\mathbb{Z})^\times$. By using all such embeddings, proofs of Theorems 1.0.1 and 1.0.2 are reduced to the case $i = 1$.

### 3.2.2 An auxiliary lemma

**Lemma 3.2.3.** *We have an equation*

$$T^p - e_0 T = a(T) + g(T) \tag{3.2.1}$$

*for some $e_0 \in \mathbb{Z}_{(p)}^*$, $a(T) \in A \cap \mathbb{Z}[[T^{-1}]][T]$ and $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$.*

*Proof.* Setting $p = 4gp' + 1$, we write

$$x^{2gp'}(1 + x^{-2g})^{2gp'} = e_+(x) + e_0 + e_-(x)$$

where $e_\pm(x) \in x^{\pm 2g}\mathbb{Z}[x^{\pm 2g}]$ and $e_0 \in \mathbb{Z}$. Note that $e_0 = \binom{2gp'}{p'}$ is a $p$-adic unit. We compute

$$\begin{aligned} e_+(x) + e_0 + e_-(x) = x^{2gp'}(1 + x^{-2g})^{2gp'} &= (x + x^{1-2g})^{2gp'} \\ &= \left(\frac{x^{2g+1} + x}{x^{2g}}\right)^{2gp'} = \left(\frac{y^2}{x^{2g}}\right)^{2gp'} = \left(\frac{-y}{x^g}\right)^{p-1}. \end{aligned}$$

Recalling $y(T) = -Tx(T)^g$, we get an equation in $K((T^{-1}))$

$$T^p - e_0 T = a(T) + g(T)$$

where $a(T) := -y(T)e_+(x(T))/x(T)^g$ and $g(T) := Te_-(x(T))$. Observe that $a(T)$ is in the image of $A = K[x, y]$ in $K((T^{-1}))$ (since $e_+(x) \in x^{2g}\mathbb{Z}[x]$) and that $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$. □

### 3.2.3 Decomposition of a Dwork loop

The result of §3.1.4 shows that $(\mathscr{O}_X, N) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$ (cf. §). Recall that $\bar{A} := \bar{W}(\mathscr{O}_X, N)$ is the closure of $A = W(\mathscr{O}_X, N)$ in $H(K)$. Let $\pi$ and $\varepsilon_0$ be $(p-1)$-st roots of $-p$ and $1/e_0$ respectively, where $e_0 \in \mathbb{Z}_{(p)}^*$ is the number appearing in Lemma 3.2.3. (They belong to $K$ by the assumption made at the beginning of this section.) For $0 \le i \le p-2$, we define a Dwork loop

$$\begin{aligned} h^{(i)}(T) &:= \exp(\pi((\zeta_{p-1}^i \varepsilon_0 T) - (\zeta_{p-1}^i \varepsilon_0 T)^p)) \\ &= \exp(-\pi \zeta_{p-1}^i \varepsilon_0^p (T^p - e_0 T)), \end{aligned}$$

where $\zeta_{p-1} := \zeta^{4g/(p-1)}$ is a $(p-1)$-st root of unity. We take a positive integer $s$ such that

$$\zeta + s \equiv 0 \mod \wp.$$

Recall that we have defined an automorphism $\bar{r}$ of $H(K)$ in §3.1.7 by

$$\bar{r}(h(T)) = h(\zeta T).$$

**Proposition 3.2.4.** *1. For all $0 \le i \le p-2$, there exist $h_A^{(i)}, h_A^{'(i)} \in \bar{A} \cap \Gamma(K)$ and $h_-^{(i)}, h_-^{'(i)} \in \Gamma_-(K)$ such that*

$$(h^{(i)})^p = h_A^{(i)} h_-^{(i)}, \qquad \bar{r}(h^{(i)})(h^{(i)})^s = h_A^{'(i)} h_-^{'(i)}.$$

2. *Let* $0 \leq i < j \leq p-2$*, and choose a positive integer* $t$ *such that* $\zeta_{p-1}^{j-i} \equiv t (\not\equiv 1) \mod \wp$*. Then, there exist* $k_A^{(ij)} \in \bar{A} \cap \Gamma(K)$ *and* $k_-^{(ij)} \in \Gamma_-(K)$ *such that*

$$h^{(j)}(h^{(i)})^{-t} = k_A^{(ij)} k_-^{(ij)}.$$

*Proof.* (1) We may suppose $i = 0$ and will omit the suffix $^{(i)}$, so that $h(T) = h^{(0)}(T)$ for instance. From the equation (3.2.1), we have

$$\begin{aligned} h(T)^p &= \exp(-p\pi\varepsilon_0^p(T^p - e_0 T)) \\ &= \exp(-p\pi\varepsilon_0^p a(T)) \cdot \exp(-p\pi\varepsilon_0^p g(T)). \end{aligned}$$

Since $a(T) \in A \cap \mathbb{Z}[[T^{-1}]][T]$ and $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$, we have

$$\begin{aligned} h_A &:= \exp(-p\pi\varepsilon_0^p a(T)) \in \bar{A} \cap \Gamma(K) \\ h_- &:= \exp(-p\pi\varepsilon_0^p g(T)) \in \Gamma_-(K), \end{aligned}$$

hence the first claim is proved.

From the equation (3.2.1) and $\zeta^p = \zeta$, we compute

$$\begin{aligned} h(\zeta T)h(T)^s &= \exp(-(\zeta + s)\pi\varepsilon_0^p(T^p - e_0 T)) \\ &= \exp(-(\zeta + s)\pi\varepsilon_0^p a(T)) \cdot \exp(-(\zeta + s)\pi\varepsilon_0^p g(T)). \end{aligned}$$

By the assumption $\zeta + s \equiv 0 \mod \wp$, we have

$$\begin{aligned} h'_A(T) &:= \exp(-(\zeta + s)\pi\varepsilon_0^p a(T)) \in \bar{A} \cap \Gamma(K) \\ h'_-(T) &:= \exp(-(\zeta + s)\pi\varepsilon_0^p g(T)) \in \Gamma_-(K), \end{aligned}$$

and we are done.

(2) Put $\delta = \zeta_{p-1}^{j-i} - t \in \wp$. Then we have

$$h^{(j)}(h^{(i)})^{-t} = \exp(-\pi\delta\zeta_{p-1}^i \varepsilon_0^p(T^p - e_0 T)).$$

The rest of the proof is the same as (1). □

### 3.2.4 Construction of $p$-torsion elements

Recall that we have constructed Dwork loops $h^{(i)}$ in §3.2.3.

**Proposition 3.2.5.** 1. *We have* $\{[h^{(i)}(\mathscr{O}_X, N)] \mid 0 \leq i \leq p-2\} = J[p]^\chi \setminus \{0\}$.

2. *We have* $J[p]^\chi \cap \Theta = \{0\}$.

*Proof.* We fix $i$ and put $h = h^{(i)}$, $(\mathscr{L}, \sigma) := h(\mathscr{O}_X, N) \in \mathrm{Kr}(X, N)$. We first show $\mathscr{L} \in J \setminus \Theta$. By Proposition 2.2.8 (1), we have $\deg(\mathscr{L}) = 0$. The result of §3.1.4 shows that $(\mathscr{O}_X, N) \in \mathrm{Kr}^0_{\mathrm{an}}(X, N)$ satisfies the assumptions (A1) and (A2) of Theorem 2.2.9. It follows that $\mathscr{L} \notin \Theta$. In particular we get $\mathscr{L} \neq 0$.

In order to prove $\mathscr{L} \in J[p]^\chi$, it suffices to show $\mathscr{L}^{\otimes p} = r^*\mathscr{L} \otimes \mathscr{L}^{\otimes s} = \mathscr{O}_X$, where $s \in \mathbb{Z}$ is the integer used in Proposition 3.2.4. For $K$-subspaces $V_1, \cdots, V_m$ of $H(K)$, we write $V_1 \cdot \ldots \cdot V_m$ for the $K$-span of $\{\prod_{j=1}^m u_j \mid u_j \in V_j\}$. When $V = V_1 = \cdots = V_m$ we write $V^m := V \cdot \ldots \cdot V$. Let $V = \bar{W}(\mathscr{L}, \sigma)$. Proposition 2.2.8 shows that $V = h\bar{A}$. Thus $V^p = h^p\bar{A}$. By Proposition 2.2.7 and §2.1.7, we have $(\mathscr{L}, \sigma)^{\otimes p} = h^p(\mathscr{O}_X, N)$. Propositions 3.2.4 (1) and 2.2.8 show $[h^p(\mathscr{O}_X, N)] = [(\mathscr{O}_X, N)]$. We conclude $\mathscr{L}^{\otimes p} = \mathscr{O}_X$. Similarly, we have $r^*(V) \cdot V^s = \bar{r}(h)h^s\bar{A}$. By Proposition 2.2.7 and §2.1.7, we have $r^*(\mathscr{L}, \sigma) \otimes (\mathscr{L}, \sigma)^{\otimes s} = \bar{r}(h)h^s(\mathscr{O}_X, N)$. Now Propositions 3.2.4 (1) and 2.2.8 show $[\bar{r}(h)h^s(\mathscr{O}_X, N)] = [(\mathscr{O}_X, N)]$. We conclude $r^*(\mathscr{L}) \otimes \mathscr{L}^{\otimes s} = \mathscr{O}_X$.

It remains to show $[h^{(i)}(\mathscr{O}_X, N)] \neq [h^{(j)}(\mathscr{O}_X, N)]$ for $0 \leq i < j \leq p-2$. Propositions 3.2.4 (2) and 2.2.8 show that $[h^{(j)}(\mathscr{O}_X, N)] = [h^{(i)}(\mathscr{O}_X, N)^{\otimes t}]$ for some integer $t \not\equiv 1 \mod p$. Since we have already seen that $[h^{(i)}(\mathscr{O}_X, N)]$ is a non-trivial element of $J[p]$, this completes the proof. □

### 3.2.5 Proof of Theorem 1.0.1

We may suppose $K$ is a finite extension of $\mathbb{Q}_p$ satisfying the conditions stated at the beginning of this section. By Remark 3.2.2, we may also assume $i = 1$. Take $\mathscr{L} \in J[2]$ and $\mathscr{L}' \in J[p]^\chi \setminus \{0\}$. We need to show $\mathscr{L} \otimes \mathscr{L}' \notin \Theta$. By Proposition 3.2.5, there exists a Dwork loop $h$ such that $\mathscr{L}' = [h(\mathscr{O}_X, N)]$. By §3.1.5, there exists an $N$-trivialization $\sigma$ of $\mathscr{L}$ such that $W(\mathscr{L}, \sigma)$ admits an admissible basis $\{w_i\}$ satisfying $w_i \in \mathbb{Z}[[T^{-1}]][T]$ for all $i$. Hence $(\mathscr{L}, \sigma)$ belongs to $\mathrm{Kr}^0_{\mathrm{an}}(X, N)$ and satisfies the assumptions (A1) and (A2) of Theorem 2.2.9. It follows that $[h(\mathscr{L}, \sigma)] \notin \Theta$. By Propositions 2.2.7, 2.2.8 and §2.1.7, we have $[h(\mathscr{L}, \sigma)] = [(\mathscr{L}, \sigma)] \otimes [h(\mathscr{O}_X, N)] = \mathscr{L} \otimes \mathscr{L}'$.

### 3.2.6 Proof of Theorem 1.0.2

We may assume $Q$ is a non-Weierstrass point by Theorem 1.0.1. Then the same proof as the previous subsection works if we put §3.1.6 in the place of §3.1.5.

## 3.3 Geometry of a Fermat quotient

### 3.3.1 A Fermat quotient

Let $l$ be an odd prime number. Let $K$ be a field of characteristic zero that $K$ contains a primitive $l$-th root $\zeta_l$ of unity. Fix integers $a \geq b > 1$ such that $l + 1 = a + b$. Let $X$ be the smooth projective curve defined by

$$y^l = x^a(1-x)^b,$$

which is obtained as a cyclic quotient of a Fermat curve of degree $l$ (see, for example [3, 15, 19]). Note that the genus $g$ of $X$ is $(l-1)/2$. There is an automorphism $\gamma$ of $X$ of order $l$ defined by $\gamma(x, y) = (x, \zeta_l y)$. Let $\infty \in X(K)$ be the unique point at which the coordinate functions $x$ and $y$ have poles.

**Lemma 3.3.1.** *The Jacobian variety $J$ of $X$ has the structure of $\mathbb{Z}[\zeta_l]$-module such that $\zeta_l$ acts by $\gamma$.*

*Proof.* It suffices to show it when $K$ is an algebraically closed field. Since the Jacobian variety $J$ is generated by sheaves of the form $\mathscr{O}_X(P-\infty)$ $(P \in X(K))$, it suffices to show that the action of $F(\gamma)$ on $\mathscr{O}_X(P-\infty)$ for each $P \in X(K)$ vanishes, where $F(X) := X^{l-1} + X^{l-2} + \cdots + X + 1$ is the minimal polynomial of $\zeta_l$. Let $P := (x_0, y_0)$ be a closed point of $X$ and put $\mathscr{L} = \mathscr{O}_X(P-\infty)$. Then we compute

$$\begin{aligned} F(\gamma)\mathscr{L} &\cong \mathscr{O}_X(\gamma^{l-1}P + \gamma^{l-2}P + \cdots + \gamma P + P - l\infty) \\ &\cong \mathscr{O}_X(\mathrm{div}(x - x_0)) \\ &\cong \mathscr{O}_X. \end{aligned}$$

Hence $J$ has the $\mathbb{Z}[\zeta_l]$-module structure induced by $\gamma$. □

### 3.3.2 $\mathfrak{a}$-torsion subgroup

In this subsection we assume that $K$ is a subfield of $\mathbb{C}$. From Lemma 3.3.1, $J$ has complex multiplication by $\mathbb{Z}[\zeta_l]$. For an ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta_l]$, we write $J[\mathfrak{a}]$ for the $\mathfrak{a}$-torsion subgroup of $J(\mathbb{C})$.

**Lemma 3.3.2.** *For a prime ideal $\wp \subset \mathbb{Z}[\zeta_l]$, the order of $J[\wp]$ is $N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\wp)$.*

*Proof.* First we assume that $\wp = (p)$ for a prime number $p \in \mathbb{Z}$. Since $J(\mathbb{C})$ is isomorphic to $\mathbb{C}^g/\Omega\mathbb{Z}^{2g}$ for a suitable matrix $\Omega \in M_n(\mathbb{C})$, we have

$$|J[p]| = |p^{2g}| = |p^{l-1}| = N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(p).$$

We next assume that $\wp$ divides $p$ where $p$ is a prime number ($\neq l$). We set $(p) = \wp_1\wp_2\cdots\wp_f$ for prime ideals $\wp_1$ ($:= \wp$), $\wp_2$, …, $\wp_f$. As a consequence of the Chinese remainder theorem, we have

$$J[p] = \bigoplus_{i=1}^{f} J[\wp_i].$$

Since $J[\wp_i]$ are conjugate, the order of $J[\wp_i]$ is the same for all $i$. Hence we have $p^{l-1} = p^{2g} = |J[\wp]|^f$. Therefore we have

$$|J[\wp]| = p^{\frac{l-1}{f}} = N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\wp).$$

We finally assume that $\wp$ divides $l$, that is, $\wp = (1-\zeta_l)$. Then

$$l^{l-1} = l^{2g} = |J[l]| = |J[(1-\zeta_l)^{l-1}]| = |J[(1-\zeta_l)]|^{l-1}.$$

Hence we have

$$J[(1-\zeta_l)] = l = N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(1-\zeta_l).$$

□

### 3.3.3 Good trivialization for a Fermat quotient

The following is proved in a similar way as §3.1.3.

**Lemma 3.3.3.** *There exists a unique $\phi(T) \in T\mathbb{Z}[[T]]$ such that*

$$(-1)^b\phi(T)(1-\phi(T))^{-b} = T.$$

We put

$$x(T) := \frac{1}{\phi(T^{-l})}, \quad y(T) := \frac{T}{\phi(T^{-l})}.$$

Note that $x(T), y(T) \in \mathbb{Z}[[T^{-1}]][T]$, and that $x(T) \equiv T^l \bmod T^{l-1}$ and $y(T) \equiv T^{l+1} \bmod T^l$ (up to a sign), respectively. By Lemma 3.3.3, we have the equation

$$(-1)^b\phi(T^{-l})(1-\phi(T^{-l}))^{-b} = T^{-l}.$$

By multiplying $(-1)^{-b}T^l(1-\phi(T^{-l}))^b\phi(T^{-l})^{-(l+1)}$, we get

$$y(T)^l = x(T)^a(1-x(T))^b.$$

One can define an injection $K(X) \hookrightarrow K((T^{-1}))$ of $K$-algebras by associating $x$ and $y$ with $x(T)$ and $y(T)$ respectively. The isomorphism $N_0 : \hat{\mathscr{O}}_{X,\infty} \cong K[[T^{-1}]]$ induced by this injection defines the morphism of $K$-schemes

$$N : \operatorname{Spec} K((T^{-1})) \to X.$$

Therefore we can apply the results of §2.1.

### 3.3.4 $(1-\zeta_l)$-torsion points and admissible basis

From §3.3.2, we may assume that the $(1-\zeta_l)$-torsion subgroup $J[(1-\zeta_l)]$ of $J$ is a cyclic group of order $l$. Let $P_0$ (resp. $P_1$) be the unique point of $X$ at which $x$ takes the value 0 (resp. 1). Then the line bundle $\mathscr{L} := \mathscr{O}_X(P_0 - P_1)$ satisfies $\gamma^*\mathscr{L} \cong \mathscr{L}$ which is non-trivial. Therefore $\mathscr{L}$ belongs to $J[(1-\zeta_l)]$ and generates this torsion subgroup. We shall construct an admissible basis $\{w_{ij}\}_{i=1}^{\infty}$ of $L_j := W(\mathscr{L}^{\otimes j}, N)$ for each $j = 0, 1, 2, \ldots, l-1$ satisfying $w_{ij} \in \mathbb{Z}[[T^{-1}]][T]$ for all $i$. (Here $L_0 := A = W(\mathscr{O}_X, N)$ and $\mathscr{L}^{\otimes j} = \mathscr{O}_X(j(P_0) - j(P_1))$.)

Fix $0 \leq j \leq l-1$. For an integer $i \geq 0$, we define elements of $K(X)$:

$$v_{ij} := y^i x^{a_{ij}} (1-x)^{b_{ij}},$$

where

$$a_{ij} := -\left\lfloor \frac{ia+j}{l} \right\rfloor + \left\lfloor \frac{i}{l} \right\rfloor, \quad b_{ij} := -\left\lfloor \frac{ib-j}{l} \right\rfloor,$$

and $\lfloor \cdot \rfloor$ is the floor function (which takes the greatest integer). Let $\{\cdot\}$ be the fractional part function defined by

$$\{s\} := s - \lfloor s \rfloor \quad (s \in \mathbb{R}).$$

(Hence the fractional part function takes values in the interval $[0, 1)$.) Then we have

$$\begin{aligned}
\mathrm{ord}_{P_0}(v_{ij}) &= i\,\mathrm{ord}_{P_0}(y) + a_{ij}\,\mathrm{ord}_{P_0}(x) = -j + l\left\{\frac{ia+j}{l}\right\} + l\left\lfloor \frac{i}{l} \right\rfloor, \\
\mathrm{ord}_{P_1}(v_{ij}) &= i\,\mathrm{ord}_{P_1}(y) + b_{ij}\,\mathrm{ord}_{P_1}(1-x) = j + l\left\{\frac{ib-j}{l}\right\}.
\end{aligned}$$

They mean that $v_{ij}$ is a function with poles of order at most $j$ at $P_0$ and zeros of order at least $j$ at $P_1$. Hence $v_{ij}$ is a global section of $\mathscr{L}^{\otimes j}$. We also have

$$\mathrm{ord}_{\infty}(v_{ij}) = -i - l\left\{\frac{ia+j}{l}\right\} - l\left\{\frac{ib-j}{l}\right\} + l\left\{\frac{i}{l}\right\}.$$

Let $u_{ij}$ be the image of $v_{ij}$ in $K((T^{-1}))$ by the embedding $N^*$. Then we have

$$\deg(u_{ij}) = i + \Psi(i,j)l,$$

where

$$\Psi(i,j) := \left\{\frac{ia+j}{l}\right\} + \left\{\frac{ib-j}{l}\right\} - \left\{\frac{i}{l}\right\}.$$

**Lemma 3.3.4.** *For all $i$, we have*

$$\Psi(i,j) = \Psi(i+l,j) \quad \textit{and} \quad \Psi(i,j) \in \{0,1\}.$$

*Proof.* The first assertion follows from the property of fractional part functions that $\{(c+l)/l\} = \{c/l\}$ for a real number $c$. From the first assertion, a proof of the second assertion is reduced to the case that $0 \leq i \leq l-1$. Assume that $0 \leq i \leq l-1$ (hence we may assume $\{i/l\} = i/l$), and that $ib - j \geq 0$. Recalling that the integers $a$ and $b$ satisfy the condition $a + b = l + 1$, we have

$$\Psi(i,j) = i - \left\lfloor \frac{ia+j}{l} \right\rfloor - \left\lfloor \frac{ib-j}{l} \right\rfloor \in \mathbb{Z}.$$

From the property of floor functions that

$$c - \frac{l-1}{l} \leq \left\lfloor \frac{c}{l} \right\rfloor \leq \frac{c}{l}$$

with $c \geq 0$, it follows that

$$i \cdot \frac{l+1}{l} - 2 \cdot \frac{l-1}{l} \leq \left\lfloor \frac{ia+j}{l} \right\rfloor + \left\lfloor \frac{ib-j}{l} \right\rfloor \leq i \cdot \frac{l+1}{l}.$$

Therefore we have $-1 < \Psi(i,j) < 2$. Since $\Psi(i,j) \in \mathbb{Z}$, we get $\Psi(i,j) \in \{0,1\}$. Similarly, one can also show in the case that $ib - j < 0$. □

This lemma implies that $\{u_{ij}\}_{i=0}^{\infty}$ is $K$-linearly independent. To make sure that $\{u_{ij}\}_{i=0}^{\infty}$ gives a $K$-basis of $L_j$, we need to show that the cardinality of the set $\{i \mid \deg(u_{ij}) \leq l-1\}$ is precisely $g+1$. (Recall that the Riemann-Roch theorem implies that $\dim H^0(X, \mathscr{L}_l((l-1)\infty))) = 2g - g + 1 = g + 1$.) This claim is proved by the following.

**Lemma 3.3.5.** *We have*

$$\sum_{i=0}^{l-1} \Psi(i,j) = g.$$

*Proof.* Since $a$ is relatively prime to $l$, we have

$$\sum_{i=0}^{l-1} \left\{ \frac{ia+j}{l} \right\} = \frac{l-1}{2} = g.$$

Similarly we have

$$\sum_{i=0}^{l-1} \left\{ \frac{ib-j}{l} \right\} = \sum_{i=0}^{l-1} \left\{ \frac{i}{l} \right\} = \frac{l-1}{2} = g.$$

From the definition of $\Psi(i,j)$, we are done. □

We define the set $S := \{\deg u_{ij} \mid i \geq 0\}$ and its subset

$$S_0 := \{\deg u_{ij} \mid \Psi(i,j) = 0 \quad \text{and} \quad 0 \leq i \leq l-1\}.$$

For all $s \in S_0$, we have $s \leq l-1$, and by Lemma 3.3.5, $\#S_0 = g+1$. If we define $S_1 := \{s \in S \mid s \geq l\}$, then $S_1$ coincides with $\mathbb{N}_{\geq l}$ and $S_0 \cup S_1 = S$. Hence the $K$-subspace of $K((T^{-1}))$ spanned by $\{u_{ij}\}_{i=0}^{\infty}$ belongs to $\mathrm{Gr}^{alg}(K)$ of index $1-g$, hence coincides with $L_j$. We can also produce an admissible basis $\{w_{ij}\}_{i=1}^{\infty}$ of $L_j$ with required properties from $\{u_{ij}\}_{i=0}^{\infty}$ by the same procedure as §3.1.4, since $u_{ij}$ is monic up to a sign and belongs to $\mathbb{Z}[[T^{-1}]][T]$ for all $i, j$.

To consider the partition of $L_j$, we arrange the set $S_0$ in ascending order as

$$S_0 = \{s_1, s_2, \ldots, s_{g+1}\},$$

where

$$0 \leq s_1 \leq s_2 \leq \cdots \leq s_{g+1} \leq l-1.$$

**Lemma 3.3.6.** *We have $\Psi(l-1, j) = 0$. Consequently, we have*

$$s_{g+1} = l-1.$$

*Proof.* We have

$$\sum_{j=0}^{l-1} \Psi(l-1,j) = \frac{l-1}{2} + \frac{l-1}{2} - l\left\{\frac{l-1}{l}\right\} = 0.$$

Since $\Psi(l-1,j) \in \{0,1\}$, we conclude $\Psi(l-1,j) = 0$ for all $0 \leq j \leq l-1$ . □

Let $\kappa^{(j)} := (\kappa_i^{(j)})_{i=1}^{\infty}$ be the partition of $L_j$. For $1 \leq i \leq g+1$, $\kappa_i^{(j)}$ is defined by

$$\kappa_i^{(j)} = i - (1-g) - s_i.$$

(Here, by definition, $\kappa_i^{(j)} = 0$ for all $i > g+1$.) Lemma 3.3.6 implies that

$$\kappa_{g+1}^{(j)} = 0.$$

Hence it follows $\ell(\kappa^{(j)}) \leq g$, where $\ell(\kappa^{(j)})$ is the length of the partition $\kappa^{(j)}$. Moreover we have $\kappa_1^{(j)} \leq g$ (since $s_1 \geq 0$). Hence it follows

$$\max\{\kappa_1^{(j)}, \ell(\kappa^{(j)})\} \leq g.$$

### 3.3.5 Action of $\gamma$ on $\mathrm{Kr}(X, N)$

We define a $K$-algebra automorphism $\bar{\gamma}$ on $K((T^{-1}))$ (similarly as §3.1.7) by

$$\bar{\gamma}\left(\sum_i a_i T^i\right) := \sum_i a_i (\zeta_l T)^i.$$

Then the diagram

$$\begin{array}{ccc} \operatorname{Spec} K((T^{-1})) & \xrightarrow{N} & X \\ \downarrow{\scriptstyle \bar{\gamma}} & & \downarrow{\scriptstyle \gamma} \\ \operatorname{Spec} K((T^{-1})) & \xrightarrow{N} & X. \end{array}$$

commutes. By §2.1.10, we get an induced action of $\gamma$ on $\mathrm{Kr}(X, N)$, and it holds that $W(\gamma(\mathscr{L}, \sigma)) = \bar{\gamma}(W(\mathscr{L}, \sigma))$.

## 3.4 Proof of Anderson's result

We use the notation and assumption in §3.3. Let $p$ be a prime number such that

$$p \equiv 1 \bmod l.$$

Since $l$ is odd, we have $p \geq 2l+1 \geq 7$. Assume further that $K$ is a finite extension of $\mathbb{Q}_p$ containing $(p-1)$-th roots of all integer. Note that $\zeta_l \in K$.

### 3.4.1 $\wp$-torsion subgroup of the Jacobian

Let $\wp$ be a prime ideal of $\mathbb{Z}[\zeta_l]$ over $p$. (Note that the prime $p$ splits completely in $\mathbb{Z}[\zeta_l]$.) Fix the embedding $\mathbb{Q}(\zeta_l) \subset \mathbb{Q}_p$, so that we have $\wp = \mathbb{Z}[\zeta_l] \cap p\mathbb{Z}_p$. From §3.3.2, we may assume that the $\wp$-torsion subgroup $J[\wp]$ of $J$ is a cyclic group of order $p$.

### 3.4.2 An auxiliary lemma for a Fermat quotient

**Lemma 3.4.1.** *We have an equation*

$$T^p - e_0 T = a(T) + g(T)$$

*for some* $e_0 \in \mathbb{Z}_{(p)}^*$, $a(T) \in A \cap \mathbb{Z}[[T^{-1}]][T]$ *and* $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$.

*Proof.* Put $p = ll' + 1$. We write

$$(-1)^{bl'} x^{l'} \left(1 - \frac{1}{x}\right)^{bl'} = e_+(x) + e_0 + e_-(x)$$

where $e_\pm(x) \in x^{\pm 1}\mathbb{Z}[x^{\pm 1}]$ and $e_0 \in \mathbb{Z}$. Note that $e_0 = \binom{bl'}{l'}$ is a $p$-adic unit. We compute

$$\begin{aligned} e_+(x) + e_0 + e_-(x) = (-1)^{bl'} x^{l'} \left(1 - \frac{1}{x}\right)^{bl'} &= \frac{x^{(a+b)l'}}{x^{ll'}} (-1)^{bl'} \left(1 - \frac{1}{x}\right)^{bl'} \\ &= \left(\frac{x^a (1-x)^b}{x^l}\right)^{l'} = \left(\frac{y}{x}\right)^{ll'} = \left(\frac{y}{x}\right)^{p-1}. \end{aligned}$$

Recalling $y(T) = Tx(T)$, we get an equation in $K((T^{-1}))$

$$T^p - e_0 T = a(T) + g(T)$$

where $a(T) := y(T)e_+(x(T))/x(T)$ and $g(T) := Te_-(x(T))$. Observe that $a(T)$ is in the image of $A = K[x, y]$ in $K((T^{-1}))$ (since $e_+(x) \in x\mathbb{Z}[x]$) and that $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$. □

### 3.4.3 Proof of Theorem 1.0.4

The result of §3.3.4 shows that $(\mathscr{O}_X, N) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$. Let $\pi$ and $\varepsilon_0$ be $(p-1)$-st roots of $-p$ and $1/e_0$ respectively, where $e_0 \in \mathbb{Z}_{(p)}^*$ is the number appearing in Lemma 3.4.1. For an integer $0 \leq i \leq p-2$, we define a Dwork loop by

$$h^{(i)}(T) := \exp(-\pi \zeta_{p-1}^i \varepsilon_0^p (T^p - e_0 T)),$$

where $\zeta_{p-1} := \zeta^{l/(p-1)}$ is a $(p-1)$-st root of unity. Let $s$ be a positive integer such that

$$\zeta_l + s \equiv 0 \bmod \wp.$$

By Lemma 3.4.1, one can show that the Dwork loop has the decomposition (cf. Proposition 3.2.4):

$$(h^{(i)})^p = h_A^{(i)} h_-^{(i)}, \qquad \bar{\gamma}(h^{(i)})(h^{(i)})^s = {h'_A}^{(i)} {h'_-}^{(i)},$$

where $h_A^{(i)}, {h'_A}^{(i)} \in \bar{A} \cap \Gamma(K)$ and $h_-^{(i)}, {h'_-}^{(i)} \in \Gamma_-(K)$. Since $A = W(\mathscr{O}_X, N)$ satisfies the assumptions (A1) and (A2) of Theorem 2.2.9, one can prove the result corresponding to Proposition 3.2.5. The result of §3.3.4 also shows that $(\mathscr{L}, N)$ for $\mathscr{L} \in J[(1-\zeta_l)] \setminus \{0\}$ belongs to $\mathrm{Kr}_{\mathrm{an}}(X, N)$ and that $L := W(\mathscr{L}, N)$ satisfies the assumption (A1) and (A2) of Theorem 2.2.9. Therefore one can prove Theorem 1.0.4 in the same procedure as §3.2.5

# Bibliography


[1] E. Arbarello, *Sketches of KdV*, Symposium in Honor of C. H. Clemens (Salt Lake City, UT, 2000), Contemp. Math., vol. 312, Amer. Math. Soc., Providence, RI, 2002, pp. 9–69.

[2] G. W. Anderson, *Torsion points on Jacobians of quotients of Fermat curves and $p$-adic soliton theory*, Invent. Math. **118** (1994), no. 3, 475–492.

[3] N. Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves*, Amer. J. Math. **113** (1991), no. 5, 779–833.

[4] M. H. Baker, *Torsion points on modular curves*, Invent. Math. **140** (2000), no. 3, 487–509.

[5] M. H. Baker and K. A. Ribet, *Galois theory and torsion points on curves*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 11–32 (English, with English and French summaries). Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[6] J. Boxall and D. Grant, *Examples of torsion points on genus two curves*, Trans. Amer. Math. Soc. **352** (2000), no. 10, 4533–4555.

[7] R. F. Coleman, *Torsion points on curves and $p$-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168.

[8] R. F. Coleman, A. Tamagawa, and P. Tzermias, *The cuspidal torsion packet on the Fermat curve*, J. Reine Angew. Math. **496** (1998), 73–81.

[9] R. F. Coleman, B. Kaskel, and K. A. Ribet, *Torsion points on $X_0(N)$*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proc. Sympos. Pure Math., vol. 66, Amer. Math. Soc., Providence, RI, 1999, pp. 27–49.

[10] B. Dwork, *On the zeta function of a hypersurface*, Inst. Hautes Études Sci. Publ. Math. (1962), no. 12, 5–68.

[11] D. Grant, *Torsion on theta divisors of hyperelliptic Fermat Jacobians*, Compos. Math. **140** (2004), no. 6, 1432–1438.

[12] R. Hirota, *Exact solutions of the Korteveg de Vries equation for multiple collision of solitons*, Phys. Rev. Lett. **27** (1971), 1192–1194.

[13] ———, *Direct method of finding exact solutions of nonlinear evolution equations*, Bäcklund transformations, the inverse scattering method, solitons, and their applications (Workshop Contact Transformations, Vanderbilt Univ., Nashville, Tenn., 1974), Springer, Berlin, 1976, pp. 40–68. Lecture Notes in Math., Vol. 515.

[14] T. Ichikawa, *Algebraic and rigid geometry on the Schottky problem*, preprint.

[15] N. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. **30** (1978), no. 6, 1183–1205.

[16] N. Koblitz, *p-adic analysis: a short course on recent work*, London Mathematical Society Lecture Note Series, vol. 46, Cambridge University Press, Cambridge, 1980.

[17] P. D. Lax, *Periodic solutions of the KdV equation*, Comm. Pure Appl. Math. **28** (1975), 141–188.

[18] ———, *Almost periodic solutions of the KdV equation*, SIAM Rev. **18** (1976), no. 3, 351–375.

[19] C.-H. Lim, *The Jacobian of a cyclic quotient of a Fermat curve*, Nagoya Math. J. **125** (1992), 73–92.

[20] Y. Miyasaka and T. Yamazaki, *Torsion points on hyperelliptic Jacobians via Anderson's p-adic soliton theory*, preprint.

[21] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[22] ———, *An algebro-geometric construction of commuting operators and of solutions to the Toda lattice equation, Korteweg deVries equation and related nonlinear equation*, Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977), Kinokuniya Book Store, Tokyo, 1978, pp. 115–153.

[23] ———, *Tata lectures on theta. II*, Progress in Mathematics, vol. 43, Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations; With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[24] Y. Ohta, J. Satsuma, D. Takahashi, and T. Tokihiro, *An elementary introduction to Sato theory*, Progr. Theoret. Phys. **80** (1988), no. 4, 742.

[25] B. Poonen, *Computing torsion points on curves*, Experiment. Math. **10** (2001), no. 3, 449–465.

[26] M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 327–352 (French).

[27] M. Sato and Y. Sato, *Soliton equations as dynamical systems on infinite-dimensional Grassmann manifold*, Nonlinear partial differential equations in applied science (Tokyo, 1982), North-Holland Math. Stud., vol. 81, North-Holland, Amsterdam, 1983, pp. 259–271.

[28] M. Sato, *The KP hierarchy and infinite-dimensional Grassmann manifolds*, Theta functions —Bowdoin 1987, Part 1 (Brunswick, ME, 1987), Proc. Sympos. Pure Math., vol. 49, Amer. Math. Soc., Providence, RI, 1989, pp. 51–66.

[29] G. Segal and G. Wilson, *Loop groups and equations of KdV type*, Inst. Hautes Études Sci. Publ. Math. (1985), no. 61, 5–65.

[30] J.-P. Serre, *Endomorphismes complètement continus des espaces de Banach p-adiques*, Inst. Hautes Études Sci. Publ. Math. (1962), no. 12, 69–85 (French).

[31] T. Shiota, *Characterization of Jacobian varieties in terms of soliton equations*, Invent. Math. **83** (1986), no. 2, 333–382.

[32] A. Tamagawa, *Ramification of torsion points on curves with ordinary semistable Jacobian varieties*, Duke Math. J. **106** (2001), no. 2, 281–319.

[33] P. Tzermias, *The Manin-Mumford conjecture: a brief survey*, Bull. London Math. Soc. **32** (2000), no. 6, 641–652.