ASIAN J. MATH.
Vol. 20, No. 2, pp. 323–352, April 2016
© 2016 International Press
005

TORSION POINTS ON JACOBIAN VARIETIES VIA ANDERSON'S p-ADIC SOLITON THEORY*

SHINICHI KOBAYASHI† AND TAKAO YAMAZAKI†

Abstract. Anderson introduced a p-adic version of soliton theory. He then applied it to the Jacobian variety of a cyclic quotient of a Fermat curve and showed that torsion points of certain prime order lay outside of the theta divisor. In this paper, we evolve his theory further. As an application, we get a stronger result on the intersection of the theta divisor and torsion points on the Jacobian variety for more general curves. New examples are discussed as well. A key new ingredient is a map connecting the p-adic loop group and the formal group.

Key words. Sato Grassmannian, p-adic tau function, p-adic loop group, formal group.

AMS subject classifications. 11G20 (14H40, 14K25, 37J35).

1. Introduction. In [1], G. Anderson introduced a striking new machinery to investigate the Jacobian variety and theta divisor of an algebraic curve, which he called the *p-adic soliton theory*. He then applied his theory to the Jacobian variety of a cyclic quotient of a Fermat curve and showed that torsion points of certain prime order lay outside of the theta divisor (see Thm. 1.1 and Rem. 5.2 below for details). His proof can be divided into two parts:

1. A description of the Jacobian variety and theta divisor in terms of the (p-adic) Sato Grassmannian, tau function and loop group. This part is applicable for a more general class of curves.
2. Explicit construction of good elements of the Sato Grassmannian and loop group. This part involves heavy computation depending on the defining equation of the curve. No attempt has been made (as far as the authors know) to carry out this part for other classes of curves, except [15].

The main purpose of the present paper is to develop a more general and refined theory for (2). In §1.1 below, we state our result for a cyclic quotient of Fermat curves, which explains how our theory refines Anderson's result. Then in §1.2, after introducing more notations, we will state our main result, which explains how general our theory is. Results in §1.1 will be deduced from results in §1.2 as a special case. We will see our main result can be applied to many new examples in §5.2.

A key step in our theory is a map (3.17) connecting the p-adic loop group and the formal group, which is constructed using the theory of the Hasse-Witt matrix and Artin-Hasse exponential. We expect this new map could be useful for other purpose.

1.1. Cyclic quotient of Fermat curves. Let p be a prime and K a finite extension of $\mathbb{Q}_p$. Let d be an odd prime such that $p \equiv 1 \mod d$ and let $a \in \mathbb{Z}$ be such that $1 < a < l$. We consider the smooth projective model X of an affine curve over K defined by

$$y^d = x^a(x-1)^{d+1-a}. \tag{1.1}$$

*Received October 17, 2014; accepted for publication November 28, 2014.

†Mathematical Institute, Tohoku University, Aoba, Sendai 980-8578, Japan ({shinichi}; {ytakao}@math.tohoku.ac.jp). The authors are supported by Inamori Foundation. The second author is supported by Grant-in-Aid for Challenging Exploratory Research (24654001) and Grant-in-Aid for Young Scientists (A) (22684001).

The genus of X is $g = (d-1)/2$. Let ∞ be the unique point on X which does not lie above the affine curve (1.1). The Jacobian variety $\mathrm{Jac}(X)$ and theta divisor Θ of X are defined as the group of isomorphism classes of invertible sheaves on X of degree zero and

$$\Theta := \{\mathcal{L} \in \mathrm{Jac}(X) \mid H^0(X, \mathcal{L}((g-1)\infty)) \neq 0\} \subset \mathrm{Jac}(X) \tag{1.2}$$

respectively. For any $n \in \mathbb{Z}_{>0}$, we denote by $\mathrm{Jac}(X)[p^n]$ the subgroup of $\mathrm{Jac}(X)$ consisting of the elements of order divisible by p^n. Fix a primitive d-th root of unity $\zeta_d \in K^*$ which actually belongs to $\mathbb{Z}_p \subset K$ by the assumption $p \equiv 1 \mod d$. We define

$$\mathrm{Jac}(X)[p^n]_1 := \{\mathcal{L} \in \mathrm{Jac}(X)[p^n] \mid \delta^*(\mathcal{L}) = \zeta_d \mathcal{L}\}, \tag{1.3}$$

where $\zeta_d \mathcal{L}$ makes sense since $\mathrm{Jac}(X)[p^n]$ is a $\mathbb{Z}_p$-module. We have $\mathrm{Jac}(X)[p^n]_1 \cong \mathbb{Z}/p^n\mathbb{Z}$ if K is sufficiently large (see Prop. 4.8). A part of Anderson's result is the following:

THEOREM 1.1 (Anderson [1]). *We have* $\mathrm{Jac}(X)[p]_1 \cap \Theta = \{0\}$.

We will generalize this result by showing the following:

THEOREM 1.2. *For any* $n \in \mathbb{Z}_{>0}$, *we have* $\mathrm{Jac}(X)[p^n]_1 \cap \Theta = \{0\}$.

REMARK 1.3.

1. In Thm. 1.1, Anderson also proved a similar statement for certain translates of Θ (see Rem. 5.2). We will generalize this result as well (see Thm. 5.1). A similar remark applies to Thm. 1.4 below too. (see Thm. 4.11).
2. When X is a hyperelliptic curve (that happens if and only if $a = 2, (d+1)/2, d-1$), Thm. 1.2 (and the same statement for $p \equiv -1 \mod d$) was proved by Grant [6].

1.2. Main result. In order to state our main result, we introduce some notations and definitions. Let p be a prime and K a finite extension of $\mathbb{Q}_p$. Let X be a smooth projective geometrically connected curve over K of genus $g \geq 2$. Suppose that X admits a smooth projective model $\mathfrak{X}$ over the ring of integers O_K in K. We write $Y := \mathfrak{X} \otimes_{O_K} \mathbb{F}$ for the special fiber of $\mathfrak{X}$, where $\mathbb{F}$ is the residue field of K. Suppose also that we are given a distinguished K-rational point $\infty \in X(K)$ and write $\overline{\infty} \in Y(\mathbb{F})$ for the reduction of ∞. Recall that the *Weierstrass gap sequence* of X at ∞ is defined by

$$WG_\infty(X) := \{n \in \mathbb{Z}_{\geq 0} \mid H^0(X, \mathcal{O}_X(n\infty)) = H^0(X, \mathcal{O}_X((n-1)\infty))\}, \tag{1.4}$$

which is a subset of $\{1, 2, \ldots, 2g-1\}$ with cardinality g. This definition applies to Y and $\overline{\infty}$ as well. We define $\mathrm{Jac}(X), \mathrm{Jac}(X)[p^n]$ and Θ as in §1.1 (see (1.2) and around). The main results of this paper are the following two theorems.

THEOREM 1.4. *Let* $\delta : X \to X$ *be an automorphism of* X *defined over* K *such that* $\delta(\infty) = \infty$. *We suppose the following conditions:*

1. *The order* d *of* δ *satisfies* $d \geq 2g+1$ *and* $p \equiv 1 \mod d$;
2. Y *is ordinary;*
3. $WG_\infty(X) = WG_{\overline{\infty}}(Y)$.

It then turns out that, for any uniformizer t at ∞, the value $\zeta_d = (t/\delta^*(t))(\infty)$ of the rational function $t/\delta^*(t)$ at ∞ is a primitive d-th root of unity and is independent of the choice of t (see §4.6). Let $n \in \mathbb{Z}_{>0}$ and define $\mathrm{Jac}(X)[p^n]_1$ *by the formula* (1.3). *(We have* $\mathrm{Jac}(X)[p^n]_1 \cong \mathbb{Z}/p^n\mathbb{Z}$ *if K is sufficiently large, see Prop. 4.8). Then we have*

$$\mathrm{Jac}(X)[p^n]_1 \cap \Theta = \{0\}.$$

Let $\widehat{\mathrm{Jac}}(X)[p]$ be the kernel of the specialization map $\mathrm{Jac}(X)[p] \to \mathrm{Jac}(Y)[p]$ (see (4.1)). This is isomorphic to the group of p-torsion points on the formal group $\hat{J}_X/O_K$ attached to the Jacobian variety of X. If Y is ordinary and if K is sufficiently large, we have $\widehat{\mathrm{Jac}}(X)[p] \cong (\mathbb{Z}/p\mathbb{Z})^g$.

THEOREM 1.5. *We suppose the following conditions:*

1. *$p \geq 2g$;*
2. *Y is ordinary;*
3. *$WG_\infty(X) = WG_{\overline{\infty}}(Y) = \{1, 2, \ldots, g\}$. (In other words, both ∞ and $\overline{\infty}$ are non-Weierstrass points).*

Then we have

$$|\,\widehat{\mathrm{Jac}}(X)[p] \cap \Theta\,| \leq p^{g-1}.$$

In some cases, we expect that Theorem 1.5 combined with other methods could be used to determine the set $\mathrm{Jac}(X)[p] \cap \Theta$ completely. (A similar strategy is taken in [2] and [24] for the Manin-Mumford conjecture.) In this paper, however, we do not pursuit this direction and leave it as a further problem.

REMARK 1.6.

1. Theorem 1.2 will be deduced from Theorem 1.4 as a special case. See Theorem 5.1 for details.
2. The assumption in Theorem 1.4 is quite restrictive. If X admits an automorphism of *prime* order $d > g + 1$, then X must be isomorphic to a cyclic quotient of a Fermat curve over an algebraic closure of K (see [9]). There are, however, many curves that admits an automorphism of non-prime order $d \geq 2g + 1$. We will discuss such examples in §5.2.
3. On the other hand, the assumption in Theorem 1.5 is quite mild. Indeed, the assumptions (2) and (3) are satisfied in "generic" situation.

1.3. The p-adic soliton theory. We explain the outline of the proof. We use the notations introduced in §1.2.

The completion $\widehat{K(X)}_\infty$ of the function field $K(X)$ of X at ∞ is isomorphic to the field of Laurent power series $K((\frac{1}{T}))$. We fix such an isomorphism, and let A be the image of the composition $H^0(X \setminus \{\infty\}, \mathcal{O}_X) \hookrightarrow K(X) \hookrightarrow \widehat{K(X)}_\infty \cong K((\frac{1}{T}))$. Then A is an element of the *A-part of the Sato Grassmannian* $\mathrm{Gr}_A^{\mathrm{alg}}(K)$, which is by definition the set of all A-submodules V of $K((\frac{1}{T}))$ such that both $V \cap K[[\frac{1}{T}]]$ and $K((\frac{1}{T}))/(V + K[[\frac{1}{T}]])$ are finite dimensional over K. A pair $(\mathcal{L}, \sigma)$ of an invertible sheaf $\mathcal{L}$ on X and a trivialization σ of $\mathcal{L}$ on the infinitesimal neighborhood at ∞ is called a *Krichever pair*. For a Krichever pair $(\mathcal{L}, \sigma)$, we write $V(\mathcal{L}, \sigma)$ for the image of the composition $H^0(X \setminus \{\infty\}, \mathcal{L}) \hookrightarrow K(X) \hookrightarrow \widehat{K(X)}_\infty \cong K((\frac{1}{T}))$, where the first arrow is induced by σ. Then $V(\mathcal{L}, \sigma) \in \mathrm{Gr}_A^{\mathrm{alg}}(K)$, and the correspondence $(\mathcal{L}, \sigma) \mapsto V(\mathcal{L}, \sigma)$

defines a bijection between the set of isomorphism classes of Krichever pairs and $\mathrm{Gr}_A^{\mathrm{alg}}(K)$. Consequently, we obtain a surjective map

$$[\cdot]_A : \mathrm{Gr}_A^{\mathrm{alg}}(K) \to \mathrm{Pic}(X), \quad V = V(\mathcal{L}, \sigma) \mapsto [V]_A := \mathcal{L}$$

where $\mathrm{Pic}(X)$ is the Picard group of X. (So far the base field K can be arbitrary.)

Now let us assume that A has a nice p-adic property which we call *strictly integral* (see Definition 3.1; roughly speaking, this corresponds to the assumption (3) in Theorem 1.4). Then we have the *Sato tau function* $\tau_{A^{\mathrm{an}}} : \Gamma \to K$ which enjoys the 'key property' explained below. Here, Γ is the *p-adic loop group* which contains a subgroup Γ_+ of all formal power series $h(T) \in 1 + TO_K[[T]]$ whose radius of convergence is strictly larger than 1. There exists a non-trivial action of Γ on a subset of $\mathrm{Gr}_A^{\mathrm{alg}}(K)$ (which contains A). The 'key property' of the Sato tau function is that, for $h(T) \in \Gamma_+$, one has $\tau_{A^{\mathrm{an}}}(h(T)) = 0$ if and only if $[h(T)A]_A \in \Theta$. Therefore, given an invertible sheaf $\mathcal{P}$ on X, one can prove $\mathcal{P} \notin \Theta$ by the following strategy:

1. Find a good isomorphism $\widehat{K(X)}_\infty \cong K((\frac{1}{T}))$ for which A is strictly integral.
2. Construct $h(T) \in \Gamma_+$ such that $[h(T)A]_A = \mathcal{P}$.
3. Show that $\tau_{A^{\mathrm{an}}}(h(T)) \neq 0$.

When X is given by (1.1), Anderson worked out the constructions (1) and (2) by explicit calculation using the defining equation. We will develop a general theory for (1) and (2) by using the Hasse-Witt matrix of Y and Artin-Hasse exponential. Let us explain a bit more about (2), under the situation of Theorem 1.4. In order to construct p-torsion points, Anderson used the *Dwork exponential* [1, §3.5]

$$h(T) = \exp((-p)^{1/(p-1)}((uT) - (uT)^p))$$

for suitable $u \in O_K^*$. The key property is that the radius of convergence of $h(T)$ is > 1 and hence $h(T)$ belongs to Γ_+. In order to construct p^n-torsion points for $n \geq 1$, we will use the *Artin-Hasse exponential*

$$e^{AH}(T) := \exp(\sum_{k=0}^{\infty} \frac{1}{p^k} T^{p^k}).$$

The key property is that $e^{AH}(T)$ belongs to $\mathbb{Z}_{(p)}[[T]]$, and hence $h(T;\pi) := e^{AH}(\pi T)$ belongs to Γ_+ for any element π of the maximal ideal of O_K. We will construct a certain formal power series $l_1(X)$ (see (3.33)) which has the following property: if $l_1(\pi) = 0$ and the absolute value of π is $p^{-1/(p^n - p^{n-1})}$, then $[h(T;\pi)A]_A$ belongs to $\mathrm{Jac}(X)[p^n]_1$. The coefficients of $l_1(X)$ are closely related to the *Hasse-Witt matrix* of Y, which is invertible if and only if Y is ordinary. This last fact enables us to have a good control of the absolute value of π such that $l_1(\pi) = 0$. (Actually, $l_1(X)$ gives rise to the logarithm function of a direct summand of the formal group $\hat{J}_X/O_K$ arising from the Jacobian variety of X, at least when K is absolutely unramified. See Theorem 4.5 and Remark 4.7.)

For (3), we follow Anderson's method [1]. Namely, we use an expression of $\tau_{A^{\mathrm{an}}}(h(T))$ as an infinite sum of the product of the *Schur functions* and *Plücker coordinates* (see Theorem 3.4 (2)). This fact was also critical in the classical (complex analytic) soliton theory (compare [22, Proposition 8.3]).

1.4. Notations. For an abelian group A and $n \in \mathbb{Z}$, we write $A[n] := \{a \in A \mid na = 0\}$. For any scheme S, we denote by $\mathrm{Pic}(S)$ the Picard group of S. If X is a smooth projective irreducible curve over a field, we write $\mathrm{Jac}(X) = \{\mathcal{L} \in \mathrm{Pic}(X) \mid \deg \mathcal{L} = 0\}$.

2. Sato Grassmannian and Krichever correspondence.

2.1. Partitions and Maya diagrams. A sequence $\kappa = (\kappa_i)_{i=1}^{\infty}$ of non-negative integers is called a *partition* if $\kappa_i \geq \kappa_{i+1}$ for all $i \in \mathbb{Z}_{>0}$ and if $\kappa_i = 0$ for all sufficiently large i. For a partition κ, we define the *length* $l(\kappa)$ and *weight* $|\kappa|$ of κ by

$$l(\kappa) := \min\{i \in \mathbb{Z}_{>0} \mid \kappa_i = 0\} - 1 \in \mathbb{Z}_{\geq 0} \qquad \text{and} \qquad |\kappa| := \sum_{i=1}^{\infty} \kappa_i \in \mathbb{Z}_{\geq 0}.$$

We write $\underline{\mathrm{Par}}$ for the set of all partitions. The set $\underline{\mathrm{Par}}$ is equipped with a partial ordering defined by $\lambda \leq \kappa$ if and only if $\lambda_i \leq \kappa_i$ for all $i \in \mathbb{Z}_{>0}$.

A subset M of $\mathbb{Z}$ is called a *Maya diagram* if both $M \cap \mathbb{Z}_{\leq 0}$ and $\mathbb{Z}_{>0} \setminus M$ are finite. We write $\underline{\mathrm{Maya}}$ for the set of all Maya diagrams. For $M \in \underline{\mathrm{Maya}}$, we define the *index* $i(M)$ and *partition* $\kappa(M) = (\kappa_i(M))_{i=1}^{\infty}$ of M by $i(M) := |M \cap \mathbb{Z}_{\leq 0}| - |\mathbb{Z}_{>0} \setminus M| \in \mathbb{Z}$ and $\kappa_i(M) := i - i(M) - s_i(M)$, where $\{s_i(M)\}_{i=1}^{\infty}$ is a (unique) increasing sequence of integers such that $M = \{s_i(M) \mid i \in \mathbb{Z}_{>0}\}$. It is well-known (and easy to show) that $\kappa(M)$ is indeed a partition, and that

$$\underline{\mathrm{Maya}} \to \mathbb{Z} \times \underline{\mathrm{Par}}, \qquad M \mapsto (i(M), \kappa(M)) \tag{2.1}$$

is a bijective map.

2.2. Sato Grassmannian. Let F be a field. We work with the field of Laurent power series

$$F((\frac{1}{T})) := \{v(T) = \sum_{i=-\infty}^{n} v_i T^i \mid n \in \mathbb{Z},\ v_i \in F\}$$

with coefficients in F. The *degree* of $v(T) = \sum_{i=-\infty}^{n} v_i T^i \in F((\frac{1}{T}))$ $(v_i \in F)$ is defined to be $\deg v(T) := n$ if $v_n \neq 0$; if further $v_n = 1$ we call $v(T)$ *monic*. For an F-linear subspace V of $F((\frac{1}{T}))$, we define a subset

$$\underline{M}(V) := \{\deg v(T) \mid v(T) \in V \setminus \{0\}\}$$

of $\mathbb{Z}$ and a natural map

$$f_V : V \to F((\frac{1}{T}))/F[[\frac{1}{T}]], \qquad v \mapsto v + F[[\frac{1}{T}]].$$

Note that we have

$$\dim \ker(f_V) = |\underline{M}(V) \cap \mathbb{Z}_{\leq 0}|, \qquad \dim \mathrm{coker}(f_V) = |\underline{M}(V) \setminus \mathbb{Z}_{>0}|. \tag{2.2}$$

The *Sato Grassmannian* $\mathrm{Gr}^{\mathrm{alg}}(F)$ is the set of all F-linear subspaces V of $F((\frac{1}{T}))$ such that both $\ker(f_V)$ and $\mathrm{coker}(f_V)$ are finite dimensional. By (2.2), an F-linear subspace $V \subset F((\frac{1}{T}))$ belongs to $\mathrm{Gr}^{\mathrm{alg}}(F)$ if and only if $\underline{M}(V) \in \underline{\mathrm{Maya}}$. For $V \in \mathrm{Gr}^{\mathrm{alg}}(F)$, we call $i(V) := i(\underline{M}(V))$ (resp. $\kappa(V) := \kappa(\underline{M}(V))$) the *index* (resp. *partition*) of V.

Let $V,\ V' \in \mathrm{Gr}^{\mathrm{alg}}(F)$. We define their product VV' to be the F-linear subspace of $F((\frac{1}{T}))$ spanned by $\{vv' \in F((\frac{1}{T})) \mid v \in V, v' \in V'\}$, which belongs to $\mathrm{Gr}^{\mathrm{alg}}(F)$. We call V and V' *homothety equivaliant* if $V = u(T)V'$ for some $u \in F[[\frac{1}{T}]]^*$. This equivalence relation is denoted by $\sim$. If $V \sim V'$, then we have $\underline{M}(V) = \underline{M}(V')$, and hence $i(V) = i(V')$, $\kappa(V) = \kappa(V')$. The product $(V, V') \mapsto VV'$ descends to the set $\mathrm{Gr}^{\mathrm{alg}}(F)/\sim$ of all homothety equivalence classes.

2.3. Standard basis and Plücker coordinate. Let $V \in \mathrm{Gr}^{\mathrm{alg}}(F)$. Put $M = \underline{M}(V)$ and write $M = \{s_i\}_{i=1}^{\infty}$ with a strictly increasing sequence of integers $\{s_i\}$. There exists a unique basis $\{v_i(T) = \sum_j v_{ij}T^j\}_{i=1}^{\infty}$ of V satisfying the following conditions:

1. $v_i(T)$ is monic of degree s_i for all $i \geq 1$:
2. $v_{i,s_j} = 0$ for all $i > j \geq 1$.

We call such $\{v_i(T)\}_{i=1}^{\infty}$ the *standard basis* of V. For a fixed Maya diagram $M = \{s_i\}_{i=1}^{\infty} \in \underline{\mathrm{Maya}}$, the set $\{V \in \mathrm{Gr}^{\mathrm{alg}}(F) \mid \underline{M}(V) = M\}$ (called a *Schubert cell*) is in one-to-one correspondence with the set of all $\{v_i(T) \in F((\frac{1}{T}))\}_{i=1}^{\infty}$ satisfying (1) and (2) above.

Let $V \in \mathrm{Gr}^{\mathrm{alg}}(F)$ and take the standard basis $\{v_i(T) = \sum_j v_{ij}T^j\}_{i=1}^{\infty}$. The Plücker coordinate $P_\lambda(V)$ of V at $\lambda \in \underline{\mathrm{Par}}$ is defined to be the common value of

$$P_\lambda(V) := \det(v_{i,j-\lambda_j-i(V)})_{i,j=1}^{n} \tag{2.3}$$

for all sufficiently large n. The following lemma is an immediate consequence of definition (see [1, §2.6]).

LEMMA 2.1. *Let $V \in \mathrm{Gr}^{\mathrm{alg}}(F)$. We have $P_{\kappa(V)}(V) = 1$. If $\lambda \in \underline{\mathrm{Par}}$ satisfies $P_\lambda(V) \neq 0$, then we have $\lambda \geq \kappa(V)$.*

2.4. A-part of the Sato Grassmannian. Let A be an F-subalgebra of $F((\frac{1}{T}))$ such that

$$A \cap F[[\frac{1}{T}]] = F, \qquad g_A := \dim F((\frac{1}{T}))/(A + F[[\frac{1}{T}]]) < \infty. \tag{2.4}$$

(In the next subsection, we will construct examples of A arising from geometry.) It follows that $\underline{M}(A) \subset \mathbb{Z}_{\geq 0}$ and there exist integers $\mu_1, \ldots, \mu_{g_A}$ such that

$$\mathbb{Z}_{\geq 0} \setminus \underline{M}(A) = \{\mu_1, \ldots, \mu_{g_A}\}, \qquad 1 \leq \mu_1 < \cdots < \mu_{g_A}. \tag{2.5}$$

Hence A is an element of $\mathrm{Gr}^{\mathrm{alg}}(F)$ of index $1 - g_A$. There is a decomposition of F-vector spaces

$$F((\frac{1}{T})) = A \oplus \frac{1}{T}F[[\frac{1}{T}]] \oplus (\bigoplus_{i=1}^{g_A} FT^{\mu_i}). \tag{2.6}$$

We define the *A-part of the Sato Grassmannian* $\mathrm{Gr}_A^{\mathrm{alg}}(F)$ by

$$\mathrm{Gr}_A^{\mathrm{alg}}(F) := \{V \in \mathrm{Gr}^{\mathrm{alg}}(F) \mid aV \subset V \text{ for all } a \in A\}.$$

Note that $\mathrm{Gr}_A^{\mathrm{alg}}(F)$ is stable under the product and homothety equivalence. The product structure makes $\mathrm{Gr}_A^{\mathrm{alg}}(F)$ (resp. $\mathrm{Gr}_A^{\mathrm{alg}}(F)/\sim$) a commutative semi-group with the unit element A (resp. the class of A).

REMARK 2.2. The semi-groups $\mathrm{Gr}_A^{\mathrm{alg}}(F)$ and $\mathrm{Gr}_A^{\mathrm{alg}}(F)/\sim$ are not necessary groups in general, but this is the case in the examples we will construct in the next subsection. (See Theorem 2.3 (1) and Remark 2.4 for details.)

2.5. Coordinate ring of a curve minus one point. Let X be a smooth projective geometrically connected curve of genus $g \geq 2$ over F equipped with an F-rational point $\infty \in X(F)$. Let $\hat{\mathcal{O}}_{X,\infty}$ be the completion of the local ring $\mathcal{O}_{X,\infty}$ of X at ∞. We fix an isomorphism $N_0 : \hat{\mathcal{O}}_{X,\infty} \cong F[[\frac{1}{T}]]$ of F-algebras. We denote by the same letter N_0 the composition map $\operatorname{Spec} F[[\frac{1}{T}]] \stackrel{N_0}{\to} \operatorname{Spec} \hat{\mathcal{O}}_{X,\infty} \to X$. We write N for the map $\operatorname{Spec} F((\frac{1}{T})) \to X$ induced by N_0. We define

$$A = A(X, \infty, N) := \{N^*(f) \in F((\frac{1}{T})) \mid f \in H^0(X \setminus \{\infty\}, \mathcal{O}_X)\}. \tag{2.7}$$

Then A is an F-subalgebra of $F((\frac{1}{T}))$ such that $\operatorname{Spec} A \cong X \setminus \{\infty\}$. We write $\underline{M}(A) = \{s_i \mid i \in \mathbb{Z}_{>0}\}$ with a strictly increasing sequence of integers $\{s_i\}_{i=1}^{\infty}$. The Riemann-Roch theorem shows that

$$s_1 = 0, \quad s_2 \geq 2 \quad \text{and} \quad s_i = i - 1 + g \quad \text{if } i > g. \tag{2.8}$$

It follows that A satisfies (2.4) with $g_A = g$. The Maya diagram $\underline{M}(A)$ of A is called the *Weierstrass semi-group* of X at ∞. The complement $\mathbb{Z}_{\geq 0} \setminus \underline{M}(A)$ is nothing other than the Weierstrass gap sequence $WG_\infty(X)$ of X at ∞ (see (1.4)). From (2.8), we get a constraint on the values of $\mu_1, \cdots, \mu_g$ defined in (2.5):

$$WG_\infty(X) = \{\mu_1, \cdots, \mu_g\}, \qquad 1 = \mu_1 < \cdots < \mu_g \leq 2g - 1. \tag{2.9}$$

2.6. Krichever pair. An *N-trivialization* of an invertible sheaf $\mathcal{L}$ on X is an isomorphism $\sigma : N^*\mathcal{L} \cong F((\frac{1}{T}))$ of $F((\frac{1}{T}))$-vector spaces induced by an isomorphism $\sigma_0 : N_0^*\mathcal{L} \cong F[[\frac{1}{T}]]$ of $F[[\frac{1}{T}]]$-modules. A pair $(\mathcal{L}, \sigma)$ of an invertible sheaf $\mathcal{L}$ on X and an N-trivialization σ of $\mathcal{L}$ is called a *Krichever pair*. Two Krichever pairs are said to be isomorphic if there is an isomorphism of invertible sheaves compatible with N-trivializations. The set of all isomorphism classes of Krichever pairs forms an abelian group under tensor product with the unit element $(\mathcal{O}_X, N)$.

Suppose we are given a divisor $D = \sum_{P \in X} n_P P$ on X. The associated invertible sheaf $\mathcal{O}_X(D)$ admits an N-trivialization $\sigma(D)$ induced by the composition $\mathcal{O}_X(D) \hookrightarrow F(X) \stackrel{N^*}{\to} F((\frac{1}{T})) \stackrel{T^{-n_\infty}}{\to} F((\frac{1}{T}))$. (Here n_∞ is the coefficient of ∞ in D.) Thus we obtain a Krichever pair $(\mathcal{O}_X(D), \sigma(D))$.

2.7. Krichever correspondence. To a Krichever pair $(\mathcal{L}, \sigma)$, we associate an F-linear subspace $V(\mathcal{L}, \sigma)$ of $F((\frac{1}{T}))$ by

$$V(\mathcal{L}, \sigma) := \{\sigma N^* f \in F((\frac{1}{T})) \mid f \in H^0(X \setminus \{\infty\}, \mathcal{L})\}. \tag{2.10}$$

Note that $A = V(\mathcal{O}_X, N)$, and that $V(\mathcal{L}, \sigma)$ belongs to the A-part of the Sato Grassmannian $\operatorname{Gr}_A^{\mathrm{alg}}(F)$. If $(\mathcal{L}, \sigma)$ and $(\mathcal{L}', \sigma')$ are two Krichever pairs, one has $V(\mathcal{L} \otimes \mathcal{L}', \sigma \otimes \sigma') = V(\mathcal{L}, \sigma)V(\mathcal{L}', \sigma')$ (the product introduced at the end of §2.2).

We define the theta divisor Θ by

$$\Theta := \{\mathcal{L} \in \operatorname{Jac}(X) \mid H^0(X, \mathcal{L}((g-1)\infty)) \neq 0\}. \tag{2.11}$$

THEOREM 2.3 (Krichever correspondence).

1. *The correspondence $(\mathcal{L}, \sigma) \mapsto V(\mathcal{L}, \sigma)$ defines a bijective map, compatible with the product structures, between the set of all isomorphism classes of Krichever*

pairs and $\mathrm{Gr}_A^{\mathrm{alg}}(K)$. *In particular, the semi-group* $\mathrm{Gr}_A^{\mathrm{alg}}(K)$ *is actually an abelian group. Let us denote by*

$$[\cdot]_A : \mathrm{Gr}_A^{\mathrm{alg}}(F) \to \mathrm{Pic}(X)$$

the canonical surjective homomorphism characterized by $[V(\mathcal{L},\sigma)]_A = \mathcal{L}$ *for any Krichever pair* $(\mathcal{L},\sigma)$.

2. *We have the following:*
   (a) $\ker[\cdot]_A = \{u(T)A \mid u(T) \in F[[\frac{1}{T}]]^*\}$. *In particular,* $[\cdot]_A$ *induces an isomorphism*

$$(\mathrm{Gr}_A^{\mathrm{alg}}(F)/\sim) \;\cong\; \mathrm{Pic}(X). \tag{2.12}$$

   (b) $i(V) = \deg[V]_A - g + 1$ *for all* $V \in \mathrm{Gr}_A^{\mathrm{alg}}(F)$.
   (c) *Let* $n \in \mathbb{Z}$ *and* $V \in \mathrm{Gr}_A^{\mathrm{alg}}(F)$. *Then, there is an isomorphism*

$$H^0(X, [V]_A(n\infty)) \cong V \cap T^n F[[\frac{1}{T}]].$$

   (d) *For* $V \in \mathrm{Gr}_A^{\mathrm{alg}}(F)$, *it holds* $[V]_A \in \Theta$ *if and only if* $i(V) = 1-g$ *and* $V \cap T^{g-1}F[[\frac{1}{T}]] \neq 0$.

A proof can be found in [1, §2.3-2.4] (see also [16] and [22, §6]).

Let $\mathcal{L} \in \mathrm{Pic}(X)$. It follows from (2c) that $\underline{M}(V(\mathcal{L},\sigma)) \in \underline{\mathrm{Maya}}$ does not depend on the choice of an N-trivialization σ of $\mathcal{L}$. Hence we may write $\underline{M}(\mathcal{L}) := \underline{M}(V(\mathcal{L},\sigma))$ and $\kappa(\mathcal{L}) := \kappa(V(\mathcal{L},\sigma))$. Suppose now $\mathcal{L} \in \mathrm{Jac}(X)$. Then we have $\underline{M}(\mathcal{L}) \subset \mathbb{Z}_{\geq 0}$. Recall that the *Weierstrass gap sequence* $WG_\infty(\mathcal{L})$ of $\mathcal{L}$ at ∞ is defined by

$$WG_\infty(\mathcal{L}) := \{n \in \mathbb{Z}_{\geq 0} \mid H^0(X, \mathcal{L}(n\infty)) = H^0(X, \mathcal{L}((n-1)\infty))\}. \tag{2.13}$$

(We have $WG_\infty(X) = WG_\infty(\mathcal{O}_X)$, see (1.4).) We have $\underline{M}(\mathcal{L}) = \mathbb{Z}_{\geq 0} \setminus WG_\infty(\mathcal{L})$. It holds $\mathcal{L} \notin \Theta$ if and only if $\kappa(\mathcal{L}) = (0, 0, \cdots)$. Many results on special divisors can be stated in terms of $\kappa(\mathcal{L})$. For instance, Clifford's theorem [7, Theorem 5.4] can be stated as an inequality $\kappa(\mathcal{L}) \leq (g, g-1, \cdots, 1)$. In particular, we have

$$\kappa_1(\mathcal{L}) + l(\kappa(\mathcal{L})) \leq 2g. \tag{2.14}$$

Remark 2.4. The Krichever correspondence can be extended to any integral proper geometrically connected curve X over F with a smooth F-rational point $\infty \in X(F)$, upon replacing $\mathrm{Pic}(X)$ by its compactification [20] (which is no longer an abelian group). See [16] and [22, §6] for details.

2.8. Hermite basis. Let $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_g)$ be as in (2.9). By Serre duality, we have $WG_\infty(X) = \{\mathrm{ord}_\infty(\omega) + 1 \mid \omega \in H^0(X, \Omega^1_{X/F})\}$. Hence there exists a unique basis $\omega_1, \cdots, \omega_g$ of $H^0(X, \Omega^1_{X/F})$ such that $N^*(\omega_i) \in \Omega^1_{F((\frac{1}{T}))/F}$ are expanded as

$$N^*(\omega_i) = \sum_{j=\mu_i}^{\infty} c_{ij} (\frac{1}{T})^{j-1} d(\frac{1}{T}) \qquad (i = 1, \cdots, g) \tag{2.15}$$

with $c_{ij} \in F$ satisfying $c_{i\mu_j} = \delta_{ij}$ (Kronecker's delta) for all $i, j \in \{1, \cdots, g\}$. Such a basis is called the *Hermite basis*.

Let $m \in \mathbb{Z}_{>0}$. It follows from (2.6) that there exist (unique)

(2.16)
$$\vec{b}^{[m]}(T) = (b_j^{[m]}(T))_{j=1}^g \in (A \oplus \frac{1}{T}F[[\frac{1}{T}]])^{\oplus g} \quad \text{and} \quad \mathbf{e}^{[m]} = (e_{i,j}^{[m]})_{i,j=1}^g \in M_g(F)$$
$$\text{such that} \quad T^{\mu_j m} = b_j^{[m]}(T) + \sum_{i=1}^g e_{i,j}^{[m]} T^{\mu_i} \quad \text{for all } j \in \{1, \cdots, g\}.$$

The following result is due to Stöhr and Viana:

Proposition 2.5 (Stöhr-Viana [23], Proposition 2.3). *Let $m \in \mathbb{Z}_{>0}$. We have an equality in $M_g(F)$:*

$$(e_{i,j}^{[m]})_{i,j=1}^g = (c_{i,m\mu_j})_{i,j=1}^g.$$

Proof. For the completeness sake, we recall the proof given in loc. cit. We write $b_j^{[m]}(T) = a_j^{[m]}(T) + g_j^{[m]}(T)$ with $a_j^{[m]}(T) \in A$ and $g_j^{[m]}(T) \in \frac{1}{T}F[[\frac{1}{T}]]$. Then $a_j^{[m]}(T)\omega_i \in \Omega^1_{F(X)/F}$ is regular except at ∞, and its residue at ∞ is given by $c_{i,m\mu_j} - e_{ij}^{[m]}$. (Here $F(X)$ is the function field of X.) The proposition follows from the residue theorem. □

2.9. Hasse-Witt invariant. Suppose now that F is a perfect field of characteristic $p > 0$. We also assume $p \geq 2g$. There exists an additive map $C : \Omega^1_{F(X)/F} \to \Omega^1_{F(X)/F}$ called the *Cartier operator* (see, for example, [13, A2]). It is characterized by the following properties: (i) $C(x^p\omega) = xC(\omega)$ for any $x \in F(X)$ and $\omega \in \Omega^1_{F(X)/F}$; (ii) $C(x^{p-1}dx) = dx$ for any $x \in F(X)$. It preserves the space $H^0(X, \Omega^1_{X/F})$ of regular differentials.

Let $\omega_1, \cdots, \omega_g$ be a basis of $H^0(X, \Omega^1_{X/F})$. We take a matrix $(\gamma_{ij})_{i,j=1}^g \in M_g(F)$ such that $C(\omega_i) = \sum_{j=1}^g \gamma_{ij}\omega_j$. Then the matrix $(\gamma_{ij}^{1/p})_{i,j=1}^g$ is called the *Hasse-Witt matrix* (with respect to the basis $\omega_1, \cdots, \omega_g$), and its rank is called the *Hasse-Witt invariant* of X. The Hasse-Witt invariant is g if and only if X is *ordinary*.

Now let us suppose $\omega_1, \cdots, \omega_g$ to be the Hermite basis with expansion (2.15). It follows from the definition that the Hasse-Witt matrix with respect to $\omega_1, \cdots, \omega_g$ is given by $(c_{i,p\mu_j})$. More generally, for any $k \in \mathbb{Z}_{\geq 0}$ we have

$$C^k(\omega_i) = \sum_{j=1}^g c_{i,p^k\mu_j}^{1/p^k} \omega_j,$$

and hence we get an equality in $M_g(F)$

$$(c_{i,p^k\mu_j}) = (c_{i,p\mu_j})(c_{i,p\mu_j}^p) \cdots (c_{i,p\mu_j}^{p^{k-1}}). \tag{2.17}$$

Proposition 2.6. *Suppose $p \geq 2g$. We set $\mathbf{e}^{(k)} = \mathbf{e}^{[p^k]}$ for all $k \in \mathbb{Z}_{\geq 0}$ (see (2.16)).*

1. *The matrix $\mathbf{e}^{(1)}$ is the Hasse-Witt matrix of X with respect to the Hermite basis.*
2. *The following conditions are equivalent:*
   (a) X is ordinary;

(b) $\det(\mathbf{e}^{(1)}) \in F^*$;
(c) $\det(\mathbf{e}^{(k)}) \in F^*$ *for all* k.

Proof. This is an immediate consequence of Proposition 2.5 and (2.17). □

REMARK 2.7. In loc. cit., Stöhr and Viana also deal with the case $p < 2g$, but we will not need this result.

3. p-adic theory of Sato Grassmannian. In this section, p is a fixed prime number and K is a finite extension of $\mathbb{Q}_p$. We write $|\cdot|$ for the absolute value on K such that $|p| = 1/p$. We set $O_K = \{a \in K \mid |a| \le 1\}$, $\mathcal{M}_K = \{a \in K \mid |a| < 1\}$, and $\mathbb{F} = O_K/\mathcal{M}_K$.

3.1. The reduction map. We study the relation between $\mathrm{Gr}^{\mathrm{alg}}(K)$ and $\mathrm{Gr}^{\mathrm{alg}}(\mathbb{F})$. For $a = \sum a_i T^i \in K((\frac{1}{T}))$, we write $||a|| := \sup_{i\in\mathbb{Z}} |a_i| \in \mathbb{R}_{\ge 0} \cup \{\infty\}$.

DEFINITION 3.1. Let $V \in \mathrm{Gr}^{\mathrm{alg}}(K)$. Let $\{v_i(T)\}_{i=1}^{\infty}$ be the standard basis of V (see §2.3). (Note that $||v_i|| = 1$ if and only if $||v_i|| \le 1$ because v_i is supposed to be monic.)

1. We call V *bounded* if $||v_i|| < \infty$ for all $i \in \mathbb{Z}_{>0}$ (hence $||v|| < \infty$ for all $v \in V$).
2. We call V *integral* if V is bounded and $||v_i|| \le 1$ for all sufficiently large $i \in \mathbb{Z}_{>0}$.
3. We call V *strictly integral* if V is bounded and $||v_i|| \le 1$ for all $i \in \mathbb{Z}_{>0}$.

We set $\mathrm{Gr}^{\mathrm{alg,int}}(K) := \{V \in \mathrm{Gr}^{\mathrm{alg}}(K) \mid V \text{ is integral }\}$.

We shall rewrite these properties using the *reduction map*

$$\mathrm{red} : O_K[[\frac{1}{T}]][T] \to \mathbb{F}((\frac{1}{T})), \quad \sum a_i T^i \mapsto \sum (a_i \bmod \mathcal{M}_K) T^i. \tag{3.1}$$

For a subset V of $K((\frac{1}{T}))$, we define

$$\begin{aligned} O(V) &:= \{v \in V \mid ||v|| \le 1\} = V \cap O_K[[\frac{1}{T}]][T], \\ V^{\mathrm{red}} &:= \{\mathrm{red}\, v \in \mathbb{F}((\frac{1}{T})) \mid v \in O(V)\}. \end{aligned} \tag{3.2}$$

The restriction of (3.1) induces a surjection $O(V) \to V^{\mathrm{red}}$. For $n \in \mathbb{Z}$, we set

$$V_n := V \cap T^n K[[\frac{1}{T}]], \qquad (V^{\mathrm{red}})_n := V^{\mathrm{red}} \cap T^n \mathbb{F}[[\frac{1}{T}]]. \tag{3.3}$$

The definitions in 3.1 are best understood in terms of the Maya diagrams of V and V^{red} (see §2.2).

PROPOSITION 3.2. *Let V be a bounded element of* $\mathrm{Gr}^{\mathrm{alg}}(K)$.

1. *The following conditions are equivalent:*
   (a) V is integral;
   (b) the reduction map induces surjective maps $O(V_n) \to (V^{\mathrm{red}})_n$ for all sufficiently large $n \in \mathbb{Z}_{>0}$;
   (c) $\underline{M}(V^{\mathrm{red}}) \in \underline{\mathrm{Maya}}$ and $i(V) = i(V^{\mathrm{red}})$.
   If these conditions hold, we have $\kappa(V) \le \kappa(V^{\mathrm{red}})$.
2. *The following conditions are equivalent:*
   (a) V is strictly integral;

(b) *the reduction map induces surjective maps* $O(V_n) \to (V^{\mathrm{red}})_n$ *for all* $n \in \mathbb{Z}_{>0}$;
(c) $\underline{M}(V) = \underline{M}(V^{\mathrm{red}})$;
(c') $\underline{M}(V) \supset \underline{M}(V^{\mathrm{red}})$.

Proof. Let $\{v_i(T)\}_{i=1}^{\infty}$ the standard basis of V, and let $\{s_i\}_{i=1}^{\infty}$ (resp. $\{\bar{s}_i\}_{i=1}^{\infty}$) be the strictly increasing sequence of integers such that $\underline{M}(V) = \{s_i \mid i \in \mathbb{Z}_{>0}\}$ (resp. $\underline{M}(V^{\mathrm{red}}) = \{\bar{s}_i \mid i \in \mathbb{Z}_{>0}\}$).

First we prove (2). If (a) holds, then $\{v_i(T)\}_{i=1}^{\infty}$ is an O_K-basis of $O(V)$. Hence (b) and (c) follow immediately. It is easy to see that (c') is implied by either of (b) or (c). It remains to prove the implication (c') $\Rightarrow$ (a). We prove its contraposition. Suppose that $||v_n(T)|| > 1$ for some n. Take $c \in O_K$ such that $|c| = ||v_n(T)||^{-1}$. Then $\deg \mathrm{red}(cv_n(T))$ is an element of $\underline{M}(V^{\mathrm{red}})$ which does not belong to $\underline{M}(V)$. This completes the proof of (2).

We prove (1). Suppose (a). Take $n_1 \in \mathbb{Z}_{>0}$ such that $||v_i(T)|| = 1$ for all $i \geq n_1$. Let V' be the K-linear span of $\{v_i(T)\}_{i=n_1}^{\infty}$. Then V' is a strictly integral element of $\mathrm{Gr}^{\mathrm{alg}}(K)$. Thus we get the surjectivity of $O(V'_n) \to (V^{'\,\mathrm{red}})_n$ for all n by (2). On the other hand, let U be the K-linear span of $v_1(T), \cdots, v_{n_1-1}(T)$. As we have remarked before (3.3), the reduction map $O(U) \to U^{\mathrm{red}}$ is surjective. It follows that $O(U_n) \to (U^{\mathrm{red}})_n$ is surjective for any $n \geq s_{n_1-1}$ because we have $U_n = U$ and $U^{\mathrm{red}} = (U^{\mathrm{red}})_n$. We conclude that $O(V_n) \to (V^{\mathrm{red}})_n$ is surjective for all $n \geq \max(n_1, s_{n_1-1})$.

Suppose (b). Take $n_1 \in \mathbb{Z}_{>0}$ such that $O(V_n) \to (V^{\mathrm{red}})_n$ is surjective for all $n \geq n_1$. Let i_1 be the minimal integer such that $s_{i_1} \geq n_1$. Let V' be the K-linear span of $\{v_i(T)\}_{i=i_1}^{\infty}$. Then V' is a strictly integral element of $\mathrm{Gr}^{\mathrm{alg}}(K)$, and we get $\underline{M}(V') = \underline{M}(V^{'\,\mathrm{red}})$ by (2). On the other hand, let U be the K-linear span of $v_1(T), \cdots, v_{i_1-1}(T)$. Then $|\underline{M}(U^{\mathrm{red}})| = i_1 - 1$ and $\underline{M}(U^{\mathrm{red}}) \subset (-\infty, s_{i_1}]$. This proves (c).

Suppose (c). Take $i_1 \in \mathbb{Z}_{>0}$ such that $s_i = \bar{s}_i = i - i(V)$ for all $i \geq i_1$. Let V' be the K-linear span of $\{v_i(T)\}_{i=i_1}^{\infty}$. Then V' is a strictly integral element of $\mathrm{Gr}^{\mathrm{alg}}(K)$ by (2), and hence V is integral.

If the condition (b) is satisfied, then $s_i \geq \bar{s}_i$ holds for all i. Hence $\kappa(V) \leq \kappa(V^{\mathrm{red}})$. □

3.2. p-adic analytic Sato Grassmannian. In addition to the field of Laurent power series $K((\frac{1}{T}))$, we will work with another field

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

This is a complete discrete valuation field whose absolute value is given by

$$\left\| \sum_{i=-\infty}^{\infty} a_i T^i \right\| := \sup_{i=-\infty}^{\infty} |a_i|.$$

We regard H as an ultrametric Banach algebra over K equipped with a norm $\| \cdot \|$. We define closed subspaces H_+ and H_- of H by

$$H_+ := \{ \sum_{i=-\infty}^{\infty} a_i T^i \in H \mid a_i = 0 \ (i \leq 0)\}, \quad H_- := \{ \sum_{i=-\infty}^{\infty} a_i T^i \in H \mid a_i = 0 \ (i > 0)\}$$

so that we have $H = H_- \oplus H_+$.

Following Anderson [1, §3.1], we define the *p-adic Sato Grassmannian* $\mathrm{Gr}^{\mathrm{an}}(K)$ to be the set of all K-linear subspaces W of H such that W is the image of an injective K-linear map $w : H_+ \to H$ satisfying the following condition: there exist $i_0 \in \mathbb{Z}$, a K-linear operator $w_1 : H_+ \to H_-$ with $\|w_1\| \leq 1$, and a K-linear endomorphism w_2 on H_+ with $\|w_2\| \leq 1$ that is a uniform limit of bounded K-linear operators of finite rank (i.e. *completely continuous*), such that $T^{i_0}w : H_+ \to H = H_- \oplus H_+$ agrees with $w_1 \oplus (1 + w_2)$.

This sophisticated definition admits an elementary interpretation as follows [1, §3.2]. We regard both $K((\frac{1}{T}))$ and H as K-linear subspaces of $\prod_{i\in\mathbb{Z}} KT^i$ (which itself is no longer a ring). For a subset W of H, we set $W^{\mathrm{alg}} := W \cap K((\frac{1}{T}))$. For a subset V of $K((\frac{1}{T})) \cap H$, the closure of V in H is denoted by V^{an}. Note that if $V \in \mathrm{Gr}^{\mathrm{alg}}(K)$ is bounded (see Definition 3.1), then $V \subset K((\frac{1}{T})) \cap H$.

Proposition 3.3 (Anderson [1], §3.2).
1. *If $W \in \mathrm{Gr}^{\mathrm{an}}(K)$, then one has $W^{\mathrm{alg}} \in \mathrm{Gr}^{\mathrm{alg}}(K)$. This defines an injective map* $\mathrm{alg} : \mathrm{Gr}^{\mathrm{an}}(K) \to \mathrm{Gr}^{\mathrm{alg}}(K)$.
2. *Let $V \in \mathrm{Gr}^{\mathrm{alg}}(K)$. The following conditions are equivalent:*
   (a) *There exists $W \in \mathrm{Gr}^{\mathrm{an}}(K)$ such that $V = W^{\mathrm{alg}}$.*
   (b) *V is integral (see Definition 3.1).*

Consequently, we get a bijective map

$$\mathrm{alg} : \mathrm{Gr}^{\mathrm{an}}(K) \to \mathrm{Gr}^{\mathrm{alg,int}}(K) \tag{3.4}$$

whose inverse is given by $V \mapsto V^{\mathrm{an}}$.

For a subset W of H, we set $O(W) := \{w \in W \mid ||w|| \leq 1\}$ and $\mathcal{M}(W) := \{w \in W \mid ||w|| < 1\}$. There is a canonical surjective map

$$\mathrm{red} : O(H) \to \mathbb{F}((\frac{1}{T})), \qquad \sum a_i T^i \mapsto \sum (a_i \bmod \mathcal{M}_K)T^i \tag{3.5}$$

(which agrees with (3.1) on $O(H) \cap O_K[[\frac{1}{T}]][T]$).

3.3. The p-adic loop group. For a real number ρ such that $0 \leq \rho < 1$, we define

$$\Gamma_\rho := \{h(T) = \sum_{i=-\infty}^{\infty} h_i T^i \in H^* \mid ||h(T)|| = |h_0| = 1,\ |h_i| \leq \rho^i \text{ for all } i > 0\}. \tag{3.6}$$

(When $\rho = 0$, the group Γ_0 is written by Γ_- in [1].) The *p-adic loop group* Γ is defined to be the union of Γ_ρ for all $0 \leq \rho < 1$.

We have an action of Γ on $\mathrm{Gr}^{\mathrm{an}}(K)$ given by $h(T)W := \{h(T)w(T) \in H \mid w(T) \in W\}$ for any $h(T) \in \Gamma$ and $W \in \mathrm{Gr}^{\mathrm{an}}(K)$. This induces an action of Γ on $\mathrm{Gr}^{\mathrm{alg,int}}(K)$ through (3.4). Explicitly, for $V \in \mathrm{Gr}^{\mathrm{alg,int}}(K)$ and $h(T) \in \Gamma$ we have

$$h(T)V = \{h(T)w(T) \in H \mid w(T) \in V^{\mathrm{an}}\} \cap K((\frac{1}{T})). \tag{3.7}$$

The action of

$$\Gamma_+ := \{h(T) = \sum h_i T^i \in \Gamma \mid h_0 = 1,\ h_i = 0 \text{ for all } i < 0\}$$

on $\mathrm{Gr}^{\mathrm{alg,int}}(K)$ reduces to the trivial action on $\mathrm{Gr}^{\mathrm{alg}}(\mathbb{F})$, that is,

$$(h(T)V)^{\mathrm{red}} = V^{\mathrm{red}} \qquad \text{for any } V \in \mathrm{Gr}^{\mathrm{alg,int}}(K) \text{ and } h(T) \in \Gamma_+. \tag{3.8}$$

3.4. Schur function. Let λ be a partition (see §2.1) and $h = \sum h_i T^i \in \Gamma_+$. The *Schur function* $S_\lambda(h)$ is defined by

$$S_\lambda(h) := \det(h_{\lambda_i - i+j})_{i,j=1}^{l(\lambda)} \in \mathbb{Z}[h_1, h_2, \cdots]. \tag{3.9}$$

If we declare the degree of h_i to be i, then $S_\lambda(h)$ is homogeneous of degree $|\lambda|$. It follows that, if $h(T) \in \Gamma_\rho \cap \Gamma_+$ for some $0 < \rho < 1$, then we have

$$|S_\lambda(h(T))| \leq \rho^{|\lambda|}. \tag{3.10}$$

3.5. Sato tau function. Let $W \in \mathrm{Gr}^{\mathrm{an}}(K)$. Anderson constructed the *Sato tau function* $\tau_W : \Gamma \to K$ which plays a central role in his theory. We refer to [1, §3.3] for its definition. The important properties of the Sato tau function are summarized in the following theorem:

THEOREM 3.4 (Anderson [1], §3.3, §3.4). *Let $W \in \mathrm{Gr}^{\mathrm{an}}(K)$.*

1. *For $h(T) \in \Gamma$, we have $\tau_W(h(T)) = 0$ if and only if*

$$h(T)W^{\mathrm{alg}} \cap T^{i(W^{\mathrm{alg}})} K[[\frac{1}{T}]] \neq 0.$$

   (Compare Theorem 2.3 (2d).)
2. *Suppose that W^{alg} is strictly integral (see Definition 3.1). Then the following equality (Sato expansion) holds for any $h(T) \in \Gamma_+$:*

$$\tau_W(h(T)) = \sum_{\lambda \in \underline{\mathrm{Par}}} P_\lambda(W^{\mathrm{alg}}) S_\lambda(h).$$

   Here $P_\lambda(W^{\mathrm{alg}})$ is the Plücker coordinate (2.3) *and $S_\lambda(h)$ is the Schur function* (3.9).

COROLLARY 3.5. *Let $W \in \mathrm{Gr}^{\mathrm{an}}(K)$ be such that W^{alg} is strictly integral. Let $0 < \rho < 1$ and suppose $h(T) \in \Gamma_+ \cap \Gamma_\rho$ satisfies $|S_\kappa(h(T))| = \rho^{|\kappa|}$ with $\kappa := \kappa(W^{\mathrm{alg}})$. Then we have $h(T)W^{\mathrm{alg}} \cap T^{i(W^{\mathrm{alg}})} K[[\frac{1}{T}]] = 0$.*

Proof. We follow Anderson's proof of [1, Lemma 3.5.1]. Since W^{alg} is strictly integral, we have $|P_\lambda(W^{\mathrm{alg}})| \leq 1$ for all λ. Furthermore, Lemma 2.1 shows that $P_\kappa(W^{\mathrm{alg}}) = 1$ and $P_\lambda(W^{\mathrm{alg}}) = 0$ unless $\lambda \in \underline{\mathrm{Par}}$ satisfies $\lambda \geq \kappa$. On the other hand, (3.10) shows that if $\lambda \in \underline{\mathrm{Par}}$ satisfies $\lambda \neq \kappa$ and $\lambda \geq \kappa$, then we have $|S_\lambda(h(T))| < |S_\kappa(h(T))| = \rho^{|\kappa|}$. By Theorem 3.4 (2), this proves $\tau_W(h(T)) \neq 0$. Now Theorem 3.4 (1) completes the proof. □

3.6. Artin-Hasse exponential. Put $l(T) := \sum_{k=0}^{\infty} \frac{1}{p^k} T^{p^k}$. Recall that the Artin-Hasse exponential $\exp(l(T))$ belongs to $\mathbb{Z}_{(p)}[[T]]$. Therefore, for any $\pi \in \mathcal{M}_K$, the series

$$h(T; \pi) := \exp(l(\pi T)) \tag{3.11}$$

belongs to Γ_+. More precisely, writing $h(T; \pi) = \sum_{i=0}^{\infty} h_i T^i$ we have

$$|h_i| \leq |\pi|^i \quad \text{for all } i \geq 0 \quad \text{and} \quad h_i = \frac{\pi^i}{i!} \quad \text{for } i = 0, 1, \cdots p-1, \tag{3.12}$$

whence $h(T;\pi) \in \Gamma_{|\pi|} \cap \Gamma_+$. For a finite sequence of positive integers $\boldsymbol{\mu} = (\mu_1, \dots, \mu_g)$ and for $\vec{\pi} = (\pi_i)_{i=1}^g \in \mathcal{M}_K^{\oplus g}$, we define

$$h_{\boldsymbol{\mu}}(T;\vec{\pi}) := \prod_{i=1}^{g} h(T^{\mu_i};\pi_i) = \exp\Big(\sum_{i=1}^{g} l(\pi_i T^{\mu_i})\Big) \in \Gamma_\rho \cap \Gamma_+, \tag{3.13}$$

where $\rho := \max_i |\pi_i|^{1/\mu_i}$.

Proposition 3.6. *We suppose one of the following conditions:*

1. *Let $\pi \in \mathcal{M}_K \setminus \{0\}$ and set $h(T) = h(T;\pi)$, $\rho = |\pi|$. Let $\kappa \in \underline{\mathrm{Par}}$ be a partition satisfying $\kappa_1 + l(\kappa) \le p$.*
2. *Let g be an integer such that $0 < g < p$ and $\vec{\pi} = (\pi_i)_{i=1}^g \in \mathcal{M}_K^{\oplus g}$. Suppose $|\pi_i| \le |\pi_g|$ for all $i = 1, 2, \cdots, g-1$. Set $\boldsymbol{\mu} = (1, 2, \cdots, g)$, $h(T) = h_{\boldsymbol{\mu}}(T;\vec{\pi})$, $\rho = |\pi_g|^{1/g}$, and $\kappa = (g, 0, 0, \cdots)$.*

Then we have $h(T) \in \Gamma_+ \cap \Gamma_\rho$ and $|S_\kappa(h(T))| = \rho^{|\kappa|}$. Consequently, we have $h(T)W^{\mathrm{alg}} \cap T^{i(W^{\mathrm{alg}})}K[[\frac{1}{T}]] = 0$ for any $W \in \mathrm{Gr}^{\mathrm{an}}(K)$ such that W^{alg} is strictly integral and $\kappa = \kappa(W^{\mathrm{alg}})$.

Proof. It is clear from the definition that $h(T) \in \Gamma_+ \cap \Gamma_\rho$ in both cases. We prove $|S_\kappa(h(T))| = \rho^{|\kappa|}$. The proof of (1) is again the same as Anderson's proof of [1, Lemma 3.5.1]. The point is that, by the latter part of (3.12), one can combinatorially compute $S_\lambda(h(T))$ for a small partition λ. The result is (see loc. cit.)

$$S_\lambda(h(T)) = \Big(\prod_{1\le i\le l(\lambda),\ 1\le j\le \lambda_i} HL(\lambda;(i,j))\Big)^{-1} \pi^{|\lambda|} \qquad \text{if } \ l(\lambda) + \lambda_1 \le p,$$

where the *hook length* $HL(\lambda;(i,j))$ is by definition the cardinality of the set

$$\{(i',j') \in \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \mid (i' = i \text{ and } j \le j' \le \lambda_i) \text{ or } (i \le i' \text{ and } j' = j \le \lambda_{i'})\}.$$

By the assumption $\kappa_1 + l(\kappa) \le p$, we see that $HL(\kappa;(i,j))$ is a p-adic unit for all $1 \le i \le l(\kappa)$, $1 \le j \le \kappa_i$. This shows (1). Next, we consider (2). In this case, $S_\kappa(h(T))$ is given by the coefficient of T^g in $h(T)$. By assumption, we get

$$|S_\kappa(h(T))| = \Big|\sum_{j_1+2j_2+\cdots+gj_g=g} \frac{\pi_1^{j_1}\cdots\pi_g^{j_g}}{j_1!\cdots j_g!}\Big| = |\pi_g| = \rho^{|\kappa|},$$

which proves (2). The last statement follows from Corollary 3.5. □

3.7. g-dimensional family of p-adic loops. Let A be a K-subalgebra of $K((\frac{1}{T}))$. Assume that A satisfies (2.4) and

$$A \text{ is a strictly integral element of } \mathrm{Gr}^{\mathrm{alg}}(K) \ \text{ (see Definition 3.1).} \tag{3.14}$$

Let A^{an} be the closure of A in H, so that A^{an} is a K-subalgebra of H. By the definition of the action of Γ on $\mathrm{Gr}^{\mathrm{an}}(K)$ and on $\mathrm{Gr}^{\mathrm{alg,int}}(K)$ (see (3.7)), we have

$$\{h(T) \in \Gamma \mid h(T)A = A\} = \{h(T) \in \Gamma \mid h(T)A^{\mathrm{an}} = A^{\mathrm{an}}\} = (A^{\mathrm{an}})^* \cap \Gamma. \tag{3.15}$$

We define an abelian group Γ_A by

$$\Gamma_A := \Gamma/((A^{\mathrm{an}})^* \cap \Gamma)\Gamma_0.$$

(Here Γ_0 is the group (3.6) with $\rho = 0$.) We write $[h(T)]$ for the class of $h(T) \in \Gamma$ in Γ_A. Then we get a well-defined injective map

$$\Gamma_A \to \mathrm{Gr}_A^{\mathrm{alg,int}}(K)/\sim, \qquad [h(T)] \mapsto [h(T)A]_A. \tag{3.16}$$

Recall from §2.4 that the assumption (2.4) implies that $\underline{M}(A) \subset \mathbb{Z}_{\geq 0}$ and there exists an increasing sequence $1 \leq \mu_1 < \cdots < \mu_{g_A}$ of positive integers satisfying (2.5). Set $g := g_A = 1 - i(\underline{M}(A))$ and $\boldsymbol{\mu} := (\mu_1, \ldots, \mu_g)$. Using (3.13), we define a map

$$\mathcal{M}_K^{\oplus g} \to \Gamma_A, \qquad \vec{\pi} = (\pi_i)_{i=1}^g \mapsto [h_{\boldsymbol{\mu}}(T; \vec{\pi})]. \tag{3.17}$$

(It should be noted that (3.17) is not a group homomorphism, even if we endow $\mathcal{M}_K^{\oplus g}$ with an abelian group structure induced by the formal group in Theorem 4.5 below.)

Proposition 3.7. *The map* (3.17) *is injective.*

For the proof, we need an auxiliary lemma. Let $\pi \in \mathcal{M}_K$. There is a homomorphism (see (3.6))

$$\Gamma_{|\pi|} \to \mathbb{F}[[T]]^*, \qquad \sum_{i=-\infty}^{\infty} h_i T^i \mapsto \sum_{i=0}^{\infty} (\frac{h_i}{\pi^i} \bmod \mathcal{M}_K) T^i. \tag{3.18}$$

The kernel of (3.18) is denoted by $\Gamma_{|\pi|-}$. Hence we get an injective homomorphism

$$\Gamma_{|\pi|}/\Gamma_{|\pi|-} \to \mathbb{F}[[T]]^*. \tag{3.19}$$

Lemma 3.8. *Let $\pi \in \mathcal{M}_K$ and set $\rho = |\pi|$. Take $h(T) = \sum_{j\in\mathbb{Z}} h_j T^j \in A^{\mathrm{an}} \cap \Gamma_\rho$. Let $\sum_{i=0}^{\infty} b_i T^i \in \mathbb{F}[[T]]^*$ be the image of $h(T)\Gamma_{\rho-}$ by* (3.19)*. Then, we have $b_{\mu_j} = 0$ for all $j = 1, \ldots, g$.*

Proof. We take the standard basis $\{a_i(T) = \sum_j a_{ij} T^j\}_i$ of A (see §2.3). Note that $|a_{ij}| \leq 1$ for all i, j by (3.14). Since $h(T) \in A^{\mathrm{an}}$, we can write $h(T) = \sum_{i=1}^{\infty} c_i a_i(T)$ with $c_i \in K$. By the definition of standard basis, for all $i \geq 1$ we have $c_i = h_{s_i}$ and hence $|c_i| = |h_{s_i}| \leq \rho^{s_i}$. Take $j \in \{1, \ldots, g\}$. Let l be the smallest integer such that $\mu_j < s_l$. Then we have $|h_{\mu_j}| = |\sum_{i=s_l}^{\infty} c_i a_{i\mu_j}| \leq \rho^{s_l} < \rho^{\mu_j}$. This proves the lemma. □

Proof of Proposition 3.7. We take a uniformizer $\pi_K \in \mathcal{M}_K$. For $q \in \mathbb{R}_{>0}$, we define $\bar{\mathcal{M}}_K^q := \mathcal{M}_K^q/\mathcal{M}_K^{q+1}$ (equipped with an abelian group structure induced by the addition of $\mathcal{M}_K$) if $q \in \mathbb{Z}_{>0}$, and $\bar{\mathcal{M}}_K^q := 0$ otherwise. By passing to the quotient, (3.17) induces an injective *homomorphism*

$$\bigoplus_{j=1}^{g} \bar{\mathcal{M}}_K^{i/\mu_j} \to \Gamma_{|\pi_K|^i}/\Gamma_{|\pi_K|^i-}$$

for any $i \in \mathbb{R}_{>0}$. It suffices to show the the injectivity of the homomorphism

$$\bigoplus_{j=1}^{g} \bar{\mathcal{M}}_K^{i/\mu_j} \to \Gamma_{|\pi_K|^i}/\Gamma_{|\pi_K|^i-}((A^{\mathrm{an}})^* \cap \Gamma_{|\pi_K|^i}) \tag{3.20}$$

induced by (3.17) for all i. Fix i and take $\vec{\pi} = (\pi_j) \in \mathcal{M}_K^{\oplus g}$. Suppose $|\pi_j| \leq |\pi_K|^{i/\mu_j}$ for all j and the class of $\vec{\pi}$ belongs to the kernel of (3.20). We need to show the class of π_j in $\bar{\mathcal{M}}_K^{i/\mu_j}$ is trivial for all j. This amounts to showing $b_{\mu_j} = 0$ for all $j = 1, \ldots, g$, where $\sum_{k=0}^{\infty} b_k T^k \in \mathbb{F}[[T]]^*$ is the image of $h(T) = h_{\boldsymbol{\mu}}(T; \vec{\pi})$ by (3.19) (with $\rho := |\pi_K|^i$). However, this holds for any $h(T) \in \Gamma_{|\pi_K|^i-}((A^{\mathrm{an}})^* \cap \Gamma_{|\pi_K|^i})$ by Lemma 3.8. This completes the proof of Proposition 3.7. □

3.8. p^n-torsion points. We keep the assumption that $A \subset K((\frac{1}{T}))$ is a K-subalgebra satisfying (2.4) and (3.14). By the assumption (3.14), the decomposition (2.6) restricts to a decomposition of O_K-modules

$$O_K[[\frac{1}{T}]][T] = O(A) \oplus \frac{1}{T}O_K[[\frac{1}{T}]] \oplus (\bigoplus_{i=1}^{g} O_K T^{\mu_i}). \tag{3.21}$$

(Recall that $\boldsymbol{\mu} = (\mu_1, \dots, \mu_g)$ is a sequence of positive integers satisfying (2.5).)

By (3.21), for all $k \in \mathbb{Z}_{\geq 0}$ there exist (unique)

$$\begin{aligned} &\vec{b}^{(k)}(T) = (b_j^{(k)}(T))_{j=1}^{g} \in (O(A) \oplus \frac{1}{T}O_K[[\frac{1}{T}]])^{\oplus g} \text{ and} \\ &\mathbf{e}^{(k)} = (e_{i,j}^{(k)})_{i,j=1}^{g} \in M_g(O_K) \text{ such that} \\ &T^{\mu_j p^k} = b_j^{(k)}(T) + \sum_{i=1}^{g} e_{i,j}^{(k)} T^{\mu_i} \qquad \text{for all } j \in \{1, \cdots, g\}. \end{aligned} \tag{3.22}$$

(This is to say, with the notation in (2.16), $\vec{b}^{(k)}(T) = \vec{b}^{[p^k]}(T)$ and $\mathbf{e}^{(k)} = \mathbf{e}^{[p^k]}$.) Using the matrix $\mathbf{e}^{(k)}$, we introduce a vector of formal power series:

$$\vec{l}(X_1, \cdots, X_g) := \sum_{k=0}^{\infty} \frac{1}{p^k} \mathbf{e}^{(k)} \begin{pmatrix} X_1^{p^k} \\ \vdots \\ X_g^{p^k} \end{pmatrix} \in O_K[[X_1, \cdots, X_g]]^{\oplus g}. \tag{3.23}$$

Note that $\vec{l}(\vec{\pi})$ converges in $K^{\oplus g}$ for any $\vec{\pi} \in \mathcal{M}_K^{\oplus g}$. For $\vec{\pi} = (\pi_1, \cdots, \pi_g) \in \mathcal{M}_K^{\oplus g}$, we write $||\vec{\pi}|| := \max(|\pi_1|, \cdots, |\pi_g|)$. We define for each $n \in \mathbb{Z}_{\geq 0}$

$$T_n := \{\vec{\pi} \in \mathcal{M}_K^{\oplus g} \mid \vec{l}(\vec{\pi}) = 0,\ ||\vec{\pi}|| \leq |p|^{1/(p^n - p^{n-1})}\}. \tag{3.24}$$

Proposition 3.9. *Let $n \in \mathbb{Z}_{>0}$. For any $\vec{\pi} \in T_n$, we have $[h_{\boldsymbol{\mu}}(T; \vec{\pi})^{p^n}] = 1$ in Γ_A. (See* (3.13) *for the definition of $h_{\boldsymbol{\mu}}(T; \vec{\pi})$.) Consequently, we get an injective map*

$$T_n \to \Gamma_A[p^n], \qquad \vec{\pi} \mapsto [h_{\boldsymbol{\mu}}(T; \vec{\pi})]. \tag{3.25}$$

For the proof, we need a lemma, which will be used in the proof of Proposition 3.13 again.

Lemma 3.10. *Let $b(T) \in O(A) \oplus \frac{1}{T}O_K[[\frac{1}{T}]]$ and $n \in \mathbb{Z}_{>0}$. If two elements c and π of $\mathcal{M}_K$ satisfy $|c| < |p^{n-1}|$ and $|\pi| \leq |p|^{1/(p^n - p^{n-1})}$, then we have*

$$[\exp(c \sum_{k=0}^{\infty} \frac{\pi^{p^k}}{p^k} b(T))] = 1 \qquad \text{in } \Gamma_A.$$

Proof. For all $k \in \mathbb{Z}_{\geq 0}$, we have

$$|c \cdot \frac{\pi^{p^k}}{p^k}| < |p|^{n-1-k+\frac{p^k}{p^n - p^{n-1}}} \leq |p|^{\frac{1}{p-1}}. \tag{3.26}$$

(The latter equality holds if and only if $k = n, n-1$.) Since the radius of convergence of $\exp(T)$ is $|p|^{1/(p-1)}$, it follows that $\exp(c\sum \frac{\pi^{p^k}}{p^k} a(T)) \in (A^{\mathrm{an}})^* \cap \Gamma$ for all $a(T) \in O(A^{\mathrm{an}})$, and $\exp(c\sum \frac{\pi^{p^k}}{p^k} g(T)) \in \Gamma_0$ for all $g(T) \in \frac{1}{T} O_K[[\frac{1}{T}]]$. We are done. □

Proof of Proposition 3.9. We calculate

$$\begin{aligned} h_{\boldsymbol{\mu}}(T;\vec{\pi})^{p^n} &= \exp\Big(\sum_{j=1}^{g}\sum_{k=0}^{\infty} \frac{\pi_j^{p^k}}{p^k} T^{\mu_j p^k}\Big)^{p^n} \\ &= \exp\Big(p^n \sum_{j=1}^{g}\sum_{k=0}^{\infty} \frac{\pi_j^{p^k}}{p^k} \Big(\sum_{i=1}^{g} e_{ij}^{(k)} T^{\mu_i} + b_j^{(k)}(T)\Big)\Big) \\ &\overset{(*)}{=} \exp\Big(p^n \sum_{j=1}^{g}\sum_{k=0}^{\infty} \frac{\pi_j^{p^k}}{p^k} b_j^{(k)}(T)\Big), \end{aligned}$$

where we used $\vec{l}(\vec{\pi}) = \vec{0}$ at $(*)$. Now Lemma 3.10 proves $[h_{\boldsymbol{\mu}}(T;\vec{\pi})^{p^n}] = 1$ in Γ_A. The injectivity of (3.25) follows from Proposition 3.7. □

The following proposition will be used in the proof of Theorem 1.5:

PROPOSITION 3.11. *Suppose that* $\det(\mathbf{e}^{(1)}) \in O_K^*$. *Then there exists a finite extension* K' *of* K *such that, upon replacing* K *by* K', *we have* $|T_1| = p^g$ *and the set*

$$\{\vec{\pi} = (\pi_1, \dots, \pi_g) \in T_1 \mid |\pi_g| = |p|^{1/(p-1)}\} \tag{3.27}$$

contains at least $p^g - p^{g-1}$ *elements.*

Proof. We shall use the following classical result [8, §3, Satz 10]: Let $\bar{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$. Let $L \in M_g(\mathbb{F})$, and let ρ be the rank of the matrix $LL^{(p)} \cdots L^{(p^{g-1})}$, where $L^{(p^i)}$ denotes the matrix obtained from L by raising all the entries to its p^i-th power. Then we have

$$\Big| \Big\{ \begin{pmatrix} u_1 \\ \vdots \\ u_g \end{pmatrix} \in \bar{\mathbb{F}}^{\oplus g} \;\Big|\; \begin{pmatrix} u_1 \\ \vdots \\ u_g \end{pmatrix} + L \begin{pmatrix} u_1^p \\ \vdots \\ u_g^p \end{pmatrix} = \vec{0} \Big\} \Big| = p^{\rho}. \tag{3.28}$$

Consequently, for any $L \in GL_g(\mathbb{F})$ we get

$$\Big| \Big\{ \begin{pmatrix} u_1 \\ \vdots \\ u_g \end{pmatrix} \in \bar{\mathbb{F}}^{\oplus g} \;\Big|\; \begin{pmatrix} u_1 \\ \vdots \\ u_g \end{pmatrix} + L \begin{pmatrix} u_1^p \\ \vdots \\ u_g^p \end{pmatrix} = \vec{0},\ u_g \neq 0 \Big\} \Big| \geq p^g - p^{g-1}. \tag{3.29}$$

To prove the proposition, we may suppose that there exists $\varpi \in K$ such that $\varpi^{p-1} = p$. Then we have

$$\frac{1}{\varpi} \vec{l}(\varpi X_1, \cdots, \varpi X_g) \equiv \begin{pmatrix} X_1 \\ \vdots \\ X_g \end{pmatrix} + \mathbf{e}^{(1)} \begin{pmatrix} X_1^p \\ \vdots \\ X_g^p \end{pmatrix} \mod \varpi.$$

By (3.28) and Hensel's lemma, after replacing K by its finite unramified extension, we get p^g elements $(u_1, \dots, u_g) \in O_K^{\oplus g}$ such that $\vec{l}(\varpi u_1, \cdots, \varpi u_g) = 0$, each of which gives rise to an element $(\pi_1, \dots, \pi_g) = (\varpi u_1, \dots, \varpi u_g)$ of T_1. Moreover, at least $p^g - p^{g-1}$ elements among them satisfy $|u_g| = 1$ by (3.29), and each of them gives rise to an element $(\pi_1, \dots, \pi_g) = (\varpi u_1, \dots, \varpi u_g)$ of the set (3.27). We are done. □

3.9. Cyclic group action. Let d be an integer such that $p \equiv 1 \mod d$ and let $\zeta_d \in \mathbb{Z}_p \subset K$ be a primitive d-th root of unity. We define a K-algebra automorphism $\delta : K((\frac{1}{T})) \to K((\frac{1}{T}))$ by $\delta(\sum_n a_n T^n) = \sum_n a_n (\zeta_d T)^n$. In this subsection, $A \subset K((\frac{1}{T}))$ is a K-subalgebra satisfying (2.4), (3.14) and the following condition:

(3.30) δ restricts to an automorphism of A.

We also assume

$$d \geq \mu_g. \tag{3.31}$$

By (3.31), we have $\mu_i \not\equiv \mu_j \mod d$ for any $1 \leq i < j \leq g$. Since the action of δ on $K((\frac{1}{T}))$ respects the decomposition (3.21), the matrix $\mathbf{e}^{(k)}$ introduced in (3.22) must be diagonal. In particular, we have

$$\det(\mathbf{e}^{(k)}) = e_{11}^{(k)} \cdots e_{gg}^{(k)}. \tag{3.32}$$

We define

$$l_i(X) = \sum_{k=0}^{\infty} \frac{e_{ii}^{(k)}}{p^k} X^{p^k} \ (i = 1, \ldots, g) \tag{3.33}$$

so that we have

$$\vec{l}(X_1, \cdots, X_g) = \begin{pmatrix} l_1(X_1) \\ \vdots \\ l_g(X_g)) \end{pmatrix}. \tag{3.34}$$

We also define for each $i \in \{1, \ldots, g\}$

$$T_{n,i} = \{\pi_i \in \mathcal{M}_K \mid l_i(\pi_i) = 0, \ |\pi_i| \leq |p|^{1/(p^n - p^{n-1})}\}$$

so that $T_n = T_{n,1} \times \cdots \times T_{n,g}$.

PROPOSITION 3.12. *Let $i \in \{1, \ldots, g\}$ and $n \in \mathbb{Z}_{>0}$. Suppose that $e_{ii}^{(k)} \in O_K^*$ for all $k \in \mathbb{Z}_{\geq 0}$. Then there exists a finite extension K' of K such that, upon replacing K by K',*

$$|T_{n,i}| = p^n. \tag{3.35}$$

Moreover, for any $\pi \in T_{n,i} \setminus \{0\}$ there exists $s \in \{1, \ldots, n\}$ such that $|\pi| = |p|^{1/(p^s - p^{s-1})}$. For any $s \in \{1, \ldots, n\}$, the cardinality of the set

$$\{\pi \in T_{n,i} \mid |\pi| = |p|^{1/(p^s - p^{s-1})}\} \tag{3.36}$$

is exactly $p^s - p^{s-1}$.

Proof. It is seen from the derivation that $l_i(X)$ has no multiple root. Then the proposition is deduced by looking at the Newton polygon (see, for example, [5, Proposition 2.9]). □

There exists a unique continuous K-algebra automorphism $H \to H$ which coincides with δ on $H \cap K((\frac{1}{T}))$. We denote this automorphism by the same letter δ.

It induces an automorphism Γ_A, which is also denoted by δ. For $\mu \in \mathbb{Z}/d\mathbb{Z}$ and a $\mathbb{Z}_p$-module M equipped with a $\mathbb{Z}_p$-linear automorphism δ of order d, we define

$$M_\mu := \{\alpha \in M \mid \delta\alpha = \zeta_d^\mu \alpha\}. \tag{3.37}$$

PROPOSITION 3.13. *Let $\pi \in T_{n,i}$ for some $n \in \mathbb{Z}_{>0}$ and $i \in \{1, \dots, g\}$, and let $h(T) := h(T^{\mu_i}; \pi)$ (see (3.11)). Then we have $[h(T)] \in \Gamma_A[p^n]_{\mu_i}$. Consequently, we get an injective map*

$$T_{n,i} \to \Gamma_A[p^n]_{\mu_i}, \qquad \pi \mapsto [h(T^{\mu_i}; \pi)]. \tag{3.38}$$

Proof. We see $[h(T)] \in \Gamma_A[p^n]$ from Proposition 3.9. In order to show $[h(T)] \in \Gamma_A[p^n]_{\mu_i}$, we take $s \in \mathbb{Z}$ such that $|\zeta_d - s| < |p^n|$. We need to show $\delta([h(T)]) = [h(T)^{s^{\mu_i}}]$. Recall that $h(T) = \exp(l(\pi T^{\mu_i}))$ where $l(T) = \sum_{k=0}^\infty \frac{1}{p^k} T^{p^k}$. Since $\delta(l(T)) = l(\zeta_d T) = \zeta_d l(T)$, we get (see (3.21)),

$$\begin{aligned}
\delta(h(T))h(T)^{-s^{\mu_i}} &= \exp((\zeta_d^{\mu_i} - s^{\mu_i}) \sum_{k=0}^\infty \frac{\pi^{p^k}}{p^k} T^{\mu_i p^k}) \\
&= \exp((\zeta_d^{\mu_i} - s^{\mu_i}) \sum_{k=0}^\infty \frac{\pi^{p^k}}{p^k} (e_{ii}^{(k)} T^{\mu_i} + b_i^{(k)}(T))) \\
&\overset{(*)}{=} \exp((\zeta_d^{\mu_i} - s^{\mu_i}) \sum_{k=0}^\infty \frac{\pi^{p^k}}{p^k} b_i^{(k)}(T)),
\end{aligned}$$

where we used $l_i(\pi) = 0$ at $(*)$. Now Lemma 3.10 completes the proof. □

4. Curves over p-adic fields.

4.1. Notations. We use the same notations for $p, K, |\cdot|, O_K, \mathcal{M}_K$ and $\mathbb{F}$ as in the previous section. Let π_K be a uniformizer of O_K. Let $\mathfrak{X}$ be a regular scheme over O_K such that the structure morphism $\mathfrak{X} \to \operatorname{Spec} O_K$ is separated, smooth and projective of relative dimension one with geometrically connected fibers. We write $X := \mathfrak{X} \otimes_{O_K} K$ (resp. $Y := \mathfrak{X} \otimes_{O_K} \mathbb{F}$) for the generic (resp. closed) fiber. Suppose that the genus g of X satisfies $g \geq 2$. Suppose also that there exists a section $\widetilde{\infty} : \operatorname{Spec} O_K \to \mathfrak{X}$ of the structure morphism. We regard the image of $\widetilde{\infty}$ as a reduced closed subscheme of $\mathfrak{X}$, which is also denoted by $\widetilde{\infty}$. We write $\infty = \widetilde{\infty} \otimes_{O_K} K$ (resp. $\overline{\infty} = \widetilde{\infty} \otimes_{O_K} \mathbb{F}$) for the generic (resp. closed) point of $\widetilde{\infty}$.

Recall that the inclusion map $j : X \to \mathfrak{X}$ (resp. $i : Y \to \mathfrak{X}$) induces an isomorphism $j^* : \operatorname{Pic}(\mathfrak{X}) \cong \operatorname{Pic}(X)$ (resp. a surjection $i^* : \operatorname{Pic}(\mathfrak{X}) \to \operatorname{Pic}(Y)$). The composition

$$\operatorname{Pic}(X) \overset{j^{*-1}}{\cong} \operatorname{Pic}(\mathfrak{X}) \overset{i^*}{\to} \operatorname{Pic}(Y), \qquad \mathcal{L} \mapsto \bar{\mathcal{L}} := i^* j^{*-1} \mathcal{L} \tag{4.1}$$

is called the *specialization*. The kernel of this map is denoted by $\widehat{\operatorname{Jac}}(X)$:

$$\widehat{\operatorname{Jac}}(X) := \{\mathcal{L} \in \operatorname{Pic}(X) \mid \bar{\mathcal{L}} = 0\}. \tag{4.2}$$

4.2. Existance of a good trivialization. Let $\hat{\mathcal{O}}_{\mathfrak{X},\overline{\infty}}$ be the completion of the local ring $\mathcal{O}_{\mathfrak{X},\overline{\infty}}$ of $\mathfrak{X}$ at $\overline{\infty}$, which is a regular two dimensional local O_K-algebra. The prime ideal $\mathcal{P}_{\widetilde{\infty}}$ of $\hat{\mathcal{O}}_{\mathfrak{X},\overline{\infty}}$ defined by $\widetilde{\infty}$ is of height one, hence principal. Thus there is an isomorphism

$$\mathcal{N}_0 : \hat{\mathcal{O}}_{\mathfrak{X},\overline{\infty}} \cong O_K[[\frac{1}{T}]] \tag{4.3}$$

of O_K-algebras such that $\mathcal{N}_0^{-1}((\frac{1}{T})) = \mathcal{P}_{\widetilde{\infty}}$. Note that we have $O_K[[\frac{1}{T}]] \subset K((\frac{1}{T})) \cap H$ and for any $f \in \hat{\mathcal{O}}_{\mathfrak{X},\overline{\infty}}$

$$\deg \mathcal{N}_0(f) = -v_{\widetilde{\infty}}(f), \qquad ||\mathcal{N}_0(f)|| = |\pi_K|^{v_Y(f)}, \tag{4.4}$$

where $v_{\widetilde{\infty}}$ (resp. v_Y) is the normalized discrete valuation on $\hat{\mathcal{O}}_{\mathfrak{X},\overline{\infty}}$ given by $\mathcal{P}_{\widetilde{\infty}}$ (resp. the height one prime ideal defined by Y). We write $\mathcal{N}$ for the induced embedding of the function field $K(X)$ of X into the fraction field of $O_K[[\frac{1}{T}]]$. The isomorphism $\mathcal{N}_0$ also induces four maps:

$$N_0 : \hat{\mathcal{O}}_{X,\infty} \cong K[[\frac{1}{T}]], \qquad \bar{N}_0 : \hat{\mathcal{O}}_{Y,\overline{\infty}} \cong \mathbb{F}[[\frac{1}{T}]],$$
$$N : \operatorname{Spec} K((\frac{1}{T})) \to X, \qquad \bar{N} : \operatorname{Spec} \mathbb{F}((\frac{1}{T})) \to Y.$$

We denote the composition map $\operatorname{Spec} O_K[[\frac{1}{T}]] \overset{\mathcal{N}_0}{\to} \operatorname{Spec} \hat{\mathcal{O}}_{\mathfrak{X},\widetilde{\infty}} \to \mathfrak{X}$ (resp. $\operatorname{Spec} K[[\frac{1}{T}]] \overset{N_0}{\to} \operatorname{Spec} \hat{\mathcal{O}}_{X,\infty} \to X$, resp. $\operatorname{Spec} \mathbb{F}[[\frac{1}{T}]] \overset{\bar{N}_0}{\to} \operatorname{Spec} \hat{\mathcal{O}}_{Y,\widetilde{\infty}} \to Y$) by the same letter $\mathcal{N}_0$ (resp. N_0, resp. $\bar{N}_0$).

Using N and $\bar{N}$, we define (see (2.7)).

$$A = A(X, \infty, N) \subset K((\frac{1}{T})), \qquad B = A(Y, \overline{\infty}, \bar{N}) \subset \mathbb{F}((\frac{1}{T})). \tag{4.5}$$

Proposition 4.1.

1. *The element A of $\mathrm{Gr}^{\mathrm{alg}}(K)$ is integral (see Definition 3.1 (2)).*
2. *If $WG_\infty(X) = WG_{\overline{\infty}}(Y)$, then A is strictly integral (see Definition 3.1 (3)).*

We will prove a more general proposition. Define a subset of X by

$$D_* := \{P \mid P \text{ is a closed point of } X \text{ whose reduction is } \overline{\infty}\} \setminus \{\infty\}. \tag{4.6}$$

Proposition 4.1 is a special case of the following proposition applied to $D = 0$:

Proposition 4.2. *Let D be a divisor on X such that $\operatorname{Supp}(D) \cap D_* = \emptyset$. Let $(\mathcal{L}, \sigma) := (\mathcal{O}_X(D), \sigma(D))$ be the Krichever pair constructed in §2.6. Then we have the following.*

1. *The element $V(\mathcal{L}, \sigma)$ of $\mathrm{Gr}^{\mathrm{alg}}(K)$ is integral.*
2. *If moreover $\underline{M}(\mathcal{L}) = \underline{M}(\bar{\mathcal{L}})$ (see (4.1)), then $V(\mathcal{L}, \sigma)$ is strictly integral.*

For the proof, we need a lemma.

Lemma 4.3. *Let $f \in K(X)$ be a rational function on X that has no pole on D_*. Then, we have $\mathcal{N}(f) \in O_K[[\frac{1}{T}]][\frac{1}{\pi_K}, T]$. In particular, we have $||\mathcal{N}(f)|| < \infty$.*

Proof. Since f can be written as a ratio of two elements of $\mathcal{O}_{\mathfrak{X},\overline{\infty}} (\subset \hat{\mathcal{O}}_{\mathfrak{X},\overline{\infty}})$, Weierstrass preparation theorem shows that there are two distinguished polynomials $P(\frac{1}{T}), Q(\frac{1}{T}) \in O_K[\frac{1}{T}]$, $n \in \mathbb{Z}$, and $u(T) \in O_K[[\frac{1}{T}]]^*$ such that $\mathcal{N}(f) =$

$\pi_K^n P(\frac{1}{T})Q(\frac{1}{T})^{-1}u(T)$. Since a zero of a distinguished polynomial has absolute value < 1, the assumption implies that Q can be chosen so that it has no zero other than $\frac{1}{T} = 0$, that is, $Q(\frac{1}{T}) = T^m$ for some $m \in \mathbb{Z}$. □

Proof of Proposition 4.2. The lemma proves that $V := V(\mathcal{L}, \sigma)$ is bounded. With the notations in (4.1), we set $\tilde{\mathcal{L}} = j^{*-1}(\mathcal{L})$ and $\bar{\mathcal{L}} = i^*\tilde{\mathcal{L}}$. Recall that the N-trivialization $\sigma : N^*\mathcal{L} \cong K((\frac{1}{T}))$ comes from an isomorphism $\sigma_0 : N_0^*\mathcal{L} \cong K[[\frac{1}{T}]]$. By the assumption $\mathrm{Supp}(D) \cap D_* = \emptyset$, there exists a unique isomorphism $\tilde{\sigma}_0$ which fits into a commutative diagram

$$\begin{array}{ccc} N_0^*\mathcal{L} & \overset{\sigma_0}{\cong} & K[[\frac{1}{T}]] \\ \cup & & \cup \\ \mathcal{N}_0^*\tilde{\mathcal{L}} & \overset{\tilde{\sigma}_0}{\cong} & O_K[[\frac{1}{T}]]. \end{array}$$

By restricting $\tilde{\sigma}_0$ to Y, we get an isomorphism $\bar{\sigma}_0 : \bar{N}_0^*\bar{\mathcal{L}} \cong \mathbb{F}[[\frac{1}{T}]]$, which induces an $\bar{N}$-trivialization $\bar{\sigma}$ of $\bar{\mathcal{L}}$. By construction, we have $V(\bar{\mathcal{L}}, \bar{\sigma}) = V^{\mathrm{red}}$ (see (3.2)). Since the degree of an invertible sheaf is preserved by the specialization (4.1), $\underline{M}(V^{\mathrm{red}})$ is a Maya diagram having the same index with $\underline{M}(V)$. Now (1) follows from Proposition 3.2 (1). (2) follows from (1) and Proposition 3.2 (2). □

4.3. p^n-torsion points of the Jacobian. From now on we suppose $WG_\infty(X) = WG_{\overline{\infty}}(Y)$. Then A (which we defined in (4.5)) is strictly integral by Proposition 4.1, hence we can apply the results of §3.8. Let $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_g)$ be as in (2.9). Let $n \in \mathbb{Z}_{>0}$. In view of (3.8), the composition of (3.25), (3.16) and (2.12) defines an injective map (see (4.2))

$$T_n \to \widehat{\mathrm{Jac}}(X)[p^n] \qquad \vec{\pi} \mapsto [h_{\boldsymbol{\mu}}(T; \vec{\pi})A]_A. \tag{4.7}$$

(See (3.13) for the definition of $h_{\boldsymbol{\mu}}(T; \vec{\pi})$.)

PROPOSITION 4.4. *Suppose that Y is ordinary and that $p \geq 2g$. Then there exists a finite extension K' of K such that, upon replacing K by K', we have $|T_1| = p^g$ and* (4.7) *is bijective for $n = 1$.*

Proof. Let $\mathbf{e}^{(k)} \in M_g(O_K)$ be the matrix introduced in (3.22). Since Y is ordinary and $p \geq 2g$, Proposition 2.6 shows that $\det(\mathbf{e}^{(1)}) \in O_K^*$. By Proposition 3.11, it holds that $|T_1| = p^g$ if we replace K by its finite extension. On the other hand, we have $|\widehat{\mathrm{Jac}}(X)[p]| \leq p^g$ because Y is ordinary. Since (4.7) is injective, it is surjective as well. □

4.4. Proof of Theorem 1.5. The statement of the theorem is not affected by the base change of the base field K. By Proposition 3.11, we may assume that the set (3.27) contains at least $p^g - p^{g-1}$ elements. Let $\vec{\pi}$ be an element of (3.27) and set $h(T) := h_{\boldsymbol{\mu}}(T; \vec{\pi})$. In view of Proposition 4.4, it suffices to show $[h(T)A]_A \notin \Theta$.

The assumption (3) implies that $\boldsymbol{\mu} = (1, 2, \ldots, g)$ and $\kappa(A) = (g, 0, 0, \ldots)$. By Proposition 3.6, we get $h(T)A \cap T^{g-1}K[[\frac{1}{T}]] = 0$. Now Theorem 2.3 (2d) shows $[h(T)A]_A \notin \Theta$. This completes the proof of Theorem 1.5. □

4.5. Formal group. The main result of this subsection is Theorem 4.5 below. This result will not be used in the proof of our main results, but it might be interesting for its own sake.

Let J_X/K be the Jacobian variety of X so that $J_X(K) \cong \mathrm{Jac}(X)$. Let $\mathcal{J}_X/O_K$ (resp. $\hat{J}_X/O_K$) be the Néron model (resp. the formal group) of J_X. The group of O_K-rational points $\hat{J}_X(O_K)$ on $\hat{J}_X$ is naturally identified with $\widehat{\mathrm{Jac}}(X)$ (see (4.2)).

THEOREM 4.5. *Suppose $p \geq 2g$, $WG_\infty(X) = WG_{\overline{\infty}}(Y)$ and that K is absolutely unramified. Then the vector $\vec{l}(X_1, \cdots, X_g)$ defined in* (3.23) *gives a logarithm function of a formal group over O_K which is isomorphic to $\hat{J}_X$.*

Proof. We recall basic facts in [12]. Let $(V, 0)$ be a pointed formal Lie variety over O_K. The coordinate ring $A(V)$ of the formal Lie variety V is just the formal power series ring $O_K[[X_1, \ldots, X_n]]$ and 0 is a distinguished O_K-valued point of V. We also denote by $V_K := V \otimes_{O_K} K$ the formal Lie variety over K obtained by the extension of scalars. The coordinate ring $A(V_K)$ is by definition the formal power series ring $K[[X_1, \ldots, X_n]]$. For example, the formal completion $\widehat{\mathfrak{X}}$ at the closed point $\overline{\infty}$ of $\mathfrak{X}$ and $\hat{J}_X$ are such pointed varieties. The de Rham cohomology $H^i_{\mathrm{dR}}(V/O_K)$ is defined as the O_K-module obtained by taking the i-th cohomology groups of the formal de Rham complex of V/O_K. Then by the formal Poincaré lemma, we have canonically

$$H^1_{\mathrm{dR}}(V/O_K) = \{f \in A(V_K)_0 \,|\, df \text{ is integral}\}/A(V)_0,$$

where we set

$$A(V)_0 := \{f \in A(V) \mid f(0) = 0\}, \quad A(V_K)_0 := \{f \in A(V_K) \mid f(0) = 0\}.$$

Suppose that $(V, 0)$ has a structure of commutative formal Lie groups with the identity 0. Let m, p_1, p_2 be the sum and projections $V \times V \to V$. An element a of $H^1_{\mathrm{dR}}(V/O_K)$ is called primitive if it satisfies

$$m^*a = p_1^*a + p_2^*a \qquad \text{in} \quad H^1_{\mathrm{dR}}(V \times V/O_K).$$

We define the Dieudonné module $\mathbb{D}(V/O_K)$ of V/O_K as the subgroup of $H^1_{\mathrm{dR}}(V/O_K)$ consisting of primitive elements. Explicitly, we have

$$\mathbb{D}(V/O_K) = \{f \in A(V_K)_0 \,|\, df,\ f(X[+]Y) - f(X) - f(Y) \text{ are integral}\}/A(V)_0$$

where $[+]$ denotes the addition of V.

To use Honda's theory of commutative formal groups, we also need a variant. We let

$$H^1_{\mathrm{dR}}(V/O_K; (p)) = \{f \in A(V_K)_0 \,|\, df \text{ is integral}\}/pA(V)_0$$

and define $\mathbb{D}(V/O_K; (p))$ to be

$$\{f \in A(V_K)_0 \,|\, df \text{ is integral},\ f(X[+]Y) - f(X) - f(Y) \in pO_K[[X, Y]]\}/pA(V)_0.$$

The Frobenius map

$$F : K[[X_1, \ldots, X_g]] \to K[[X_1, \ldots, X_g]], \quad f(X_1, \ldots, X_g) \mapsto f^\varphi(X_1^p, \ldots, X_g^p)$$

induces the Frobenius action F on these cohomology groups where φ is the Frobenius of $\mathrm{Gal}(K/\mathbb{Q}_p)$. (Actually, one can replace φ by any $\mathbb{Z}_p$-algebra automorphism φ_1 of K satisfying $x^{\varphi_1} \equiv x \mod p$ for all $x \in O_K$.) Then $p^{-1}F$ induces φ-linear isomorphisms

$$H^1_{\mathrm{dR}}(V/O_K; (p)) \cong H^1_{\mathrm{dR}}(V/O_K), \quad \mathbb{D}(V/O_K, (p)) \cong \mathbb{D}(V/O_K).$$

We also get isomorphisms

$$H^1_{\mathrm{dR}}(V/O_K;(p))\otimes K\cong H^1_{\mathrm{dR}}(V/O_K)\otimes K,\quad \mathbb{D}(V/O_K;(p))\otimes K\cong \mathbb{D}(V/O_K)\otimes K.$$

Let $\underline{\omega}_{V/O_K}$ be the space of invariant differentials of V/O_K. Then we have a canonical map $\underline{\omega}_{V/O_K}\to \mathbb{D}(V/O_K,(p))$ given by integration. If there is no non-trivial O_K-group homomorphism from V to $\mathbb{G}_a$, then this map is injective and we may regard $\underline{\omega}_{V/O_K}$ as a subspace of $\mathbb{D}(V/O_K,(p))$. Furthermore, if V is of finite height h, then $\mathbb{D}(V/O_K,(p))$ is a free O_K-module of rank h and is generated by $\underline{\omega}_{V/O_K}$ as an $O_K[F]$-module. Here $O_K[F]$ is an O_K-algebra generated by F subject to a relation $Fa=a^{\varphi}F$ for all $a\in O_K$. (This algebra is non-commutative unless $O_K=\mathbb{Z}_p$).

Now we return to the proof of Theorem 4.5. We follow the same argument as in [12, §VI]. Let $\omega_1,\dots,\omega_g$ be the Hermite basis of X with expansion (2.15). From (3.21), we see that the elements $e_{ij}^{[m]}$ defined in (2.16) belong to O_K for any m,i,j. By Proposition 2.5, we have $c_{ij}\in O_K$ for all i,j, and $\omega_1,\dots,\omega_g$ form an O_K-basis of $H^0(\mathfrak{X},\Omega^1_{\mathfrak{X}/O_K})$. By the Albanese map $\mathfrak{X}\to\mathcal{J}_X$ defined by using $\widetilde{\infty}$, we have a canonical isomorphism

$$H^0(\mathfrak{X},\Omega^1_{\mathfrak{X}/O_K})\cong H^0(\mathcal{J}_X,\Omega^1_{\mathcal{J}_X/O_K})$$

and regard $\omega_1,\dots,\omega_g$ as elements of $H^0(\mathcal{J}_X,\Omega^1_{\mathcal{J}_X/O_K})$. Then by the formal completion, we have a basis $\hat{\omega}_1,\dots,\hat{\omega}_g$ of $\underline{\omega}_{\hat{J}_X/O_K}\subset\mathbb{D}(\hat{J}_X/O_K,(p))$. By [10, Proposition 3.3], there exists an element

$$u(F)=p+\sum_{i=1}^{\infty}B_iF^i\in M_g(O_K)[[F]]$$

such that

$$u(F)\begin{pmatrix}\hat{\omega}_1\\ \vdots\\ \hat{\omega}_g\end{pmatrix}=0\qquad\text{in}\quad \mathbb{D}(\hat{J}_X/O_K;(p)),$$

which can be seen as an equality in $H^1_{\mathrm{dR}}(\mathfrak{X}/O_K;(p))$ as well. We write

$$\begin{pmatrix}\hat{\omega}_1\\ \vdots\\ \hat{\omega}_g\end{pmatrix}=\sum_{j=1}^{\infty}\begin{pmatrix}c_{1j}\\ \vdots\\ c_{gj}\end{pmatrix}(\frac{1}{T})^{j-1}d(\frac{1}{T})=\sum_{j=1}^{\infty}\vec{c}_j(\frac{1}{T})^{j-1}d(\frac{1}{T}).$$

It follows that

$$u(F)\left(\sum_{j=1}^{\infty}\frac{\vec{c}_j}{j}(\frac{1}{T})^j\right)\in pO_K[[\frac{1}{T}]]^{\oplus g}.$$

By looking the n-th coefficients, we have

$$p\frac{\vec{c}_n}{n}+B_1\frac{(\vec{c}_{n/p})^{\varphi}}{n/p}+\cdots+B_k\frac{(\vec{c}_{n/p^k})^{\varphi^k}}{n/p^k}+\cdots\in pO_K^{\oplus g}$$

where we regard as $\vec{c}_m = 0$ if m is not an integer. Hence we have

$$u(F)\left(\sum_{k=0}^{\infty}\frac{1}{p^k}\left(\vec{c}_{p^k\mu_1}X_1^{p^k}+\cdots+\vec{c}_{p^k\mu_g}X_g^{p^k}\right)\right)\in\ pO_K[[X_1,\cdots X_g]]^{\oplus g}.$$

On the other hand, the formal power series $\sum_{k=0}^{\infty}\frac{1}{p^k}(\vec{c}_{p^k\mu_1}X_1^{p^k}+\cdots+\vec{c}_{p^k\mu_g}X_g^{p^k})$ coincides with $\vec{l}(X_1,\cdots,X_g)$ by Proposition 2.5. By our choice of the Hermite basis, $\mathbf{e}^{(0)}$ is the identity matrix. Therefore, the logarithm of $\hat{J}_X$ and $\vec{l}(X_1,\cdots,X_g)$ have the same Honda type with the same linear term. By [10, Theorem 2], $\vec{l}(X_1,\cdots,X_g)$ is the logarithm of a formal group over O_K that is strictly isomorphic to the formal group $\hat{J}_X$. □

4.6. Good trivialization with respect to a given automorphism. Assume now that we are given an automorphism $\delta : X \to X$ over K of order d such that $\delta(\infty) = \infty$. We also assume $d \geq 2g-1$ and $p \equiv 1 \mod d$. (From Corollary 4.10 onward, we will assume $d \geq 2g+1$.) Note that this implies $p \geq 2g > \mu_g$ (see (2.9)), and hence both (3.30) and (3.31) are satisfied. Let $\zeta_d = (t/\delta^*(t))(\infty) \in K^*$ be the value of the rational function $t/\delta^*(t)$ at ∞, where t is a uniformizer at ∞. Note that ζ_d is independent of the choice of t. It follows from the following proposition that ζ_d is a primitive d-th root of unity.

PROPOSITION 4.6. *The isomorphism* (4.3) *can be chosen so that the following diagram is commutative:*

$$\begin{array}{ccc}\operatorname{Spec} K((\frac{1}{T})) & \stackrel{N}{\to} & X\\ \downarrow & & \downarrow\delta\\ \operatorname{Spec} K((\frac{1}{T})) & \stackrel{N}{\to} & X,\end{array}\tag{4.8}$$

where the left vertical map is given by $\sum a_iT^i \mapsto \sum a_i(\zeta_dT)^i$.

Proof. We first take an arbitrary isomorphism (4.3). Denote by the same letter δ the automorphism $O_K[[\frac{1}{T}]] \to O_K[[\frac{1}{T}]]$ induced by δ through (4.3). It suffices to show that there is a unit $u(T) \in O_K[[\frac{1}{T}]]^*$ such that $\delta(u(T)\cdot\frac{1}{T}) = \zeta_d^{-1}u(T)\cdot\frac{1}{T}$.

Since the ideal $(\frac{1}{T})$ is preserved by δ, there exists $v(T) \in O_K[[\frac{1}{T}]]^*$ such that $\delta(\frac{1}{T}) = v(T)\frac{1}{T}$. Write $v(T) = \zeta v_1(T)$ with $\zeta \in O_K^*$ and $v_1(T) \in 1 + \frac{1}{T}O_K[[\frac{1}{T}]]$. Since the order of δ is d, we have

$$\prod_{i=0}^{d-1}\delta^i(v_1(T)) = 1 \qquad \text{and} \qquad \zeta^d = 1.\tag{4.9}$$

Define $u(T) = \sum_{i=0}^{d-1}\prod_{j=0}^{i}\delta^j(v_1(T))$. Since $u(T) \equiv d \mod (\frac{1}{T})$, we have $u(T) \in O_K[[\frac{1}{T}]]^*$. On the other hand, we have $v_1(T)\delta(u(T)) = u(T)$ by (4.9). Therefore we get $\delta(u(T)\cdot\frac{1}{T}) = \zeta u(T)\cdot\frac{1}{T}$. Then we see $\zeta = \zeta_d^{-1}$ by the definition of ζ_d. We are done. □

From now on, we choose the isomorphism (4.3) in such a way that the diagram (4.8) commutes. By abuse of notation, we denote by δ the isomorphism $K((\frac{1}{T})) \to K((\frac{1}{T}))$ given by $\sum a_iT^i \mapsto \sum a_i(\zeta_dT)^i$.

REMARK 4.7. Suppose further that the assumptions of Theorem 4.5 are satisfied. Then the formal power series $l_i(X)$ defined in (3.33) is the logarithm of a formal group

$\hat{J}_{X,i}$ over O_K for all $i = 1, \dots, g$. Moreover, we have an isomorphism of formal groups over O_K

$$\hat{J}_X \cong \bigoplus_{i=1}^{g} \hat{J}_{X,i}. \tag{4.10}$$

This follows immediately from Theorem 4.5 and (3.34).

4.7. Decomposition of torsion points. We use the notation introduced in (3.37).

PROPOSITION 4.8. *Let $n \in \mathbb{Z}_{>0}$ and $\mu \in \mathbb{Z}/d\mathbb{Z}$. Suppose that K contains all p^n-torsion points on* $\mathrm{Jac}(X)$*, that is,* $|\mathrm{Jac}(X)[p^n]| = p^{2ng}$.

1. *If $\mu \equiv \mu_i \mod d$ for some $i = 1, \cdots, g$, then $\widehat{\mathrm{Jac}}(X)[p^n]_\mu$ is a cyclic group of order p^n. Otherwise, $\widehat{\mathrm{Jac}}(X)[p^n]_\mu = 0$.*
2. *Set $M_\pm := \{\pm\mu_i \mod d \mid i = 1, \dots, g\} \subset \mathbb{Z}/d\mathbb{Z}$ and define*

$$\rho := \begin{cases} 0 & \text{if } \mu \notin M_+ \cup M_- \\ 2 & \text{if } \mu \in M_+ \cap M_- \\ 1 & \text{otherwise.} \end{cases}$$

Then $\mathrm{Jac}(X)[p^n]_\mu$ is a free $\mathbb{Z}/p^n\mathbb{Z}$-module of rank ρ.

Proof. Let $T_p\hat{J}_X$ be the Tate module of the formal group $\hat{J}_X/O_K$ associated to the Jacobian variety of X. By Tate's theorem [25], we have

$$T_p\hat{J}_X \otimes_{\mathbb{Z}_p} \mathbb{C}_p \cong \mathrm{Hom}_K(H^0(X, \Omega^1_{X/K}), \mathbb{C}_p),$$

where $\mathbb{C}_p$ is the completion of an algebraic closure of K. On the other hand, it is shown in [14, Theorem 5] that

$$\det(t \cdot \mathrm{id} - \delta | H^0(X, \Omega^1_{X/K})) = \prod_{i=1}^{g} (t - \zeta_d^{-\mu_i}).$$

Combining two results, we get $\det(t \cdot \mathrm{id} - \delta | T_p\hat{J}_X) = \prod_{i=1}^{g}(t - \zeta_d^{\mu_i})$. Recall that we assumed $2g - 1 \leq d$ so that $\mu_i \not\equiv \mu_j \mod d$ for any $1 \leq i < j \leq g$. Now (1) follows from the isomorphisms $\widehat{\mathrm{Jac}}(X)[p^n] \cong T_p\hat{J}_X/p^nT_p\hat{J}_X$. (2) is a standard consequence of (1). □

4.8. μ-part of the torsion points. For $n \in \mathbb{Z}_{>0}$ and $i \in \{1, \dots, g\}$, the composition of (3.38), (3.16) and (2.12) defines an injective map

$$T_{n,i} \to \widehat{\mathrm{Jac}}(X)[p^n]_{\mu_i} \qquad \pi \mapsto [h(T^{\mu_i}; \pi)A]_A. \tag{4.11}$$

(See (3.11) for the definition of $h(T; \pi)$.)

PROPOSITION 4.9. *Let $n \in \mathbb{Z}_{>0}$ and $i \in \{1, \dots, g\}$. Suppose that $e_{ii}^{(1)} \in O_K^*$. Then there exists a finite extension K' of K such that, upon replacing K by K', we have $|T_{n,i}| = p^n$ and* (4.11) *is bijective.*

Proof. Recall that the matrix $\mathbf{e}^{(k)} = (e_{ij}^{(k)})$ introduced in (3.22) is diagonal (see the remark before (3.32)). From Proposition 2.5 and (2.17), we have $e_{ii}^{(k)} \in O_K^*$ for all

k. By Proposition 3.12 it holds that $|T_{n,i}| = p^n$ if we replace K by its finite extension. On the other hand, we have $|\widehat{\mathrm{Jac}}(X)[p^n]_{\mu_i}| \leq p^n$ by Proposition 4.8 (1). Since (4.11) is injective, it is surjective as well. □

COROLLARY 4.10. *Suppose $d \geq 2g+1$ and $e_{11}^{(1)} \in O_K^*$. Let $n \in \mathbb{Z}_{>0}$. Then there exists a finite extension K' of K such that, upon replacing K by K', we have $|T_{n,1}| = p^n$ and we have a bijection*

$$T_{n,1} \to \mathrm{Jac}(X)[p^n]_1 \qquad \pi \mapsto [h(T;\pi)A]_A. \tag{4.12}$$

Proof. Recall that we have $1 = \mu_1 < \cdots < \mu_g \leq 2g-1$ (see (2.9)). Hence the assumption $d \geq 2g+1$ implies that $1 = \mu_1 \in M_+ \setminus M_-$ in Proposition 4.8 (2). It follows that $\mathrm{Jac}(X)[p^n]_1 = \widehat{\mathrm{Jac}}(X)[p^n]_1$. The proposition applied to $i = 1$ completes the proof. □

THEOREM 4.11. *Let D be a divisor on X such that $\delta^*(D) = D$, $\deg D = 0$ and $\mathrm{Supp}(D) \cap D_* = \emptyset$ (see (4.6)). Let $(\mathcal{L}, \sigma) := (\mathcal{O}_X(D), \sigma(D))$ be the Krichever pair constructed in §2.6. Suppose $WG_\infty(X) = WG_{\overline{\infty}}(Y)$, $WG_\infty(\mathcal{L}) = WG_{\overline{\infty}}(\bar{\mathcal{L}})$, $e_{11}^{(1)} \in O_K^*$, $p \equiv 1 \mod d$ and $d \geq 2g+1$. Then we have for any $n \in \mathbb{Z}_{>0}$*

$$\mathrm{Jac}(X)[p^n]_1 \cap (\Theta - \mathcal{L}) \subset \{0\}.$$

Proof. By Proposition 4.2, $V := V(\mathcal{L}, \sigma) \in \mathrm{Gr}_A^{\mathrm{alg}}(K)$ is strictly integral. By Proposition 3.12, we may assume $|T_{n,1}| = p^n$. Let $\pi \neq 0$ be an element of (3.36) for some $s \in \{1, \ldots, n\}$ and set $h(T) := h(T;\pi)$. In view of Corollary 4.10, it suffices to show $[h(T)V]_A \notin \Theta$.

From (2.14) we see $\kappa_1(V) + l(\kappa(V)) \leq 2g \leq d-1 < p$. By Proposition 3.6, we get $h(T)V \cap T^{g-1}K[[\frac{1}{T}]] = 0$. Now Theorem 2.3 (2d) shows $[h(T)V]_A \notin \Theta$. This completes the proof of Theorem 4.11. □

4.9. Proof of Theorem 1.4. From (3.32) and Proposition 2.6, we have $e_{11}^{(1)} \in O_K^*$ if Y is ordinary. Thus Theorem 1.4 follows from Theorem 4.11 applied to $D = 0$. □

5. Examples.

5.1. Cyclic quotient of a Fermat curve. In this subsection, we work under the assumption and notations in Thm. 1.2. We shall prove the following result, which implies Thm. 1.2 as a special case $\mathcal{L} = 0$.

THEOREM 5.1. *Let $\mathcal{L} \in \mathrm{Jac}(X)$ be such that $\delta^*(\mathcal{L}) = \mathcal{L}$. Then, for any $n \in \mathbb{Z}_{>0}$, we have*

$$\mathrm{Jac}(X)[p^n]_1 \cap (\Theta - \mathcal{L}) \subset \{0\}.$$

REMARK 5.2. Anderson [1] proved Thm. 5.1 for $n = 1$.

Proof. It follows from [4, Proposition 5.1] that the assumption $p \equiv 1 \mod d$ implies that Y is ordinary. (See also Remark 5.4 below.) For $i = 0, 1$, let P_i be the closed points on X characterized by $x(P_i) = i$, $y(P_i) = 0$, so that we have $\delta(P_i) = P_i$.

The assumption implies that there is a $j \in \{0, 1, \cdots, d-1\}$ such that $\mathcal{L} \cong \mathcal{O}_X(j(P_0 - P_1))$ (cf. [1, §4.2]). An elementary computation shows

$$WG_\infty(\mathcal{L}) = WG_{\overline{\infty}}(\bar{\mathcal{L}}) = \{i \in \{0, \ldots, d-1\} \mid \langle \frac{ia+j}{d} \rangle + \langle \frac{i(d+1-a)-j}{d} \rangle - \langle \frac{i}{d} \rangle = 1\}$$

where $\langle\cdot\rangle$ is the fractional part function. Hence all the assumptions of Theorem 4.11 are satisfied, and Theorem 5.1 follows. □

In [1], Anderson computed the decomposition (3.22) explicitly for $k = 1$. His computation can easily be generalized to $k > 1$. Combined with Theorem 4.5, this result gives rise to an explicit formula for the formal group of the Jacobian variety of X. In the rest of this subsection, we work out such a formula.

Set $b := d + 1 - a$. There exists a unique $u(T) \in 1 + \frac{1}{T}\mathbb{Z}[[T]]$ such that

$$u(T)^{b-1} = (u(T) - \frac{1}{T^d})^b.$$

We define $x(T) := T^d u(T)$, $y(T) := T^{d+1}u(T) = Tx(T) \in \mathbb{Z}[[\frac{1}{T}]][T]$ so that $x(T) \equiv T^d \mod T^{d-1}\mathbb{Z}[[\frac{1}{T}]]$ and $y(T) \equiv T^{d+1} \mod T^d\mathbb{Z}[[\frac{1}{T}]]$. One checks $y(T)^d = x(T)^a(x(T)-1)^b$. We get an embedding of $\mathbb{Q}_p$-algebras

$$H^0(X \setminus \{\infty\}, \mathcal{O}_X) \hookrightarrow \mathbb{Q}_p((\frac{1}{T})) \tag{5.1}$$

which sends x and y to $x(T)$ and $y(T)$ respectively. We define the trivialization N_0 to be the one induced by (5.1).

Let $k \in \mathbb{Z}_{\geq 0}$ and write $p^k - 1 = dm$ ($m \in \mathbb{Z}_{\geq 0}$). We have

$$T^{p^k-1} = (\frac{y(T)^d}{x(T)^d})^m = (\frac{x(T)^a(x(T)-1)^b}{x(T)^d})^m = x(T)^m(1 - \frac{1}{x(T)})^{bm}.$$

It follows that

$$T^{p^k} = \sum_{i=m-bm}^{m} \gamma_i^{(k)} x(T)^i T, \qquad \gamma_i^{(k)} = (-1)^{i-m}\binom{mb}{m-i} \in \mathbb{Z}.$$

(Here we define $\binom{0}{0} = 1$ by convention.) If $i > 0$, then $x(T)^i T = x(T)^{i-1}y(T) \in O(A)$. If $i < 0$, then $x(T)^i T \in \frac{1}{T}\mathbb{Z}_p[[\frac{1}{T}]]$. This shows that

$$b_1^{(k)}(T) = \sum_{i\neq 0} \gamma_i^{(k)} x(T)^i T, \qquad e_{1,1}^{(k)} = \gamma_0^{(k)} = \binom{\frac{p^k-1}{d}b}{\frac{p^k-1}{d}} \tag{5.2}$$

in (3.22). Recall that we have a decomposition $\hat{J}_X \cong \oplus_{i=1}^g \hat{J}_{X,i}$ of the formal group $\hat{J}_X/\mathbb{Z}_p$ associated to the Jacobian variety of X (see (4.10)). By Remark 4.7, we get the following result (compare [12]).

Proposition 5.3. *The formal power series*

$$l_1(X) = \sum_{k=0}^{\infty} \frac{1}{p^k}\binom{\frac{p^k-1}{d}b}{\frac{p^k-1}{d}} X^{p^k}$$

is the logarithm function of a formal group over $\mathbb{Z}_p$, which is isomorphic to $\hat{J}_{X,1}/\mathbb{Z}_p$.

Remark 5.4. In the proof of Theorem 1.2, we made a use of a result in [4]. However, what we actually needed is $e_{11}^{(1)} \in \mathbb{Z}_{(p)}^*$, and this follows from (5.2).

5.2. Other examples. We collect a few more examples for which Theorem 4.11 can be applied. All results can be proved by the same way as Theorem 1.2 and Proposition 5.3, hence the proofs are omitted.

EXAMPLE 5.5. (Compare [15].) Let $g \geq 2$ be an integer such that $p \equiv 1 \mod d := 4g$. Let X be the hyperelliptic curve of genus g over $\mathbb{Q}_p$ defined by $y^2 = x^{2g+1} + x$. Let ∞ be the unique point on X which does not lie above its affine part. Fix a primitive d-th root of unity $\zeta_d \in \mathbb{Q}_p^*$, and define an automorphism δ of X by $\delta(x, y) = (\zeta_d^2 x, -\zeta_d y)$. The order of δ is d. Then we have the following for any $n \in \mathbb{Z}_{>0}$:

1. It holds $\mathrm{Jac}(X)[p^n]_1 \cap \Theta = \{0\}$.
2. The formal power series

$$l_1(X) = \sum_{k=0}^{\infty} \frac{1}{p^k} \begin{pmatrix} \frac{p^k-1}{2} \\ \frac{p^k-1}{4g} \end{pmatrix} X^{p^k}$$

is the logarithm function of a formal group over $\mathbb{Z}_p$, which is isomorphic to $\hat{J}_{X,1}/\mathbb{Z}_p$.

EXAMPLE 5.6. Let l be a prime such that $p \equiv 1 \mod d := l(l+1)$. Let X be the smooth projective model of an affine curve over $\mathbb{Q}_p$ defined by $y^l = x^{l+1} + 1$. The genus of X is $g = l(l-1)/2$. Let ∞ be the unique point on X which does not lie above its affine part. Fix a primitive d-th root of unity $\zeta_d \in \mathbb{Q}_p^*$, and define an automorphism δ of X by $\delta(x, y) = (\zeta_d^l x, \zeta_d^{l+1} y)$. The order of δ is d. Then we have the following for any $n \in \mathbb{Z}_{>0}$:

1. It holds $\mathrm{Jac}(X)[p^n]_1 \cap \Theta = \{0\}$.
2. The formal power series

$$l_1(X) = \sum_{k=0}^{\infty} \frac{1}{p^k} \begin{pmatrix} \frac{p^k-1}{l} \\ \frac{p^k-1}{l+1} \end{pmatrix} X^{p^k}$$

is the logarithm function of a formal group over $\mathbb{Z}_p$, which is isomorphic to $\hat{J}_{X,1}/\mathbb{Z}_p$.

EXAMPLE 5.7. Let l be an odd prime such that $p \equiv 1 \mod d := 2l$. Let X be the smooth projective model of an affine curve over $\mathbb{Q}_p$ defined by $y^l = x^{2a}(x^2+1)^b$, where a, b are positive integers such that $2(a+b) = l+1$. The genus of X is $g = l-1$. Let ∞ be the unique point on X which does not lie above its affine part. Fix a primitive l-th root of unity $\zeta_l \in \mathbb{Q}_p^*$, and define an automorphism δ of X by $\delta(x, y) = (-x, \zeta_l y)$. The order of δ is d. Then we have the following for any $n \in \mathbb{Z}_{>0}$:

1. It holds $\mathrm{Jac}(X)[p^n]_1 \cap \Theta = \{0\}$.
2. The formal power series

$$l_1(X) = \sum_{k=0}^{\infty} \frac{1}{p^k} \begin{pmatrix} \frac{p^k-1}{l} b \\ \frac{p^k-1}{l}(2b-1) \end{pmatrix} X^{p^k}$$

is the logarithm function of a formal group over $\mathbb{Z}_p$, which is isomorphic to $\hat{J}_{X,1}/\mathbb{Z}_p$.

Acknowledgement. Part of this work was done while the authors were visiting National Center for Theoretical Sciences in Hsinchu, Taiwan. We would like to thank Professor Yifan Yang and the institute for their hospitality.

REFERENCES

[1] G. W. Anderson, *Torsion points on Jacobians of quotients of Fermat curves and p-adic soliton theory*, Invent. Math., 118:3 (1994), pp. 475–492.
[2] R. F. Coleman, *Ramified torsion points on curves*, Duke Math. J., 54:2 (1987), pp. 615–640.
[3] R. Gerritzen and M. van der Put, *Schottky Groups and Mumford Curves*, Lecture Notes in Math. 817, Springer-Verlag, 1980.
[4] J. González, *Hasse-Witt matrices for the Fermat curves of prime degree*, Tohoku Math. J. (2), 49:2 (1997), pp. 149–163.
[5] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Volume 35. Springer-Verlag, Berlin, 1996.
[6] D. Grant, *Torsion on theta divisors of hyperelliptic Fermat Jacobians*, Compos. Math., 140:6 (2004), pp. 1432–1438.
[7] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52. Springer-Verlag, 1977.
[8] H. Hasse and E. Witt, *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p*, Monatshefte f. Math. und Phys., 43 (1936), pp. 477–492.
[9] M. Homma, *Automorphisms of prime order of curves*, Manuscripta Math., 33:1 (1980/81), pp. 99–109.
[10] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan, 22 (1970), pp. 213–246.
[11] T. Ichikawa, *p-adic theta functions and solutions of the KP hierarchy*, Commun. Math. Phys., 176 (1996), pp. 383–399.
[12] N. Katz, *Crystalline cohomology, Dieudonné modules, and Jacobi sums, Automorphic forms, representation theory and arithmetic* (Bombay, 1979), pp. 165–246, Tata Inst. Fund. Res. Studies in Math., 10, Tata Inst. Fundamental Res., Bombay, 1981.
[13] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics, 112. Springer-Verlag, 1987.
[14] J. Lewittes, *Automorphisms of compact Riemann surfaces*, Amer. J. Math., 85 (1963), pp. 734–752.
[15] Y. Miyasaka and T. Yamazaki, *Torsion points on hyperelliptic Jacobians via Anderson's p-adic soliton theory*, Tokyo J. Math., 36 (2013), pp. 387–403.
[16] D. Mumford, *An algebro-geometric construction of commuting operators and solutions to the Toda lattice equation, KdV equation and related nonlinear equations*, International Symposium on Algebraic Geometry (Kyoto, 1977) (M. Nagata, ed.), Kinokuniya, Tokyo, 1978, pp. 115–53.
[17] D. Mumford, *An analytic construction of degenerating curves over complete local rings*, Compositio Math., 24 (1972), pp. 129–174.
[18] P. Norman, *p-adic theta functions*, Amer. J. Math., 107:3 (1985). pp. 617–661.
[19] M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, Arithmetic and geometry, Vol. I, pp. 327–352, Progr. Math., 35, Birkhäuser Boston, Boston, MA, 1983.
[20] C. J. Rego, *The compactified Jacobian*, Ann. Sci. École Norm. Sup., 13 (4) (1980), no. 2, pp. 211–223.
[21] M. Sato and Y. Sato, *Soliton equations as dynamical systems on infinite-dimensional Grassmann manifold*, Nonlinear partial differential equations in applied science (Tokyo, 1982), pp. 259–271, North-Holland Math. Stud., 81, North-Holland, Amsterdam, 1983.
[22] G. Segal and G. Wilson, *Loop groups and equations of KdV type*, Inst. Hautes Études Sci. Publ. Math., 61 (1985), pp. 5–65.
[23] K.-O. Stöhr and P. Viana, *A study of Hasse-Witt matrices by local methods*, Math. Z., 200:3 (1989), pp. 397–407.
[24] A. Tamagawa, *Ramification of torsion points on curves with ordinary semistable Jacobian varieties*, Duke Math. J., 106:2 (2001), pp. 281–319.
[25] J. T. Tate, *p-divisible groups*, Proc. Conf. Local Fields (1967), pp. 158–183. Springer, Berlin