Galois Groups and Fundamental Groups
MSRI Publications
Volume **41**, 2003

On the Tame Fundamental Groups of Curves over Algebraically Closed Fields of Characteristic > 0

AKIO TAMAGAWA

Abstract. We prove that the isomorphism class of the tame fundamental group of a smooth, connected curve over an algebraically closed field k of characteristic $p > 0$ determines the genus g and the number n of punctures of the curve, unless $(g, n) = (0, 0), (0, 1)$. Moreover, assuming $g = 0$, $n > 1$, and that k is the algebraic closure of the prime field $\mathbb{F}_p$, we prove that the isomorphism class of the tame fundamental group even completely determines the isomorphism class of the curve as a scheme (though not necessarily as a k-scheme). As a key tool to prove these results, we generalize Raynaud's theory of theta divisors.

Introduction

Let k be an algebraically closed field of characteristic $p > 0$, and U a smooth, connected curve over k. (A curve is a separated scheme of dimension 1.) We denote by X the smooth compactification of U and put $S = X - U$. We define non-negative integers g and n to be the genus of X and the cardinality of the point set S, respectively.

In [T2], we proved that the isomorphism class of the (profinite) fundamental group $\pi_1(U)$ of U determines the pair (g, n), and that, when $g = 0$ and k is the algebraic closure $\overline{\mathbb{F}}_p$ of the prime field $\mathbb{F}_p$, the isomorphism class of $\pi_1(U)$ even completely determines the isomorphism class of the curve as a scheme.

The aim of the present paper is to generalize these results to the case that $\pi_1(U)$ is replaced by its quotient $\pi_1^{\mathrm{t}}(U)$, the tame fundamental group of U (see [SGA1], Exp. XIII and [GM]), as the author announced in [T2], Note 0.3. Thus the main results of the present paper are the following.

Theorem (0.1). (See (4.1).) *The isomorphism class of the profinite group $\pi_1^{\mathrm{t}}(U)$ determines the pair (g, n), unless $(g, n) = (0, 0), (0, 1)$.*

THEOREM (0.2). (See (5.9).) *Assume $g = 0$, $n > 1$, and either $k = \overline{\mathbb{F}}_p$ or $n \leq 4$. Then the isomorphism class of the profinite group $\pi_1^{\mathrm{t}}(U)$ completely determines the isomorphism class of the scheme U.*

More precisely, for two such curves U_i/k $(i = 1, 2)$, $\pi_1^{\mathrm{t}}(U_1) \simeq \pi_1^{\mathrm{t}}(U_2)$ if and only if $U_1 \simeq U_2$ as schemes.

Since it is rather easy to see that the quotient $\pi_1^{\mathrm{t}}(U)$ of $\pi_1(U)$ can be recovered group-theoretically from $\pi_1(U)$ ([T2], Corollary 1.5), the results of the present paper are stronger than those of [T2].

REMARK (0.3). (i) When g and n are small (more precisely, when $2g + n \leq 4$), (0.1) has been settled by Bouw. See [B] for this and other related results.

(ii) In [T1], a result similar to (0.2) was proved for U affine, smooth, geometrically connected curve (of arbitrary genus) over a finite field $\mathbb{F}$. In this case, the (arithmetic) tame fundamental group $\pi_1^{\mathrm{t}}(U)$ is an extension of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ by the geometric tame fundamental group $\pi_1^{\mathrm{t}}(U \otimes_{\mathbb{F}} \overline{\mathbb{F}})$, and we exploited the (outer) Galois action on the geometric tame fundamental group. (0.2) above shows that (for $g = 0$) the geometric tame fundamental group, without the Galois action, is enough to recover the moduli of the curve.

REMARK (0.4). For a profinite group Π, let Π_A denote the set of isomorphism classes of all finite quotients of Π. It is known that the subset Π_A of the set of isomorphism classes of all finite groups completely determines the isomorphism class of the profinite group Π, if Π is finitely generated ([FJ], Proposition 15.4).

We shall write $\pi_A^{\mathrm{t}}(U)$ instead of $\pi_1^{\mathrm{t}}(U)_A$. Then, since $\pi_1^{\mathrm{t}}(U)$ is finitely generated, the information carried by $\pi_A^{\mathrm{t}}(U)$ is equivalent to the information carried by (the isomorphism class of) $\pi_1^{\mathrm{t}}(U)$. Therefore, we can restate the above theorems in terms of $\pi_A^{\mathrm{t}}(U)$. Moreover, as for (0.1), we can say how $\pi_A^{\mathrm{t}}(U)$ determines the pair (g, n) explicitly, by looking carefully at the proofs in the present paper. For this, see [T3].

In [T2], the result corresponding to (0.1) followed from a quick argument combining the Hurwitz formula and the Deuring–Shafarevich formula, which involves wild ramification. However, in our case, we cannot resort to wild ramification, and we need another strategy.

In order to explain our strategy to prove (0.1), first we shall assume $n = 0$, or, equivalently, $U = X$. (Under this assumption, it is elementary to prove (0.1), though. See (4.3)(i).) Note that then we have $\pi_1^{\mathrm{t}}(U) = \pi_1(X)$. In this case, all the ingredients of our strategy are given by Raynaud's theory of theta divisors ([R1]).

(i) The p-rank (or Hasse–Witt invariant) γ_X of X is defined to be the dimension of the $\mathbb{F}_p$-vector space $\mathrm{Hom}(\pi_1(X), \mathbb{F}_p)$. More generally, for each surjective homomorphism $\rho : \pi_1(X) \twoheadrightarrow G$, where G is a finite cyclic group of order N prime to p, $\mathrm{Ker}(\rho)$ may be identified with $\pi_1(Y)$, where $Y \to X$ is the finite étale G-covering corresponding to ρ. Then, G acts on $\mathrm{Hom}(\pi_1(Y), \mathbb{F}_p)$, and

$\mathrm{Hom}(\pi_1(Y), \mathbb{F}_p) \otimes k$ admits a canonical decomposition as a direct sum, corresponding to the decomposition of the group algebra $k[G]$ as the direct product of N copies of k, each of which corresponds to a character $G \to k^\times$. Now, the dimension of each direct summand of $\mathrm{Hom}(\pi_1(Y), \mathbb{F}_p) \otimes k$ is the so-called generalized Hasse–Witt invariant (see [Ka], [Na], and [B]).

(ii) On the other hand, it is well-known that the set of connected finite étale G-coverings of X is in one-to-one correspondence with the set of isomorphism classes of line bundles on X of order N, or, equivalently, the set of points of order N of the Jacobian variety J of X. More precisely, this one-to-one correspondence is given by fixing an isomorphism $G \xrightarrow{\sim} \boldsymbol{\mu}_N(k)$. For each line bundle L of order N, let f be the order of p mod N in $(\mathbb{Z}/N\mathbb{Z})^\times$. Then, taking the composite of the p^f-th power map $L \to L^{\otimes p^f}$ and the isomorphism $L^{\otimes p^f} = L \otimes L^{\otimes (p^f - 1)} \xrightarrow{\sim} L$, we get a map $L \to L$, which induces a p^f-linear map $\varphi_{[L]} : H^1(X, L) \to H^1(X, L)$. Now, the generalized Hasse–Witt invariant $\gamma_{[L]}$ with respect to L and $G \xrightarrow{\sim} \boldsymbol{\mu}_N(k) \subset k^\times$ coincides with the dimension of the k-vector space $\bigcap_{r \geq 1} \mathrm{Im}((\varphi_L)^r)$.

(iii) Raynaud ([R1]) defined a certain divisor Θ_B of J (more naturally, of the Frobenius twist J_1 of J) in a canonical way depending only on X, such that $[L] \in J$ belongs to Θ_B if and only if the p-linear map $H^1(X, L) \to H^1(X, L^{\otimes p})$ induced by the p-th power map $L \to L^{\otimes p}$ is an isomorphism. In particular, if $[L]$ is a torsion element of order N prime to p as above, $\varphi_{[L]}$ is an isomorphism (or, equivalently, $\gamma_{[L]} = \dim_k(H^1(X, L))$), if and only if $[L^{\otimes p^i}] \notin \Theta_B$ for all $i = 0, 1, \ldots, f - 1$.

(iv) More precisely, Raynaud defined a vector bundle B with rank $p - 1$, degree $(p - 1)(g - 1)$, and Euler–Poincaré characteristic 0 to be the cokernel of (the linearization of) the p-th power map $\mathcal{O}_X \to \mathcal{O}_X$. Then, he defined Θ_B as the theta divisor of B. (That is to say, $[L] \notin \Theta_B$ if and only if $H^0(X, B \otimes L) = H^1(X, B \otimes L) = 0$.) It is easy to see that Θ_B is a closed subscheme of codimension ≤ 1 of J, and the main difficulty consists in proving that Θ_B does not coincide with J. To prove this, Raynaud resorted to a ring-theoretic argument involving the Koszul complex over the (regular) local ring at the origin of J.

(v) By using intersection theory, Raynaud proved $\#(\Theta_B \cap J[N]) = O(N^{2g-2})$. From this, we obtain $\#\{[L] \in J[N] \mid \exists i, \text{ s.t. } [L^{\otimes i}] \in \Theta_B\} = O(N^{2g-1})$. So, as a conclusion, we can roughly say that, for 'most' prime-to-p-cyclic (finite étale) coverings of X, the generalized Hasse–Witt invariants are as large as possible. In other words, $\gamma_{[L]} = g - 1$ holds for 'most' L (unless $g = 0$). Since the generalized Hasse–Witt invariants are encoded in $\pi_1(X)$ by definition, this gives a group-theoretic characterization of the invariant $g - 1$.

For Raynaud's theory of theta divisors, see also [R2] (a generalization) and [Mad] (an exposition).

In this paper, we generalize these arguments to the (possibly) ramified case $n > 0$. Here, a cyclic (finite étale) covering of U of degree N prime to p corre-

sponds to a pair of a line bundle L and an effective divisor D (whose support is contained in S) satisfying certain conditions. (In particular, $L^{\otimes N} \simeq \mathcal{O}_X(-D)$ is required.) Then, as in (ii) above, we can describe the corresponding generalized Hasse–Witt invariant $\gamma_{([L],D)}$ in terms of a p^f-linear map $\varphi_{([L],D)} : H^1(X, L) \to H^1(X, L)$. Note that, unlike in the case $n = 0$ (and $L \not\simeq \mathcal{O}_X$), the dimension of $H^1(X, L)$ depends on L, since $\deg(L)$ varies (among $0, -1, \ldots, -(n-1)$). Then, under certain assumptions on D, we can define a vector bundle B_D^f depending on f and D, which yields a closed subscheme of J (more naturally, of the f-th Frobenius twist J_f of J). Now, the main result (2.5) says that this closed subscheme is a divisor if $\deg(D) = p^f - 1$. As a corollary, we have that, if $N = p^f - 1$, for 'most' pairs $([L], D)$ with $\deg(L) = -1$, the generalized Hasse–Witt invariant $\gamma_{([L],D)}$ is as large as possible, i.e., coincides with $\dim_k(H^1(X, L)) = g$ (if $n > 1$). On the other hand, by a combinatorial argument, we prove that, if $n > 1$ and $N = p^f - 1$, for 'most' pairs $([L], D)$, there exists an $i = 0, 1, \ldots, f-1$ such that $\deg(L_{p^i}) = -1$. (Here, L_j is a certain modification of $L^{\otimes j}$, so that the cyclic (ramified) covering of X corresponding to $([L], D)$ is the spectrum of $\bigoplus_{j=0}^{N-1} L_j$.) Combining these, we can conclude that for 'most' prime-to-p-cyclic coverings of U (with degree in the form $p^f - 1$), the generalized Hasse–Witt invariants coincide with g. This gives a group-theoretic characterization of g. Since it is easy to see that the Euler–Poincaré characteristic $2 - 2g - n$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$, this completes the proof of (0.1).

Just as in [T2], we can then prove that (for U hyperbolic) the set of inertia subgroups of $\pi_1^{\mathrm{t}}(U)$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$, by using (0.1) (see (5.2)). Now, what is missing to prove (0.2) along the lines of [T2] is only to recover the 'additive structures' of the inertia subgroups (see Section 5, (B)). In [T2], this was done by studying wild ramification again. In our case, another usage of our generalization of Raynaud's theory settles the problem. This completes the proof of (0.2).

We shall explain briefly the content of each section of the present paper, and show in which section each part of the above arguments is contained. The order of the sections does not necessarily follow the order of the above arguments, because it is natural to present the main theorems (which assure the existence of the theta divisor associated with B_D^f) as early as possible, and then to present the main results concerning $\pi_1(X)$ as corollaries of the main theorems.

In Section 1, we give a generalization of Raynaud's ring-theoretic argument in (iv) above. The main result is (1.12). In fact, Raynaud's original argument is sufficient for the proofs of the main results of the present paper. However, we include this generalization since it is done by just replacing the Koszul complex in Raynaud's proof with the so-called Eagon–Northcott complex, and since it is likely that this generalization will be applied to other related problems concerning coverings and fundamental groups.

In Section 2, after quickly reviewing Raynaud's theory concerning the theta divisor Θ_B, we define the vector bundle B_D^f, and prove (by using (1.12)) the main result (2.5) which assures the existence of the theta divisor associated with B_D^f under certain assumptions. (2.5), together with a slight generalization (2.6), plays a crucial role in the group-theoretic characterization of the genus. Moreover, with another variant (2.13), we investigate the case $n \leq 3$ in more detail (2.21). This plays a central role in the group-theoretic characterization of the additive structures of inertia groups.

In Section 3, we give a review of generalized Hasse–Witt invariants, a description (3.5) of prime-to-p-cyclic coverings of X that are unramified on U in terms of line bundles and divisors on X, and a reinterpretation of generalized Hasse–Witt invariants via this description. Then, after presenting some inputs from intersection theory (3.10), we prove the main numerical results (3.12) and (3.16) concerning the generalized Hasse–Witt invariants of prime-to-p-cyclic coverings of U, by using the results of Section 2. Note that so far the effective divisor D is fixed. Now, combining these results with a combinatorial result (3.18) (which enables D to vary), we finally establish the summarizing result (3.20) to the effect that most generalized Hasse–Witt invariants coincides with g', where $g' \stackrel{\text{def}}{=} g$ (resp. $g' \stackrel{\text{def}}{=} g - 1$) for $n > 1$ (resp. $n \leq 1$).

In Section 4, we apply the results of Section 3 and give a group-theoretic characterization of g' in an effective way (4.10) and in an ineffective but impressive way (4.11). The latter can be stated as follows. Here, for each profinite group Π and a natural number m, we denote by $\Pi(m)$ the kernel of $\Pi \twoheadrightarrow \Pi^{\mathrm{ab}} \otimes \mathbb{Z}/m\mathbb{Z}$.

Theorem (0.5). (See (4.8), (4.11), and (4.12).) *We have*

$$\lim_{f \to \infty} \gamma^{\mathrm{av}}_{p^f - 1} = g',$$

unless $(g, n) = (0, 0), (0, 1)$, *where*

$$\gamma^{\mathrm{av}}_N = \frac{\dim_{\mathbb{F}_p}(\pi_1^{\mathrm{t}}(U)(N)^{\mathrm{ab}} \otimes \mathbb{F}_p)}{\#(\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}} \otimes \mathbb{Z}/N\mathbb{Z})}.$$

Moreover, after settling a few more minor technical problems (for example, the problem that the results above do not give a characterization of g but only give a characterization of g'), we obtain the group-theoretic characterization (4.1) of the pair (g, n).

Finally, in Section 5, we give group-theoretic characterizations of the inertia subgroups (5.2) and the 'additive structures' of inertia subgroups (5.3), and present anabelian-geometric results (5.8) and (5.9) for $g = 0$.

In the Appendix, we give a proof of a partial generalization (4.17) of the limit formula (4.11). Here, the theory of uniform distribution (especially, Stegbuchner's higher-dimensional version of LeVeque's inequality) plays a key role.

Acknowledgement. When the author presented the results of [T2] in Kyoto (May, 1996) and in Oberwolfach (June, 1997), Shinichi Mochizuki and Michel Raynaud, respectively, asked the author about the possibility of generalizing the results of [T2] to the case that the fundamental group is replaced by the tame fundamental group. Although the author had already taken an interest in such possibility, their questions stimulated and encouraged the author very much. The author would like to thank them very much. Also, when the author was trying to prove a more general limit formula (4.16) of the genus, Makoto Nagata suggested the possibility of applying the theory of uniform distribution, which is essential in the Appendix of the present paper. The author would like to thank him very much.

1. A Generalization of the Ring-Theoretic Part of Raynaud's Theory

In this section, we shall give a generalization of the ring-theoretic part of Raynaud's theory ([R1], 4.2). The statement of our main result is more general than [R1], Lemme 4.2.3, but the proof is rather similar to Raynaud's proof, if we replace the Koszul complex by the so-called Eagon–Northcott complex.

Now, let Y be a connected, noetherian scheme and $f : X \to Y$ a proper morphism whose fibers are of dimension ≤ 1. Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module flat over Y. For each $y \in Y$ and $i = 0, 1$, define $h^i(y) = h^i(\mathcal{F}, y)$ to be the dimension of the $\boldsymbol{k}(y)$-vector space $H^i(X_y, \mathcal{F} \otimes \boldsymbol{k}(y))$, where X_y denotes the scheme-theoretic fiber $X \otimes \boldsymbol{k}(y)$ of f at y and $\mathcal{F} \otimes \boldsymbol{k}(y)$ denotes the $\mathcal{O}_{X_y}$- module obtained as the pull-back of $\mathcal{F}$ to X_y. By the local constancy of the Euler–Poincaré characteristic ([Mu], § 5, Corollary on p.50),

$$\chi_{\mathcal{F}} \stackrel{\text{def}}{=} h^0(y) - h^1(y)$$

is independent of y.

Definition. (i) For each $i \in \mathbb{Z}_{\geq 0}$, we denote by $Z_i = Z_i(\mathcal{F})$ the closed subscheme of Y defined by the i-th Fitting ideal $\mathrm{Fitt}_i(R^1 f_*(\mathcal{F}))$ of $\mathcal{O}_Y$.
(ii) We put $W(\mathcal{F}) \stackrel{\text{def}}{=} Z_{(-\chi_{\mathcal{F}})^+}(\mathcal{F})$, where $x^+ \stackrel{\text{def}}{=} \max(x, 0)$.

Remark (1.1). For the definition and the properties of Fitting ideals, we refer to [E], Chapter 20, where only Fitting ideals of modules over rings are treated. However, since the formation of Fitting ideals commutes with localization ([E], Corollary 20.5), we can define and treat Fitting ideals of coherent sheaves on schemes without any extra efforts. (See [SGA7I], Exp. VI, § 5.)

Lemma (1.2). *For each $y \in Y$, we have*

$$y \notin Z_i(\mathcal{F}) \iff h^1(y) \leq i.$$

In particular,

$$y \notin W(\mathcal{F}) \iff \min(h^0(y), h^1(y)) = 0.$$

PROOF. The first assertion follows from [E], Proposition 20.6 and [Mu], § 5, Corollary 3 on p. 53. The second assertion follows from the first, together with the identity

$$h^1(y) - (-\chi_{\mathcal{F}})^+ = \min(h^0(y), h^1(y)). \tag{1.3}$$ □

In the special case that $h^0(y) = 1$, we have:

LEMMA (1.4). *Let y be a point of Y, and assume that $h^0(y) = 1$ and that $h^1(y) \geq 1$. Then, in a certain open neighborhood of y, $W(\mathcal{F})$ is the maximal closed subscheme W on which $R^1 f_*(\mathcal{F})|_W$ is locally free of rank $h^1(y)$.*

PROOF. By the assumption, we have $(-\chi_{\mathcal{F}})^+ = h^1(y) - 1$, hence $W(\mathcal{F}) = Z_{h^1(y)-1}(\mathcal{F})$. Put $U = Y - Z_{h^1(y)}(\mathcal{F})$, which is an open neighborhood of y by (1.2). Then, by [E], Proposition 20.8, $W(\mathcal{F}) \cap U$ is the maximal closed subscheme W_U of U on which $R^1 f_*(\mathcal{F})|_{W_U}$ is locally free of rank $h^1(y)$, as desired. □

Next, we shall describe $W(\mathcal{F})$ by using the theory of perfect complexes.

DEFINITION. For a homomorphism $\phi : A \to B$ in an abelian category, we denote by $(A \overset{\phi}{\to} B)$ or simply by $(A \to B)$ the complex

$$\cdots \to 0 \to 0 \to A \overset{\phi}{\to} B \to 0 \to 0 \to \cdots,$$

where A (resp. B) is placed in degree 0 (resp. 1).

LEMMA (1.5). *Let y be a point of Y. Then, in some open neighborhood of y, the object $Rf_*(\mathcal{F})$ (in the derived category of $\mathcal{O}_Y$-modules) can be represented by a complex in the form $(\mathcal{O}_Y^{h^0(y)} \overset{\phi}{\to} \mathcal{O}_Y^{h^1(y)})$ with $\phi \otimes \boldsymbol{k}(y) = 0$.*

Moreover, for each homomorphism $\mathcal{F} \to \mathcal{F}'$ between coherent $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{F}'$ flat over Y, the corresponding morphism $Rf_*(\mathcal{F}) \to Rf_*(\mathcal{F}')$ can be represented by a homomorphism of complexes in the form

$$(\mathcal{O}_Y^{h^0(\mathcal{F},y)} \overset{\phi}{\to} \mathcal{O}_Y^{h^1(\mathcal{F},y)}) \to (\mathcal{O}_Y^{h^0(\mathcal{F}',y)} \overset{\phi'}{\to} \mathcal{O}_Y^{h^1(\mathcal{F}',y)}),$$

that is:

$$\begin{array}{ccc}
\vdots & & \vdots \\
\downarrow & & \downarrow \\
\mathcal{O}_Y^{h^0(\mathcal{F},y)} & \to & \mathcal{O}_Y^{h^0(\mathcal{F}',y)} \\
\phi \downarrow & & \phi' \downarrow \\
\mathcal{O}_Y^{h^1(\mathcal{F},y)} & \to & \mathcal{O}_Y^{h^1(\mathcal{F}',y)} \\
\downarrow & & \downarrow \\
\vdots & & \vdots
\end{array} .$$

PROOF. Zariski locally on Y, $Rf_*(\mathcal{F})$ can be represented by a perfect complex in the form $((\mathcal{O}_Y)^{n_0} \to (\mathcal{O}_Y)^{n_1})$. (See [Mu], § 5, the second Theorem on p.46.

We can take a complex in this form since $h^i(y) = 0$ for $y \in Y$ and $i > 1$. See also [SGA6], Exp. I–III.) In particular, we have the exact sequence

$$0 \to R^0 f_*(\mathcal{F}) \to (\mathcal{O}_Y)^{n_0} \to (\mathcal{O}_Y)^{n_1} \to R^1 f_*(\mathcal{F}) \to 0. \tag{1.6}$$

On the other hand, consider a minimal free resolution of the $\mathcal{O}_{Y,y}$-module $R^1 f_*(\mathcal{F})_y$:

$$\cdots \to (\mathcal{O}_{Y,y})^{m_0} \to (\mathcal{O}_{Y,y})^{m_1} \to R^1 f_*(\mathcal{F})_y \to 0.$$

By [E], Theorem 20.2, we can see that the exact sequence

$$(\mathcal{O}_{Y,y})^{n_0} \to (\mathcal{O}_{Y,y})^{n_1} \to R^1 f_*(\mathcal{F})_y \to 0$$

obtained by localizing (1.6) is isomorphic to the direct sum of (part of) the minimal resolution

$$(\mathcal{O}_{Y,y})^{m_0} \to (\mathcal{O}_{Y,y})^{m_1} \to R^1 f_*(\mathcal{F})_y \to 0 \tag{1.7}$$

and the complex $((\mathcal{O}_{Y,y})^{a+b} \stackrel{\text{proj.}}{\to} (\mathcal{O}_{Y,y})^a)$ for some $a, b \geq 0$. Now, taking the direct sum of (1.7) and the complex $((\mathcal{O}_{Y,y})^b \to 0)$, we obtain a new complex $((\mathcal{O}_{Y,y})^{m_0'} \to (\mathcal{O}_{Y,y})^{m_1})$, where $m_0' = m_0 + b$, which is homotopically equivalent to $((\mathcal{O}_{Y,y})^{n_0} \to (\mathcal{O}_{Y,y})^{n_1})$, by definition. Since we are dealing with only finite number of modules and homomorphisms, we can extend this homotopy equivalence to one between $((\mathcal{O}_Y)^{n_0} \to (\mathcal{O}_Y)^{n_1})$ and $((\mathcal{O}_Y)^{m_0'} \to (\mathcal{O}_Y)^{m_1})$, if we replace Y by a suitable open neighborhood of y.

By the definition of the minimality, the homomorphism $(\mathcal{O}_{Y,y})^{m_1} \to R^1 f_*(\mathcal{F})_y$ becomes an isomorphism after being tensored with $\boldsymbol{k}(y)$. Then, by [Mu], § 5, Corollary 3 on p.53, we obtain $m_1 = h^1(y)$. Thus $Rf_*(\mathcal{F})$ is represented by the complex $((\mathcal{O}_Y)^{m_0'} \to (\mathcal{O}_Y)^{h^1(y)})$. Finally, by tensoring this complex with $\boldsymbol{k}(y)$ again, we obtain $m_0' = h^0(y)$ and $\phi \otimes \boldsymbol{k}(y) = 0$, as desired.

The second assertion follows from the first assertion and a standard fact in the theory of derived categories (see, e.g., [E], Exercise A3.54). □

Corollary (1.8). *In some neighborhood of y, $W(\mathcal{F})$ is defined by the ideal generated by the maximal minors of an $h^0(y) \times h^1(y)$ matrix representing ϕ in* (1.5).

Proof. This follows from the definition of Fitting ideal, together with identity (1.3). □

Theorem (Macaulay [Mac]). (See [E], Exercise 10.9.) *Let R be a noetherian ring, and let F and G be free R-modules of finite rank. Let ϕ be an R-homomorphism $F \to G$, and choose a matrix A with coefficients in R that represents ϕ. Let I be the ideal of R generated by the maximal minors of A. Then, for each minimal prime ideal $\mathfrak{p}$ containing I, we have* $\mathrm{ht}(\mathfrak{p}) \leq |\mathrm{rk}(F) - \mathrm{rk}(G)| + 1$. □

DEFINITION. In Macaulay's theorem, if, moreover, the equality $\mathrm{ht}(\mathfrak{p}) = |\mathrm{rk}(F) - \mathrm{rk}(G)| + 1$ holds for every minimal prime ideal $\mathfrak{p}$ containing I, we say that ϕ is determinantal. (See, e.g., [E], 18.5.) Equivalently, ϕ is determinantal if and only if either $I = R$ or $\mathrm{ht}(I) = |\mathrm{rk}(F) - \mathrm{rk}(G)| + 1$.

COROLLARY (1.9). *The codimension of each irreducible component of $W(\mathcal{F})$ does not exceed $|\chi_{\mathcal{F}}| + 1$.*

PROOF. This follows from (1.8) and Macaulay's theorem above. □

DEFINITION. We say $\mathcal{F}$ is determinantal, if the codimension of every irreducible component of $W(\mathcal{F})$ coincides with $|\chi_{\mathcal{F}}| + 1$. (Equivalently, $\mathcal{F}$ is determinantal if and only if either $W(\mathcal{F}) = \varnothing$ or $\mathrm{codim}(W(\mathcal{F})) = |\chi_{\mathcal{F}}| + 1$.)

Before presenting the main result of this section, we shall establish the following key lemma, which is purely in commutative ring theory. In the special case that R is regular, $\mathrm{rk}(F) = \mathrm{rk}(F') = \dim(R)$ and $\mathrm{rk}(G) = \mathrm{rk}(G') = 1$, this can be seen in [R1], Lemme 4.2.3.

LEMMA (1.10). *Let R be a Cohen–Macaulay local ring. Let*

$$\begin{array}{ccc} F & \xrightarrow{f} & F' \\ \phi\downarrow & & \phi'\downarrow \\ G & \xrightarrow{g} & G' \end{array} \tag{1.11}$$

be a commutative diagram of R-modules, where F, G, F', G' are free R-modules of finite rank. Assume that:

(a) $\mathrm{rk}(F) - \mathrm{rk}(G) \geq 0$ *and ϕ is determinantal*;
(b) *g is surjective*;
(c) *either* $\mathrm{rk}(F) - \mathrm{rk}(G) = 0$ *or ϕ' is not surjective*; *and*
(d) $\mathrm{rk}(F) - \mathrm{rk}(G) \geq \mathrm{rk}(F') - \mathrm{rk}(G')$.

Then:

(i) $\mathrm{rk}(F) - \mathrm{rk}(G) = \mathrm{rk}(F') - \mathrm{rk}(G')$.
(ii) *ϕ' is determinantal.*
(iii) *The fiber product $F_1 \overset{\mathrm{def}}{=} G \times_{G'} F'$ is a free R-module of rank* $\mathrm{rk}(F)$, *and the determinant of the natural homomorphism $F \to F_1$ is not zero.*

PROOF. By replacing R with its completion, we may assume that R is complete. In particular, we may assume that R admits a canonical module ω (see [BH], Corollary 3.3.8).

From now on, we write χ and χ' instead of $\mathrm{rk}(F) - \mathrm{rk}(G)$ and $\mathrm{rk}(F') - \mathrm{rk}(G')$, respectively. Moreover, we denote by I and I' the ideals of R generated by the maximal minors of ϕ and ϕ', respectively.

First, we treat the easier case that ϕ' is surjective. Then we must have $\chi' \geq 0$. On the other hand, by (c) and (d), we have $\chi' \leq \chi = 0$. Thus $\chi' = \chi = 0$, which implies (i). Since ϕ' is surjective with $\chi' = 0$, ϕ' must be an isomorphism. In

particular, we have $I' = R$, hence (ii) holds. Next, the natural map $F_1 \to G$ is an isomorphism, so we have $\mathrm{rk}(F_1) = \mathrm{rk}(G) = \mathrm{rk}(F)$. Moreover, the natural map $F \to F_1$ can be identified with ϕ. Now, since ϕ is determinantal, the determinant of ϕ is non-zero. This complete the proof in the case that ϕ' is surjective.

Next, assume that ϕ' is not surjective. Put $M \stackrel{\text{def}}{=} \mathrm{Coker}(\phi)$ and $M' \stackrel{\text{def}}{=} \mathrm{Coker}(\phi')$. Since $\chi \geq 0$ by the first half of (a), we have $I = \mathrm{Fitt}_0(M)$ by definition, and I annihilates M by [E], Proposition 20.7a. By (b), the natural map $M \to M'$ is also surjective, hence I annihilates M'. In particular, $I \neq R$ as $M' \neq 0$, so, by (a), we have $\mathrm{ht}(I) = \chi + 1 \geq 1$. Now, since M' is annihilated by I with $\mathrm{ht}(I) \geq 1$, we obtain $\chi' \geq 0$. (To see this, for example, tensor the (right) exact sequence $F' \to G' \to M' \to 0$ with the residue field at any minimal prime ideal of R.) Thus we have $I' = \mathrm{Fitt}_0(M')$.

Note that g is surjective by (b) and G' is free. Accordingly, g is split surjective, or, equivalently, if we put $K \stackrel{\text{def}}{=} \mathrm{Ker}(g)$, g is a composite of an isomorphism $G \stackrel{\sim}{\to} K \times G'$ that restricts to the identity on K and the projection $K \times G' \to G'$. From this, we can easily see that the fiber product $F_1 = G \times_{G'} F'$ is free and fits naturally into the following commutative diagram whose columns are all exact:

$$\begin{array}{ccccc} F & \stackrel{f_1}{\to} & F_1 & \twoheadrightarrow & F' \\ \phi\downarrow & & \phi_1\downarrow & & \phi'\downarrow \\ G & = & G & \twoheadrightarrow & G' \\ \downarrow & & \downarrow & & \downarrow \\ M & \twoheadrightarrow & M' & = & M' \\ \downarrow & & \downarrow & & \downarrow \\ 0 & & 0 & & 0. \end{array}$$

Moreover, we have $\mathrm{rk}(F_1) - \mathrm{rk}(G) = \chi' \geq 0$. Thus, calculating $\mathrm{Fitt}_0(M')$ by using ϕ_1, we see $\mathrm{Fitt}_0(M) \subset \mathrm{Fitt}_0(M')$, or, equivalently, $I \subset I'$. Moreover, since I' annihilates $M' \neq 0$ by [E], Proposition 20.7a, we have $I' \neq R$. Thus, we have

$$\chi + 1 = \mathrm{ht}(I) \leq \mathrm{ht}(I') \leq \chi' + 1,$$

where the last inequality follows from Macaulay's theorem. Combining this with (d), we obtain $\mathrm{ht}(I') = \chi' + 1$ and $\chi' = \chi$. The former implies (ii), and the latter implies both (i) and the first half of (iii). Note that ϕ_1 is also determinantal.

To see the second half of (iii), we shall compare the Eagon–Northcott complexes associated with ϕ and ϕ_1. (For Eagon–Northcott complexes, see [E], A2.6.) So, consider the following commutative diagram whose first (resp. second) row is the Eagon–Northcott complex canonically associated with ϕ (resp. ϕ_1):

$$\begin{array}{ccccccccccc} 0 & \to & D_\chi \otimes \bigwedge^r F & \to \cdots \to & D_0 \otimes \bigwedge^s F = \bigwedge^s F & \stackrel{\bigwedge^s \phi}{\to} & \bigwedge^s & \to & \bigwedge^s \otimes R/I & \to & 0 \\ & & \downarrow & & \downarrow & & \| & & \downarrow & & \\ 0 & \to & D_\chi \otimes \bigwedge^r F_1 & \to \cdots \to & D_0 \otimes \bigwedge^s F_1 = \bigwedge^s F_1 & \stackrel{\bigwedge^s \phi_1}{\to} & \bigwedge^s & \to & \bigwedge^s \otimes R/I' & \to & 0, \end{array}$$

where $r = \mathrm{rk}(F) = \mathrm{rk}(F_1)$, $s = \mathrm{rk}(G)$, $D_i = (S_iG)^*$, and $\bigwedge^s = \bigwedge^s G$ ($\simeq R$). Since ϕ and ϕ_1 are determinantal, the two rows are exact and both $\bigwedge^s \otimes R/I$ and $\bigwedge^s \otimes R/I'$ are Cohen–Macaulay R-modules, by [E], Corollary A2.13.

Now, suppose that the determinant map $\bigwedge^r F \to \bigwedge^r F_1$ is zero. Then, the first vertical arrow $D_\chi \otimes \bigwedge^r F \to D_\chi \otimes \bigwedge^r F_1$ is also zero. So, calculating $\mathrm{Ext}_R^{\chi+1}(-,\omega)$ by using the Eagon–Northcott complexes, we see that the map $\mathrm{Ext}_R^{\chi+1}(\bigwedge^s \otimes R/I', \omega) \to \mathrm{Ext}_R^{\chi+1}(\bigwedge^s \otimes R/I, \omega)$ associated with the natural surjection $\bigwedge^s \otimes R/I \to \bigwedge^s \otimes R/I'$ must be also zero. However, since $\mathrm{ht}(I') = \mathrm{ht}(I) = \chi + 1$, the duality theory (see [BH], Theorem 3.3.10, (a)⇒(c)) tells us that this implies that the original surjection $\bigwedge^s \otimes R/I \to \bigwedge^s \otimes R/I'$ is zero. This is absurd, since $\bigwedge^s \simeq R$ and $I' \neq R$. This completes the proof. □

The following is the main result of this section.

THEOREM (1.12). *Let Y be a Cohen–Macaulay, noetherian, integral scheme. Let $f : X \to Y$ be a proper morphism whose fibers are of dimension ≤ 1. Let $\mathcal{F}_i$ $(i = 1, 2, 3)$ be coherent $\mathcal{O}_X$-modules flat over Y, and $0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ an exact sequence of $\mathcal{O}_X$-modules. Assume that*:

(a) *$\mathcal{F}_2$ is determinantal (in the sense of the Definition following* (1.9));
(b) *one of the following three conditions holds*: $\chi_{\mathcal{F}_2} < 0, W(\mathcal{F}_1) \neq \varnothing$; $\chi_{\mathcal{F}_2} = 0$; $\chi_{\mathcal{F}_2} > 0, W(\mathcal{F}_3) \neq \varnothing$; *and*
(c) $\chi_{\mathcal{F}_1} \cdot \chi_{\mathcal{F}_3} \geq 0$.

Then:

(i) $\chi_{\mathcal{F}_1} \cdot \chi_{\mathcal{F}_3} = 0$.
(ii) *$\mathcal{F}_1$ and $\mathcal{F}_3$ are determinantal.*

PROOF. First, we shall treat the case that $\chi_{\mathcal{F}_2} \geq 0$. By (1.5), in some neighborhood of each $y \in Y$, the objects $Rf_*(\mathcal{F}_2)$, $Rf_*(\mathcal{F}_3)$, and the morphism $Rf_*(\mathcal{F}_2) \to Rf_*(\mathcal{F}_3)$ can be represented by complexes $(\mathcal{O}_Y^{h^0(\mathcal{F}_2,y)} \to \mathcal{O}_Y^{h^1(\mathcal{F}_2,y)})$, $(\mathcal{O}_Y^{h^0(\mathcal{F}_3,y)} \to \mathcal{O}_Y^{h^1(\mathcal{F}_3,y)})$, and a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_Y^{h^0(\mathcal{F}_2,y)} & \to & \mathcal{O}_Y^{h^0(\mathcal{F}_3,y)} \\ \downarrow & & \downarrow \\ \mathcal{O}_Y^{h^1(\mathcal{F}_2,y)} & \to & \mathcal{O}_Y^{h^1(\mathcal{F}_3,y)} \end{array} , \tag{1.13}$$

respectively. Put $R = \mathcal{O}_{Y,y}$ and $k = \boldsymbol{k}(y)$. Localizing (1.13) at y, we obtain a commutative diagram (1.11) of free R-modules of finite rank, where $\mathrm{rk}(F) = h^0(\mathcal{F}_2, y)$, $\mathrm{rk}(G) = h^1(\mathcal{F}_2, y)$, $\mathrm{rk}(F') = h^0(\mathcal{F}_3, y)$, and $\mathrm{rk}(G') = h^1(\mathcal{F}_3, y)$. In particular, we have $\mathrm{rk}(F) - \mathrm{rk}(G) = \chi_{\mathcal{F}_2} \geq 0$ and $\mathrm{rk}(F') - \mathrm{rk}(G') = \chi_{\mathcal{F}_3}$. We shall check conditions (a)–(d) of (1.10) by using our assumptions (a)–(c). (For conditions (c) and (d) of (1.10), we need an extra assumption on y. See below.)

Condition (a) of (1.10) follows directly from our assumption that $\chi_{\mathcal{F}_2} \geq 0$ and our assumption (a). Next, since the fiber X_y is of dimension ≤ 1, we see that the map $g \otimes k : G \otimes k = H^1(X_y, \mathcal{F}_2 \otimes \boldsymbol{k}(y)) \to H^1(X_y, \mathcal{F}_3 \otimes \boldsymbol{k}(y)) = G' \otimes k$

is surjective, hence g is surjective by Nakayama's lemma. Thus condition (b) of (1.10) holds.

If $\chi_{\mathcal{F}_2} = 0$, condition (c) of (1.10) clearly holds. Moreover, in this case, our assumption (c) says $-(\chi_{\mathcal{F}_3})^2 \geq 0$, or, equivalently, $\chi_{\mathcal{F}_3} = 0$. Thus condition (d) of (1.10) holds.

If $\chi_{\mathcal{F}_2} > 0$, we shall put an extra assumption that $y \in W(\mathcal{F}_3)$. Then, by (1.2), we have $h^1(\mathcal{F}_3, y) > 0$. Since $\phi' \otimes k = 0$, this implies that $\phi' \otimes k$ is not surjective, hence ϕ' is not surjective. Thus condition (c) of (1.10) holds. Moreover, suppose that condition (d) of (1.10) does not hold. Then, we have $\chi_{\mathcal{F}_3} > \chi_{\mathcal{F}_2} \geq 0$, and $\chi_{\mathcal{F}_1} = \chi_{\mathcal{F}_2} - \chi_{\mathcal{F}_3} < 0$. Thus $\chi_{\mathcal{F}_1} \cdot \chi_{\mathcal{F}_3} < 0$, which contradicts our assumption (c).

Now, we may apply (1.10). Conclusion (i) of (1.10) implies $\chi_{\mathcal{F}_1} = 0$, hence (i) of (1.12) (and $\chi_{\mathcal{F}_3} \geq 0$). Conclusion (ii) of (1.10) implies that each irreducible component of $W(\mathcal{F}_3)$ passing through y has codimension $|\chi_{\mathcal{F}_3}| + 1 = \chi_{\mathcal{F}_3} + 1$. So, (considering all points $y \in W(\mathcal{F}_3)$) we obtain that $\mathcal{F}_3$ is determinantal. Moreover, conclusion (iii) of (1.10) implies that the map $F \to G \times_{G'} F'$ is injective, since R is an integral domain by the assumption that Y is integral. Accordingly, the map

$$R^0 f_*(\mathcal{F}_2)_y = \mathrm{Ker}(\phi) \to \mathrm{Ker}(\phi') = R^0 f_*(\mathcal{F}_3)_y$$

is injective, or, equivalently, $R^0 f_*(\mathcal{F}_1)_y = 0$. Thus, in particular, we obtain $h^0(\mathcal{F}_1, \eta) = 0$, where η is the generic point of the integral scheme Y. (Here, we have used our assumption (b) for the first time to choose a point y.) Thus, $\eta \notin W(\mathcal{F}_1)$. Since Y is integral and $|\chi_{\mathcal{F}_1}| + 1 = 1$, this implies that $\mathcal{F}_1$ is determinantal.

Next, we shall treat the case that $\chi_{\mathcal{F}_2} < 0$. In this case, by (1.5), we can take (Zariski locally) a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_Y^{h^0(\mathcal{F}_1,y)} & \to & \mathcal{O}_Y^{h^0(\mathcal{F}_2,y)} \\ \downarrow & & \downarrow \\ \mathcal{O}_Y^{h^1(\mathcal{F}_1,y)} & \to & \mathcal{O}_Y^{h^1(\mathcal{F}_2,y)} \end{array} \tag{1.14}$$

representing the morphism $Rf_*(\mathcal{F}_1) \to Rf_*(\mathcal{F}_2)$. Then, localizing (1.14) at $y \in Y$ and taking the dual ($= \mathrm{Hom}_R(-, R)$, where $R = \mathcal{O}_{Y,y}$) of the diagram, we obtain a commutative diagram of free R-modules such as

$$\begin{array}{ccc} G' & \leftarrow & G \\ \phi' \uparrow & & \phi \uparrow \\ F' & \leftarrow & F \end{array} ,$$

where $\mathrm{rk}(G') = h^0(\mathcal{F}_1, y)$, $\mathrm{rk}(F') = h^1(\mathcal{F}_1, y)$, $\mathrm{rk}(G) = h^0(\mathcal{F}_2, y)$, and $\mathrm{rk}(F) = h^1(\mathcal{F}_2, y)$. If we regard this diagram as (1.11), the proof in the case $\chi_{\mathcal{F}_2} < 0$ can be done just in parallel with that of $\chi_{\mathcal{F}_2} > 0$. This completes the proof. □

2. Generalizations of Raynaud's Theorem

Let k be an algebraically closed field and X a proper, smooth, connected curve of genus g over k.

For a vector bundle E on X (regarded as a locally free $\mathcal{O}_X$-module of finite rank), let $\mathrm{rk}(E)$, $\deg(E)$ and $h^i(E)$ $(i = 0, 1)$ denote the rank of E, the degree of E (which is defined to be the degree of the line bundle $\det(E) \overset{\text{def}}{=} \overset{\mathrm{rk}(E)}{\wedge} E$), and the dimension (as a k-vector space) of the i-th cohomology group $H^i(X, E)$. The Riemann–Roch theorem implies the following formula for the Euler–Poincaré characteristic $\chi(E) \overset{\text{def}}{=} h^0(E) - h^1(E)$ of E:

$$\chi(E) = \deg(E) - (g-1)\,\mathrm{rk}(E). \tag{2.1}$$

In [R1], Raynaud investigated the following property of a vector bundle E on X.

Definition (Condition $(\star)$). We say that E satisfies $(\star)$ if there exists a line bundle L of degree 0 on X such that $\min(h^0(E \otimes L), h^1(E \otimes L)) = 0$.

First, we shall see the relation between condition $(\star)$ and the contents of Section 1. So, Let J be the Jacobian variety of X, and let $\mathcal{L}$ be a universal line bundle on $X \times J$. Let pr_X and pr_J denote the projections $X \times J \to X$ and $X \times J \to J$, respectively. Regarding $\mathrm{pr}_J : X \times J \to J$ and $(\mathrm{pr}_X)^*(E) \otimes \mathcal{L}$ as $f : X \to Y$ and $\mathcal{F}$ in Section 1, respectively, we can apply definitions and results to our situation.

Definition. We denote by Θ_E the closed subscheme $W((\mathrm{pr}_X)^*(E) \otimes \mathcal{L})$ of J.

We have the following first properties of Θ_E.

Proposition (2.2). *Let the notations be as above.*

(i) *The definition of Θ_E is independent of the choice of $\mathcal{L}$.*

(ii) *Let L be a line bundle of degree 0 on X, and let $[L]$ denote the point of J corresponding to L. Then, $[L] \notin \Theta_E$ if and only if*

$$\min(h^0(E \otimes L), h^1(E \otimes L)) = 0.$$

(iii) *We have the following implications*:

$$\begin{array}{ccc} \Theta_E = \varnothing \text{ or } \mathrm{codim}(\Theta_E) = |\chi(E)| + 1 & \iff & (\mathrm{pr}_X)^*(E) \otimes \mathcal{L} \text{ is determinantal} \\ \Downarrow & & \\ \Theta_E \neq J & \iff & E \text{ satisfies } (\star). \end{array}$$

Moreover, if $\chi(E) = 0$, the above four conditions are all equivalent.

Proof. (i) It is known that the difference of two choices of $\mathcal{L}$ comes from a line bundle on J. So, Zariski locally on J, the difference is resolved. Since the definition of Fitting ideal is of local nature (see (1.1)), this shows the desired well-definedness of Θ_E.

(ii) The fiber $(\mathrm{pr}_J)^{-1}([L])$ is naturally identified with X, and the restriction of $(\mathrm{pr}_X)^*(E) \otimes \mathcal{L}$ to this fiber is nothing but $E \otimes L$. Now, (ii) is just the second half of (1.2).

(iii) The first $\iff$ is just the definition, if we note that $\chi_{(\mathrm{pr}_X)^*(E)\otimes\mathcal{L}}$ defined in Section 1 coincides with $\chi(E)$. The second $\Rightarrow$ is trivial, and the third $\iff$ follows from (ii). Finally, if $\chi(E) = 0$, Macaulay's theorem (see Section 1) says that either $\Theta_E = \varnothing$ or $\mathrm{codim}(\Theta_E) \leq 1$. So, in this case, the converse of the second $\Rightarrow$ also holds. □

From now on, we assume that k is of characteristic $p > 0$. For an $\mathbb{F}_p$-scheme S, we shall denote by F_S the absolute Frobenius endomorphism $S \to S$. We define X_1 to be the pull-back of X by $F_{\mathrm{Spec}(k)}$, and denote by $F_{X/k}$ the relative Frobenius morphism $X \to X_1$ over k.

We put $B = ((F_{X/k})_*(\mathcal{O}_X))/\mathcal{O}_{X_1}$, which is a vector bundle on X_1 with $\mathrm{rk}(B) = p-1$ and $\chi(B) = 0$. In [R1], Raynaud proved, among other things, the following:

THEOREM. ([R1], Théorème 4.1.1.) *The vector bundle B on X_1 satisfies* $(\star)$. □

As an application of this theorem, Raynaud proved, roughly speaking, that the p-ranks of the Jacobian varieties of 'most' (prime-to-p-)cyclic étale coverings of X are as large as can be expected. In order to generalize such a result to ramified coverings, we need to modify the vector bundle B, so that it involves a divisor whose support is in the ramification locus. So, the aim of this section is to generalize Raynaud's theorem along these lines, and, in the next section, the application to cyclic ramified coverings will be given.

Let $q = p^f$ be a power of p ($f \geq 1$). We define X_f to be the pull-back of X by $(F_{\mathrm{Spec}(k)})^f$, and define $F^f_{X/k} : X \to X_f$ to be the composite of the f relative Frobenius morphisms: $F^f_{X/k} \overset{\mathrm{def}}{=} F_{X_{f-1}/k} \circ \cdots \circ F_{X_1/k} \circ F_{X/k}$.

Let $D = \sum_{P\in X} n_P P$ be an effective divisor on X (i.e., $n_P \geq 0$ for all P). We shall write $\mathrm{ord}_P(D)$ instead of n_P, which is a non-negative integer. Then, by definition, $\deg(D) = \sum_{P\in X} \mathrm{ord}_P(D)$.

DEFINITION. We put

$$B^f_D = ((F^f_{X/k})_*(\mathcal{O}_X(D)))/\mathcal{O}_{X_f}.$$

LEMMA (2.3). (i) *B^f_D is a vector bundle on X_f if and only if the torsion-freeness condition*

$$\mathrm{ord}_P(D) < q \text{ for each } P \in X \qquad \text{(TF)}$$

holds.

(ii) *Assume that* (TF) *holds. Then we have*

$$\mathrm{rk}(B^f_D) = q-1,\ \deg(B^f_D) = \deg(D) + (g-1)(q-1),\ \chi(B^f_D) = \deg(D).$$

More generally, for a line bundle L on X_f, we have

$$\mathrm{rk}(B_D^f \otimes L) = q-1,\ \deg(B_D^f \otimes L) = \deg(D) + (g-1+\deg(L))(q-1),$$

and

$$\chi(B_D^f \otimes L) = \deg(D) + \deg(L)(q-1). \tag{2.4}$$

Proof. (i) Since B_D^f is a coherent sheaf on the (smooth) curve X_f, it is a vector bundle if and only if the stalk $(B_D^f)_{P_f}$ is a torsion-free $\mathcal{O}_{X_f,P_f}$-module for each $P_f \in X_f$. By definition, we have $(B_D^f)_{P_f} = (\mathfrak{m}_{X,P})^{-\operatorname{ord}_P(D)}/\mathcal{O}_{X_f,P_f}$, where P is the unique point of X above P_f and $\mathfrak{m}_{X,P}$ denotes the maximal ideal of the local ring $\mathcal{O}_{X,P}$. So, $(B_D^f)_{P_f}$ is torsion-free if and only if $(\mathfrak{m}_{X,P})^{-\operatorname{ord}_P(D)} \cap k(X_f) = \mathcal{O}_{X_f,P_f}$, which turns out to be equivalent to $\operatorname{ord}_P(D) < q$. This completes the proof.

(ii) We have

$$\mathrm{rk}(B_D^f) = \mathrm{rk}((F_{X/k}^f)_*(\mathcal{O}_X(D))) - \mathrm{rk}(\mathcal{O}_{X_f}) = q-1$$

and

$$\chi(B_D^f) = \chi((F_{X/k}^f)_*(\mathcal{O}_X(D))) - \chi(\mathcal{O}_{X_f}) = (\deg(D)+1-g) - (1-g) = \deg(D).$$

From these, $\deg(B_D^f)$ can be calculated by using (2.1).

Moreover, for a line bundle L on X_f, we have

$$\mathrm{rk}(B_D^f \otimes L) = \mathrm{rk}(B_D^f) = q-1$$

and

$$\deg(B_D^f \otimes L) = \deg(B_D^f) + \mathrm{rk}(B_D^f)\deg(L) = \deg(D) + (g-1+\deg(L))(q-1).$$

From these, $\chi(B_D^f \otimes L)$ can be calculated by using (2.1). □

Now, the following is one of the main results of this section.

Theorem (2.5). *Assume* $\deg(D) = q-1$, *and let* L_{-1} *be a line bundle of degree* -1 *on* X_f. *Then* $B_D^f \otimes L_{-1}$ *is a vector bundle on* X_f *with* $\chi = 0$, *and satisfies* $(\star)$.

Before proving (2.5), we shall give a slight generalization (which will be used later), assuming (2.5):

Corollary (2.6). *Let* s *be a non-negative integer. We assume that* $\deg(D) = s(q-1)$ *and that*

$$\#\{P \in X \mid \operatorname{ord}_P(D) = q-1\} \geq s-1.$$

Let L_{-s} *be a line bundle of degree* $-s$ *on* X_f. *Then* $B_D^f \otimes L_{-s}$ *is a vector bundle on* X_f *with* $\chi = 0$, *and satisfies* $(\star)$.

PROOF. Let D_0 be an effective divisor on X, and Q a point of X which is not contained in the support of D_0. We put $D_1 = D_0 + (q-1)Q$, and consider the following commutative diagram with two rows exact:

$$\begin{array}{ccccccccc}
0 \to & \mathcal{O}_{X_f}(-Q_f) & \to & (F^f_{X/k})_*(\mathcal{O}_X(D_1)) \otimes \mathcal{O}_{X_f}(-Q_f) & \to & B^f_{D_1} \otimes \mathcal{O}_{X_f}(-Q_f) & \to 0 \\
 & & & \| & & & \\
 & \bigcap & & (F^f_{X/k})_*(\mathcal{O}_X(D_0 - Q)) & & \vdots & \\
 & & & \bigcap & & \vee & \\
0 \to & \mathcal{O}_{X_f} & \to & (F^f_{X/k})_*(\mathcal{O}_X(D_0)) & \to & B^f_{D_0} & \to 0,
\end{array}$$

where Q_f denotes $F^f_{X/k}(Q)$ $(\in X_f)$. From this, we can see

$$B^f_{D_1} \otimes \mathcal{O}_{X_f}(-Q_f) \xrightarrow{\sim} B^f_{D_0}.$$

Using this isomorphism repeatedly, our assumption

$$\#\{P \in X \mid \mathrm{ord}_P(D) = q-1\} \geq s-1$$

enables us to reduce the problem to the case $s \leq 1$. The case $s = 1$ is just (2.5). The case $s = 0$ can be reduced to the case $s = 1$ again by using this isomorphism. (Choose any $Q \in X$.) □

Note that (2.6) includes Raynaud's original theorem as the case that $f = 1$ and $s = 0$.

PROOF OF (2.5). Since $\deg(D) = q - 1 < q$, (TF) clearly holds, hence B^f_D is a vector bundle by (2.3)(i). Moreover, we have $\chi(B^f_D \otimes L_{-1}) = \deg(D) + \deg(L_{-1})(q-1) = 0$ by (2.4).

We would like to prove that $B^f_D \otimes L_{-1}$ satisfies $(\star)$ by using (1.12). To do this, let J_f be the Jacobian variety of X_f, and let $\mathcal{L}_f$ be a universal line bundle on $X_f \times J_f$. Let pr_{X_f} and pr_{J_f} denote the projections $X_f \times J_f \to X_f$ and $X_f \times J_f \to J_f$, respectively.

The main difficulty is that, unlike Raynaud's original case, we cannot apply (1.12) directly to the exact sequence on $X_f \times J_f$ obtained by taking $(\mathrm{pr}_{X_f})^*(-) \otimes \mathcal{L}_f$ of the exact sequence

$$0 \to L_{-1} \to (F^f_{X/k})_*(\mathcal{O}_X(D)) \otimes L_{-1} \to B^f_D \otimes L_{-1} \to 0$$

on X_f, because $W((\mathrm{pr}_{X_f})^*(L_{-1}) \otimes \mathcal{L}_f) = \varnothing$ and condition (b) of (1.12) is not satisfied (unless $g = 0$). (Note that $h^0(L_{-1} \otimes L) = 0$ for all line bundle L of degree 0 on X_f.) This leads us to the following procedure.

Since the validity of (2.5) is independent of the choice of the line bundle L_{-1} of degree -1, we may and shall assume $L_{-1} = \mathcal{O}_{X_f}(-Q_f)$, where we fix any

$Q \in X$ and put $Q_f = F^f_{X/k}(Q)$. By definition, we have the exact sequence

$$\begin{array}{ccccccc} 0 \to \mathcal{O}_{X_f}(-Q_f) \to & (F^f_{X/k})_*(\mathcal{O}_X(D)) \otimes \mathcal{O}_{X_f}(-Q_f) & \to B^f_D \otimes \mathcal{O}_{X_f}(-Q_f) \to 0. \\ & \| & \\ & (F^f_{X/k})_*(\mathcal{O}_X(D-qQ)) & \end{array}$$

Let $E^f_{D,Q}$ be the sum of $\mathcal{O}_{X_f}$ and $(F^f_{X/k})_*(\mathcal{O}_X(D-qQ))$ in $(F^f_{X/k})_*(\mathcal{O}_X(D))$. This coincides with the amalgamated sum with respect to $\mathcal{O}_{X_f}(-Q_f)$, since $\mathcal{O}_{X_f} \cap (F^f_{X/k})_*(\mathcal{O}_X(D-qQ)) = \mathcal{O}_{X_f}(-Q_f)$. Thus the vector bundle $E^f_{D,Q}$ fits into the following commutative diagram with two rows exact:

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{O}_{X_f}(-Q_f) & \to & (F^f_{X/k})_*(\mathcal{O}_X(D-qQ)) & \to & B^f_D \otimes \mathcal{O}_{X_f}(-Q_f) & \to & 0 \\ & & \bigcap & & \bigcap & & \| & & \\ 0 & \to & \mathcal{O}_{X_f} & \to & E^f_{D,Q} & \to & B^f_D \otimes \mathcal{O}_{X_f}(-Q_f) & \to & 0. \end{array} \tag{2.7}$$

If $\Theta_{B^f_D \otimes \mathcal{O}_{X_f}(-Q_f)} = \varnothing$, the assertion of (2.5) clearly holds. So, from now on, we assume $\Theta_{B^f_D \otimes \mathcal{O}_{X_f}(-Q_f)} \neq \varnothing$. Then, in order to prove that $\Theta_{B^f_D \otimes \mathcal{O}_{X_f}(-Q_f)} \neq J_f$, we shall apply (1.12) to the exact sequence on $X_f \times J_f$ obtained by taking $(\mathrm{pr}_{X_f})^*(-) \otimes \mathcal{L}_f$ of the second row of (2.7).

First, we shall check condition (b) of (1.12). Note that

$$\chi_{(\mathrm{pr}_{X_f})^*(E^f_{D,Q}) \otimes \mathcal{L}_f} = \chi(E^f_{D,Q}) = \chi(\mathcal{O}_{X_f}) + \chi(B^f_D \otimes \mathcal{O}_{X_f}(-Q_f)) = 1 - g.$$

If $g = 0$, condition (b) is equivalent to $\Theta_{B^f_D \otimes \mathcal{O}_{X_f}(-Q_f)} \neq \varnothing$, which we have just assumed. If $g = 1$, condition (b) automatically holds. If $g > 1$, condition (b) is equivalent to $\Theta_{\mathcal{O}_{X_f}} \neq \varnothing$, which follows from $\Theta_{\mathcal{O}_{X_f}} \ni 0$. (Note that $h^0(\mathcal{O}_{X_f}) = 1$ and $h^1(\mathcal{O}_{X_f}) = g$.)

Moreover, since

$$\chi_{(\mathrm{pr}_{X_f})^*(B^f_D \otimes \mathcal{O}_{X_f}(-Q_f)) \otimes \mathcal{L}_f} = \chi(B^f_D \otimes \mathcal{O}_{X_f}(-Q_f)) = 0,$$

condition (c) of (1.12) holds.

Finally, we shall check that condition (a) holds, or, equivalently, that either $\Theta_{E^f_{D,Q}} = \varnothing$ or $\mathrm{codim}(\Theta_{E^f_{D,Q}}) = |1-g|+1$. Namely, we have to prove that $\Theta_{E^f_{D,Q}}$ is finite over k (resp. empty) if $g > 0$ (resp. $g = 0$). This is the most difficult part of our proof. (In Raynaud's original case, this part was immediate. See (2.11)(ii).)

Lemma (2.8). *We have*

$$h^0_{\max} \stackrel{\mathrm{def}}{=} \max\{h^0(E^f_{D,Q} \otimes L) \mid [L] \in J_f\} = 1$$

and

$$h^1_{\max} \stackrel{\mathrm{def}}{=} \max\{h^1(E^f_{D,Q} \otimes L) \mid [L] \in J_f\} = g.$$

PROOF. Since $\chi(E^f_{D,Q} \otimes L) = 1 - g$, it is sufficient to prove the first equality.

By (2.7), we get an exact sequence

$$0 \to (F^f_{X/k})_*(\mathcal{O}_X(D - qQ)) \to E^f_{D,Q} \to \boldsymbol{k}(Q_f) \to 0.$$

So, we have

$$\begin{aligned} h^0(E^f_{D,Q} \otimes L) &\leq h^0((F^f_{X/k})_*(\mathcal{O}_X(D - qQ)) \otimes L) + 1 \\ &= h^0(\mathcal{O}_X(D - qQ) \otimes (F^f_{X/k})^*(L)) + 1 = 1, \end{aligned}$$

the last equality following from the fact that $\deg(\mathcal{O}_X(D - qQ) \otimes (F^f_{X/k})^*(L)) = -1 < 0$. Therefore, we have $h^0_{\max} \leq 1$. On the other hand, since $E^f_{D,Q}$ contains $\mathcal{O}_{X_f}$, we have

$$1 \leq h^0(E^f_{D,Q}) \leq h^0_{\max}.$$

This completes the proof. □

We shall return to the proof of (2.5). Put $W \overset{\text{def}}{=} \Theta_{E^f_{D,Q}}$ $(\subset J_f)$ for simplicity. If $g = 0$, we have $W = \varnothing$ by (1.2) and (2.8), as desired. So, we shall assume $g > 0$ and prove that W is finite over k. Note that, again by (1.2) and (2.8), we have

$$\begin{aligned} W &= \{[L] \in J_f \mid h^0(E^f_{D,Q} \otimes L) = 1\} \\ &= \{[L] \in J_f \mid h^1(E^f_{D,Q} \otimes L) = g\}, \end{aligned}$$

set-theoretically.

We define the divisor D' on X to be the 'prime-to-Q part' of D, namely,

$$D' \overset{\text{def}}{=} \sum_{P \in X, P \neq Q} \operatorname{ord}_P(D) P,$$

and let d' denote the degree of D'. Then, by using the definition of $E^f_{D,Q}$, we see that the following exact sequence exists:

$$\begin{aligned} 0 \to (F^f_{X/k})_*(\mathcal{O}_X(D - qQ)) \to E^f_{D,Q} \oplus (F^f_{X/k})_*(\mathcal{O}_X(D' - Q)) \\ \to (F^f_{X/k})_*(\mathcal{O}_X(D')) \to 0. \end{aligned}$$

For each $[L] \in W$, we tensor this sequence with L and take the global sections. Then we will obtain

$$\begin{array}{ccccc} H^0(X_f, E^f_{D,Q} \otimes L) & \oplus & H^0(X_f, (F^f_{X/k})_*(\mathcal{O}_X(D' - Q)) \otimes L) & & \\ \wr\uparrow & & \| & & \\ k & & H^0(X, \mathcal{O}_X(D' - Q) \otimes (F^f_{X/k})^*(L)) & & \\ & & & \hookrightarrow & H^0(X_f, (F^f_{X/k})_*(\mathcal{O}_X(D')) \otimes L) \\ & & & & \| \\ & & & & H^0(X, \mathcal{O}_X(D') \otimes (F^f_{X/k})^*(L)). \end{array}$$

That is to say, each $[L] \in W$ defines a point of

$$\mid \mathcal{O}_X(D') \otimes (F^f_{X/k})^*(L) \mid - \mid \mathcal{O}_X(D' - Q) \otimes (F^f_{X/k})^*(L) \mid .$$

Here, for a line bundle M on X, $\mid M \mid$ denotes the (schematized) projective space $(H^0(X, M) - \{0\})/k^\times$.

In other words, consider the following diagram:

$$\begin{array}{ccccccc} W \subset J_f & \overset{V^f}{\hookrightarrow} & J & \overset{+(D'-Q)}{\overset{\sim}{\to}} & J^{(d'-1)} & \overset{+Q}{\overset{\sim}{\to}} & J^{(d')} \\ & & & & \uparrow & & \uparrow \\ & & & & X^{(d'-1)} & \overset{+Q}{\hookrightarrow} & X^{(d')} \\ & & & & & & \bigcup \\ & & & & & & X^{(d')} - X^{(d'-1)} \end{array} \tag{2.9}$$

where V^f denotes the composite of the f Verschiebungs, i.e., $V^f : [L] \mapsto [(F^f_{X/k})^*(L)]$, $J^{(r)}$ denotes the degree r part of the Picard variety of X (hence, in particular, $J^{(0)} = J$), and $X^{(r)}$ denotes the r-th symmetric power of X. (We put $X^{(0)} = \mathrm{Spec}(k)$ and $X^{(-1)} = \varnothing$.) In this setting, the above observation tells us that there exists a natural set-theoretic map $W \to X^{(d')} - X^{(d'-1)}$ over $J^{(d')}$.

Now, assume that this map $W \to X^{(d')} - X^{(d'-1)}$ can be regarded as a morphism (as $J^{(d')}$-schemes). Then, since $W \to J^{(d')}$ is a finite morphism, so is $W \to X^{(d')} - X^{(d'-1)}$. Now, since $X^{(d')} - X^{(d'-1)} = (X - \{Q\})^{(d')}$ is affine, so is W. On the other hand, W is proper over k as a closed subscheme of J_f. Thus W must be finite over k.

So, it suffices to prove that the above set-theoretic map $W \to X^{(d')} - X^{(d'-1)}$ is a morphism. To do this, we name the morphisms involved as follows, for the sake of simplicity:

$$\begin{array}{ccccc} X & \overset{\xi}{\leftarrow} & X \times W & & \\ & & & \searrow^{\eta} & \\ \downarrow \pi & \square & \downarrow \pi_W & \circlearrowleft & W, \\ & & & \nearrow_{\eta'} & \\ X_f & \overset{\xi'}{\leftarrow} & X_f \times W & & \end{array} \tag{2.10}$$

where $\pi = F^f_{X/k}$, π_W is the base change of π, and ξ, ξ', η and η' are projections.

We shall apply the functor (from the category of $\mathcal{O}_{X_f}$-modules to that of $\mathcal{O}_{X \times W}$-modules)

$$\eta^* \eta'_* (\xi'^*(-) \otimes (\mathcal{L}_f)_W)$$

to the natural map $E^f_{D,Q} \hookrightarrow \pi_*(\mathcal{O}_X(D'))$. By the flat base change theorem and the projection formula, we have

$$\begin{aligned} \xi'^*(\pi_*(\mathcal{O}_X(D'))) \otimes (\mathcal{L}_f)_W &= (\pi_W)_*(\xi^*(\mathcal{O}_X(D'))) \otimes (\mathcal{L}_f)_W \\ &= (\pi_W)_*(\xi^*(\mathcal{O}_X(D')) \otimes (\pi_W)^*(\mathcal{L}_f)_W). \end{aligned}$$

Thus we obtain

$$\eta^*\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)\to\eta^*\eta_*(\xi^*(\mathcal{O}_X(D'))\otimes(\pi_W)^*(\mathcal{L}_f)_W),$$

and taking the composite with the natural map $\eta^*\eta_*(-)\to(-)$, we obtain

$$\eta^*\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)\to\xi^*(\mathcal{O}_X(D'))\otimes(\pi_W)^*(\mathcal{L}_f)_W.$$

By (1.2) and (2.8), we have $Z_g(\xi'^*(E^f_{D,Q})\otimes\mathcal{L}_f)=\varnothing$. So, by (1.4) and its proof, $R^1\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)$ is a locally free $\mathcal{O}_W$-module of rank g. (Note that we have $R^1\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)=R^1\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f))|_W$.) By this and (1.5), we see that $R\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)$ can be represented Zariski locally by the complex $(\mathcal{O}_W\overset{0}{\to}\mathcal{O}_W^g)$. In particular, $\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)$ is a locally free $\mathcal{O}_W$-module of rank 1, and, for each $z\in W$, $\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)\otimes\boldsymbol{k}(z)\overset{\sim}{\to}H^0((X_f)_{\boldsymbol{k}(z)},E^f_{D,Q}\otimes L_z)$, where L_z is the line bundle on $(X_f)_{\boldsymbol{k}(z)}$ corresponding to $z\in W\subset J_f$. (We denote the base change from k to $\boldsymbol{k}(z)$ by means of a subscript $\boldsymbol{k}(z)$.) Hence the pull-back of the $\mathcal{O}_{X\times W}$-module $\eta^*\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)$ to $X_{\boldsymbol{k}(z)}$ can be identified with

$$H^0((X_f)_{\boldsymbol{k}(z)},E^f_{D,Q}\otimes L_z)\otimes_{\boldsymbol{k}(z)}\mathcal{O}_{X_{\boldsymbol{k}(z)}}.$$

On the other hand, the pull-back of $\xi^*(\mathcal{O}_X(D'))\otimes(\pi_W)^*(\mathcal{L}_f)_W$ to $X_{\boldsymbol{k}(z)}$ is $\mathcal{O}_X(D')\otimes(\pi_{\boldsymbol{k}(z)})^*(L_z)$, and we can check that the resulting map

$$H^0((X_f)_{\boldsymbol{k}(z)},E^f_{D,Q}\otimes L_z)\otimes_{\boldsymbol{k}(z)}\mathcal{O}_{X_{\boldsymbol{k}(z)}}\to\mathcal{O}_X(D')\otimes(\pi_{\boldsymbol{k}(z)})^*(L_z)$$

is the composite of

$$\left\{\begin{array}{rcl}H^0((X_f)_{\boldsymbol{k}(z)},E^f_{D,Q}\otimes L_z) & \to & H^0((X_f)_{\boldsymbol{k}(z)},\pi_*(\mathcal{O}_X(D'))\otimes L_z)\\ & & \|\\ & & H^0(X_{\boldsymbol{k}(z)},\mathcal{O}_X(D')\otimes(\pi_{\boldsymbol{k}(z)})^*(L_z))\end{array}\right\}\otimes_{\boldsymbol{k}(z)}\mathcal{O}_{X_{\boldsymbol{k}(z)}}$$

and the natural map

$$H^0(X_{\boldsymbol{k}(z)},\mathcal{O}_X(D')\otimes(\pi_{\boldsymbol{k}(z)})^*(L_z))\otimes_{\boldsymbol{k}(z)}\mathcal{O}_{X_{\boldsymbol{k}(z)}}\to\mathcal{O}_X(D')\otimes(\pi_{\boldsymbol{k}(z)})^*(L_z).$$

Here, as in the previous argument, the map

$$H^0((X_f)_{\boldsymbol{k}(z)},E^f_{D,Q}\otimes L_z)\to H^0(X_{\boldsymbol{k}(z)},\mathcal{O}_X(D')\otimes(\pi_{\boldsymbol{k}(z)})^*(L_z))$$

is injective. Since $H^0((X_f)_{\boldsymbol{k}(z)},E^f_{D,Q}\otimes L_z)$ is a one-dimensional $\boldsymbol{k}(z)$-vector space, we conclude that

$$(\eta^*\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W))\otimes\boldsymbol{k}(z)\to(\xi^*(\mathcal{O}_X(D'))\otimes(\pi_W)^*(\mathcal{L}_f)_W)\otimes\boldsymbol{k}(z)$$

is injective. Now, by [EGA4], Proposition (11.3.7), the map

$$\eta^*\eta'_*(\xi'^*(E^f_{D,Q})\otimes(\mathcal{L}_f)_W)\to\xi^*(\mathcal{O}_X(D'))\otimes(\pi_W)^*(\mathcal{L}_f)_W$$

is injective and its cokernel is flat over W. Hence it equips $\xi^*(\mathcal{O}_X(D'))\otimes(\pi_W)^*(\mathcal{L}_f)_W$ with a structure of relative effective Cartier divisor on $X\times W/W$.

Thus we are given the morphism $W \to X^{(d')}$ over $J_f^{(d')}$, whose underlying map coincides with the set-theoretic map $W \to X^{(d')} - X^{(d'-1)}$ in the previous argument. (See [Mi], § 3, especially Proposition 3.13 there.) This completes the proof of the finiteness of W.

Now, we can apply (1.12) and conclude that $(\mathrm{pr}_{X_f})^*(B_D^f \otimes \mathcal{O}_{X_f}(-Q_f)) \otimes \mathcal{L}_f$ is determinantal, or, equivalently, that $\Theta_{B_D^f \otimes \mathcal{O}_{X_f}(-Q_f)}$ $\big(= W((\mathrm{pr}_{X_f})^*(B_D^f \otimes \mathcal{O}_{X_f}(-Q_f)) \otimes \mathcal{L}_f)\ \big) \neq J_f$. This finally completes the proof of (2.5). □

Remark (2.11). (i) When $D = (q-1)Q$, $E_{D,Q}^f$ coincides with $(F_{X/k}^f)_*(\mathcal{O}_X)$. In general, $E_{D,Q}^f$ is not isomorphic to the direct image of a line bundle on X. In fact, suppose that $E_{D,Q}^f$ is isomorphic to $(F_{X/k}^f)_*(M)$ for some line bundle M on X. Then we have

$$\chi(M) = \chi((F_{X/k}^f)_*(M)) = \chi(\mathcal{O}_{X_f}) + \chi(B_D^f \otimes \mathcal{O}_{X_f}(-Q_f)) = 1 - g,$$

hence $\deg(M) = 0$. On the other hand, since $\mathcal{O}_{X_f} \subset (F_{X/k}^f)_*(M)$, M admits a non-trivial global section. Thus $M \simeq \mathcal{O}_X$. By the definition of $E_{D,Q}^f$, we can see that

$$\det((F_{X/k}^f)_*(M)) \simeq \det((F_{X/k}^f)_*(\mathcal{O}_X(D - qQ))) \otimes \mathcal{O}_{X_f}(Q_f),$$

and since $M \simeq \mathcal{O}_X$, we have

$$\det((F_{X/k}^f)_*(\mathcal{O}_X(D - qQ))) \otimes \det((F_{X/k}^f)_*(\mathcal{O}_X))^{-1} \otimes \mathcal{O}_{X_f}(Q_f) \simeq \mathcal{O}_{X_f}.$$

Here the left-hand side is known to be isomorphic to

$$\mathcal{O}_{X_f}(D_f - qQ_f) \otimes \mathcal{O}_{X_f}(Q_f) \simeq \mathcal{O}_{X_f}(D_f - (q-1)Q_f),$$

where $D_f \overset{\mathrm{def}}{=} \sum_{P \in X} \mathrm{ord}_P(D) P_f$. Thus it follows that the divisor $D_f - (q-1)Q_f$ on X_f should be principal, which does not hold in general.

(ii) When $D = (q-1)Q$, the subscheme W of J_f is nothing but $\mathrm{Ker}(V^f)$, hence its degree over k is p^f. In general, the author does not know much about the finite k-scheme W. For example, he does not know its degree over k.

In later sections, we use a slight generalization (2.13) of (2.6). First, we shall prove the following:

Lemma (2.12). *Let s be a non-negative integer.*

(i) *Let f be a natural number and D an effective divisor of degree $s(p^f - 1)$ on X satisfying* (TF) *with respect to $q = p^f$. Let f_1 be a natural number. Then the vector bundle $B_D^f \otimes L_{-s}$ on X_f satisfies condition $(\star)$ of page 59 for some (or, equivalently, all) line bundle L_{-s} of degree $-s$ on X_f, if and only if the vector bundle $B_{D_{f_1}}^f \otimes L_{1,-s}$ on X_{f_1+f} satisfies condition $(\star)$ for some (or, equivalently, all) line bundle $L_{1,-s}$ of degree $-s$ on X_{f_1+f}.*

(ii) *For each* $i = 0, 1$, *we let* f_i *be a natural number*, D_i *an effective divisor of degree* $s(p^{f_i}-1)$ *satisfying* (TF) *with respect to* $q = p^{f_i}$. *Then* $D \overset{\text{def}}{=} p^{f_1}D_0 + D_1$ *becomes an effective divisor of degree* $s(p^f - 1)$ *satisfying* (TF) *with respect to* $q = p^f$, *where* $f \overset{\text{def}}{=} f_0 + f_1$. *Moreover*, $B^f_D \otimes L_{-s}$ *satisfies condition* $(\star)$ *for some* (*or all*) *line bundle* L_{-s} *of degree* $-s$ *on* X_f, *if and only if*, *for each* $i = 0, 1$, $B^{f_i}_{D_i} \otimes L_{i,-s}$ *satisfies condition* $(\star)$ *for some* (*or all*) *line bundle* $L_{i,-s}$ *of degree* $-s$ *on* X_{f_i}.

Proof. (i) Under the natural (p^{f_1}-linear) isomorphism $X_{f_1} \overset{\sim}{\to} X$ of schemes, $B^f_{D_{f_1}}$ corresponds to B^f_D and the line bundles of degree $-s$ correspond to the line bundles of degree $-s$.

(ii) First the numerical conditions can be checked as follows:

$$\deg(D) = p^{f_1}\deg(D_0) + \deg(D_1) = p^{f_1}s(p^{f_0}-1) + s(p^{f_1}-1) = s(p^f - 1),$$

$$\operatorname{ord}_P(D) = p^{f_1}\operatorname{ord}_P(D_0) + \operatorname{ord}_P(D_1) \leq p^{f_1}(p^{f_0}-1) + (p^{f_1}-1) = p^f - 1.$$

For simplicity, we shall denote by π, π_1 and π_{0,f_1} the relative Frobenius morphisms $F^f_{X/k} : X \to X_f$, $F^{f_1}_{X/k} : X \to X_{f_1}$ and $F^{f_0}_{X_{f_1}/k} : X_{f_1} \to X_f$, respectively, so that $\pi = \pi_{0,f_1} \circ \pi_1$. We have natural homomorphisms

$$\mathcal{O}_{X_f} \to (\pi_{0,f_1})_*(\mathcal{O}_{X_{f_1}}((D_0)_{f_1})) \to \pi_*(\mathcal{O}_X(D))$$

of $\mathcal{O}_{X_f}$-modules, and obtain the following exact sequence:

$$0 \to B^{f_0}_{(D_0)_{f_1}} \to B^f_D \to (\pi_{0,f_1})_*(B^{f_1}_{D_1} \otimes \mathcal{O}_{X_{f_1}}((D_0)_{f_1})) \to 0.$$

From this, the first assertion follows. Moreover, tensoring this exact sequence with L_{-s}, we obtain

$$0 \to B^{f_0}_{(D_0)_{f_1}} \otimes L_{-s} \to B^f_D \otimes L_{-s} \to (\pi_{0,f_1})_*(B^{f_1}_{D_1} \otimes \mathcal{O}_{X_{f_1}}((D_0)_{f_1}) \otimes (\pi_{0,f_1})^*(L_{-s})) \to 0.$$

Now, since

$$\deg(\mathcal{O}_{X_{f_1}}((D_0)_{f_1}) \otimes (\pi_{0,f_1})^*(L_{-s})) = s(p^{f_0}-1) + p^{f_0}(-s) = -s,$$

the second assertion follows from the associated long exact sequence (and (i)). □

Corollary (2.13). *Let* s *be a non-negative integer*, D *an effective divisor of degree* $s(p^f - 1)$ *on* X. *Assume the following condition*:

Condition (2.14). *There exist natural numbers* f_i *and effective divisors* D_i *of degree* $s(p^{f_i} - 1)$ $(i = 0, 1, \ldots, k)$, *such that* $f = \sum_{i=0}^k f_i$, $D = \sum_{i=0}^k p^{f_{>i}} D_i$, *where* $f_{>i} \overset{\text{def}}{=} \sum_{j=i+1}^k f_j$ $(f_{>k} = 0)$, *and that*, *for each* $i = 0, 1, \ldots k$,

$$\#\{P \in X \mid \operatorname{ord}_P(D_i) = p^{f_i} - 1\} \geq s - 1.$$

Then, *for a line bundle* L_{-s} *of degree* $-s$ *on* X_f, $B^f_D \otimes L_{-s}$ *is a vector bundle on* X_f *with* $\chi = 0$, *and satisfies* $(\star)$.

PROOF. Use (2.6) for each D_i and apply (2.12) repeatedly. □

What can we expect for a more general effective divisor D? For the time being, we are interested in vector bundles with $\chi = 0$. So, considering (2.4), we shall assume that $\deg(D) = s(q-1)$ for some natural number s, and consider $B_D^f \otimes L_{-s}$ for a line bundle L_{-s} of degree $-s$ on X_f. Moreover, we have to assume the torsion-freeness condition (TF): $\mathrm{ord}_P(D) < q$ for each $P \in X$, which does not hold automatically this time. Under these assumptions, can we expect that $B_D^f \otimes L_{-s}$ satisfies $(\star)$?

In general, the answer is no. In fact, as Raynaud remarked in [R1], § 0, condition $(\star)$ for a vector bundle E with $\chi(E) = 0$ implies that E is semi-stable, in the sense that $\deg(F)/\mathrm{rk}(F) \leq \deg(E)/\mathrm{rk}(E)$ for all vector subbundles F of E. So, if $B_D^f \otimes L_{-s}$ satisfies $(\star)$, then $B_D^f \otimes L_{-s}$ is semi-stable, hence so is B_D^f.

DEFINITION. Let D be an effective divisor on X.

(i) For each natural number n, we put

$$[D/n] \stackrel{\mathrm{def}}{=} \sum_{P \in X} [\mathrm{ord}_P(D)/n]P,$$

which is an effective divisor on X.

(ii) For each natural number i, we put

$$D_i \stackrel{\mathrm{def}}{=} \sum_{P \in X} \mathrm{ord}_P(D)P_i,$$

where P_i denotes $F_{X/k}^i(P) \in X_i$. This is an effective divisor on X_i.

(iii) For $n = 0, 1, \ldots, p^f - 1$, let $n = \sum_{j=0}^{f-1} n_j p^j$ be the p-adic expansion with $n_j = 0, \ldots, p-1$. Identifying $\{0, 1, \ldots, f-1\}$ with $\mathbb{Z}/f\mathbb{Z}$ naturally, we put $n^{(i)} \stackrel{\mathrm{def}}{=} \sum_{j=0}^{f-1} n_{i+j} p^j$. Now, assume that D satisfies (TF) with respect to $q = p^f$. Then, we put

$$D^{(i)} \stackrel{\mathrm{def}}{=} \sum_{P \in X} \mathrm{ord}_P(D)^{(i)}P,$$

which is an effective divisor on X.

LEMMA (2.15). *Assume that* $\deg(D) = s(q-1)$ *for some natural number* s *and that* D *satisfies* (TF) *with respect to* $q = p^f$. *Then, if* B_D^f *is semi-stable, we have*

$$\deg(D^{(i)}) \geq \deg(D) \text{ for each } i = 0, 1, \ldots, f-1. \qquad \text{(NSS)}$$

('NSS' means 'necessary condition for semi-stability'.)

PROOF. The vector bundle B_D^f on X_f admits the vector subbundles

$$B_{[D/p^i]_i}^{f-i} \stackrel{\mathrm{def}}{=} ((F_{X_i/k}^{f-i})_*(\mathcal{O}_{X_i}([D/p^i]_i)))/\mathcal{O}_{X_f}$$

for $i = 0, 1, \ldots, f-1$. (Note that $(X_i)_{f-i} = X_f$.) We have

$$\frac{\deg(B^{f-i}_{[D/p^i]_i})}{\mathrm{rk}(B^{f-i}_{[D/p^i]_i})} = \frac{\deg([D/p^i]_i) + (g-1)(p^{f-i}-1)}{p^{f-i}-1}$$
$$= \frac{\deg([D/p^i])}{p^{f-i}-1} + g - 1,$$

so we must have

$$\frac{\deg([D/p^i])}{p^{f-i}-1} \leq \frac{\deg(D)}{p^f-1} \text{ for each } i = 0, 1, \ldots, f-1, \tag{2.16}$$

since B^f_D is assumed to be semi-stable. Now, it is elementary to check that (2.16) is equivalent to (NSS). □

Remark (2.17). We have $\deg(D^{(i)}) \equiv p^{f-i}\deg(D) \equiv 0 \pmod{p^f-1}$. So, if $\deg(D) = p^f - 1$, (NSS) automatically holds. (Of course, by (2.5) and [R1], § 0, we know that B^f_D is then semi-stable.)

Now, we are tempted to ask the following:

Question (2.18). *Let s be a natural number. Let D be an effective divisor of degree $s(q-1)$ on X satisfying* (TF) *and* (NSS), *and let L_{-s} be a line bundle of degree $-s$ on X_f. Then, $B^f_D \otimes L_{-s}$ is a vector bundle on X_f with $\chi = 0$. Does it satisfy* ($\star$)?

However, in general this fails, as the following example shows.

Example (2.19). We assume $p \neq 2$ and let $X = \mathbf{P}^1$. We put $f = 1$ and let $D = \dfrac{p-1}{2}\{(0) + (1) + (\lambda) + (\infty)\}$, where $\lambda \in k - \{0, 1\}$, so that $s = 2$. Then $B^1_D \otimes L_{-2}$ satisfies ($\star$)(if and) only if the elliptic curve $y^2 = x(x-1)(x-\lambda)$ is ordinary. (We omit the proof, which uses some contents of the next section.)

Considering Bouw's work ([B]), we might hope that the following is affirmative.

Question (2.20). *Is* (2.18) *true for U generic (in the moduli space)*?

Finally, the following proposition shows to what extent our results can be applied, in the case where $\#(\mathrm{Supp}(D))$ is small. This analysis is a key to recover 'additive structures' of inertia subgroups of tame fundamental groups in Section 5 (B). Here, for each natural number N, we denote by I_N the set $\{0, 1, \ldots, N-1\}$.

Proposition (2.21). *Let s be a non-negative integer and D an effective divisor of degree $s(p^f-1)$ satisfying* (TF) *with respect to $q = p^f$. We assume that D can be written as $D = n_1P_1 + n_2P_2 + n_3P_3$, where P_1, P_2, P_3 are three distinct points of X. Then*:

(i) *$n_h \in I_{p^f}$ holds for each $h = 1, 2, 3$, and $0 \leq s \leq 3$ holds.*
(ii) *If $s \neq 2$, D satisfies* (2.14).

(iii) *Assume* $s = 2$. *Then,* (NSS) *is equivalent to*

$$n_{1,j} + n_{2,j} + n_{3,j} = 2(p-1) \text{ for each } j = 0, 1, \ldots, f-1,$$

where $n_h = \sum_{j=0}^{f-1} n_{h,j} p^j$ *is the* p*-adic expansion with* $n_{h,j} \in I_p$ $(h = 1, 2, 3)$.

(iv) *Assume* $s = 2$ *and* (NSS).

(iv–a) *If* $n_1 \in p^{I_f} \overset{\text{def}}{=} \{p^b \mid b \in I_f\}$, *then either* $n_2 = p^f - 1$ *or* $n_3 = p^f - 1$ *holds, and* D *satisfies* (2.14).

(iv–b) *If* $n_1 \in I_{p-1} p^{I_f} \overset{\text{def}}{=} \{ap^b \mid a \in I_{p-1}, b \in I_f\}$, *then* D *satisfies* (2.14) *if and only if either* $n_2 = p^f - 1$ *or* $n_3 = p^f - 1$.

(iv–c) *For each*

$$n_1 \notin p^{I_f} \cup I_{p-1} p^{I_f} = \begin{cases} I_{p-1} p^{I_f}, & \text{if } p \neq 2, \\ I_p p^{I_f}, & \text{if } p = 2, \end{cases}$$

there exist $n_2, n_3 \in I_{p^f-1}$ *such that* $D = n_1 P_1 + n_2 P_2 + n_3 P_3$ *satisfies* (2.14).

Proof. (i) The first assertion just says that D is effective and satisfies (TF). The second assertion follows from the first, since $s(q-1) = \deg(D) = n_1 + n_2 + n_3$.

(ii) If $s \leq 1$, (2.14) requires nothing. If $s = 3$, then we must have $n_1 = n_2 = n_3 = q - 1$, which implies (2.14). (Take $k = 0$, $f = f_0$, and $D = D_0$.)

(iii) (NSS) is equivalent to saying that

$$n_1^{(j)} + n_2^{(j)} + n_3^{(j)} \geq n_1 + n_2 + n_3 = 2(p^f - 1)$$

holds for $j = 0, 1, \ldots, f-1$. Here, by definition, the left-hand side is congruent to the right-hand side modulo $p^f - 1$, hence it is a multiple of $p^f - 1$. On the other hand, it is less than or equal to $3(p^f - 1)$. Moreover, if it is equal to $3(p^f - 1)$, each of $n_1^{(j)}, n_2^{(j)}, n_3^{(j)}$ must be $p^f - 1$, which implies that each of n_1, n_2, n_3 is $p^f - 1$. This contradicts the assumption $n_1 + n_2 + n_3 = 2(p^f - 1)$. Thus (NSS) turns out to be equivalent to saying that

$$n_1^{(j)} + n_2^{(j)} + n_3^{(j)} (= n_1 + n_2 + n_3) = 2(p^f - 1)$$

holds for $j = 0, 1, \ldots, f-1$. Now, put $\nu \overset{\text{def}}{=} n_1 + n_2 + n_3 = 2(p^f - 1)$ and $\nu_j \overset{\text{def}}{=} n_{1,j} + n_{2,j} + n_{3,j}$. Since we have

$$n_h^{(j+1)} = \frac{n_h^{(j)} - n_{h,j}}{p} + n_{h,j} p^{f-1} = \frac{1}{p} n_h^{(j)} + \frac{p^f - 1}{p} n_{h,j},$$

we see that

$$\nu = \frac{1}{p} \nu + \frac{p^f - 1}{p} \nu_j, \text{ i.e., } \nu_j = 2(p-1)$$

is a necessary condition for (NSS). It is clear that this condition is also sufficient for (NSS).

(iv–a) If $n_1 = p^b$ ($b \in I_f$), we must have

$$n_{2,j} + n_{3,j} = \begin{cases} 2(p-1), & \text{if } j \neq b, \\ 2(p-1)-1, & \text{if } j = b, \end{cases}$$

by (iii), or, equivalently,

$$(n_{2,j}, n_{3,j}) = \begin{cases} (p-1, p-1), & \text{if } j \neq b, \\ (p-1, p-2) \text{ or } (p-2, p-1), & \text{if } j = b. \end{cases}$$

From this (iv–a) follows.

(iv–b) If $n_1 = ap^b$ ($a \in I_{p-1}, b \in I_f$), we have $n_{1,j} = 0$ (resp. a) for $j \neq b$ (resp. $j = b$). Accordingly, by (iii), we must have $n_{2,j} = n_{3,j} = p-1$ for $j \neq b$ and $n_{2,b} + n_{3,b} = 2(p-1) - a$. First, if either n_2 or n_3 coincides with $p^f - 1$, then it is clear that D satisfies (2.14) for $k = 0$. Conversely, suppose that there exist k, f_i and D_i as in (2.14). Since $\deg(D_i) = 2(p^{f_i} - 1)$ and $\mathrm{ord}_P(D_i) = p^{f_i} - 1$ for some $P = P_1, P_2, P_3$, we have $\mathrm{ord}_P(D_i) \leq p^{f_i} - 1$ for all $P = P_1, P_2, P_3$. From this, (considering the p-adic expansion of $n_h = \mathrm{ord}_{P_h}(D)$) we conclude that $\mathrm{ord}_{P_h}(D_i)$ should coincide with $\sum_{j=0}^{f_i - 1} n_{h, f_{>i}+j} p^j$ for each $h = 1, 2, 3$. Thus, for some $h = 1, 2, 3$ (depending on i), we must have $n_{h, f_{>i}+j} = p-1$ for $j = 0, \ldots, f_i - 1$. Now, taking the unique i such that $f_{>i} \leq b < f_{>i-1}$, we see that $n_{h,b} = p-1$ holds for some h. Since $n_{1,b} = a < p-1$, we must have either $n_{2,b} = p-1$ or $n_{3,b} = p-1$, which implies $n_2 = p^f - 1$ or $n_3 = p^f - 1$, respectively. This completes the proof of (iv–b).

(iv–c) Assume $n_1 \notin p^{I_f} \cup I_{p-1} p^{I_f}$. In particular, $n_1 \neq 0$, hence there exists $b = 0, 1, \ldots, f-1$ with $n_{1,b} > 0$. Now, we put

$$(n_{2,j}, n_{3,j}) \stackrel{\text{def}}{=} \begin{cases} (p-1, p-1-n_{1,j}), & \text{if } j \neq b, \\ (p-1-n_{1,b}, p-1), & \text{if } j = b \text{ and } n_{1,b} < p-1, \\ (p-2, 1), & \text{if } j = b \text{ and } n_{1,b} = p-1. \end{cases}$$

(Note that (NSS) holds by (iii).) Since $p - 1 \in \{n_{1,j}, n_{2,j}, n_{3,j}\}$ for each $j = 0, 1, \ldots, f-1$, we see that D satisfies (2.14). Finally, since $n_{2,b} < p-1$ by definition, we have $n_2 < p^f - 1$. On the other hand, suppose $n_3 = p^f - 1$. Then we must have $p - 1 - n_{1,j} = p-1$ for $j \neq b$, and $1 = p-1$ if $n_{1,b} = p-1$. Namely, we have $n_1 = n_{1,b} p^b$ and either $p = 2$ or $n_{1,b} < p-1$. This contradicts the assumption $n_1 \notin p^{I_f} \cup I_{p-1} p^{I_f}$. This completes the proof of (iv–c). □

3. The p-Ranks of p'-Cyclic Ramified Coverings

As in Section 2, let k be an algebraically closed field of characteristic $p > 0$ and X a proper, smooth, connected curve of genus g over k. Let S be a finite (possibly empty) set of closed points of X and denote by n the cardinality of S. We put $U = X - S$. In this section, we investigate the p-ranks of the Jacobian varieties of p'-cyclic coverings of X, étale over U and possibly ramified over S.

Cyclic coverings and generalized Hasse–Witt invariants. Let N be a natural number prime to p. We consider the elements of the étale cohomology group $H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$, where $\boldsymbol{\mu}_N = \boldsymbol{\mu}_N(k)$ is the group of N-th roots of unity. In terms of fundamental groups,

$$H^1_{\text{ét}}(U, \boldsymbol{\mu}_N) = \mathrm{Hom}(\pi_1(U), \boldsymbol{\mu}_N) = \mathrm{Hom}(\pi_1^{\mathrm{t}}(U), \boldsymbol{\mu}_N),$$

and, in terms of torsors, $H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$ can be identified with the set of isomorphism classes of (étale) $\boldsymbol{\mu}_N$-torsors of U. We shall consider the p-ranks for such $\boldsymbol{\mu}_N$-torsors, or $\boldsymbol{\mu}_N$-coverings.

Let V be a $\boldsymbol{\mu}_N$-torsor of U and $[V]$ the corresponding element of $H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$. Let Y be the normalization of X in V, to which the $\boldsymbol{\mu}_N$-action on V extends uniquely. We define the p-rank (or the Hasse–Witt invariant) $\gamma_{[V]}$ to be the dimension of the $\mathbb{F}_p$-vector space $H^1_{\text{ét}}(Y, \mathbb{F}_p)$.

To obtain finer invariants, we consider the following canonical decomposition of the group algebra $k[\boldsymbol{\mu}_N]$:

$$\begin{array}{ccc} k[\boldsymbol{\mu}_N] & \xrightarrow{\sim} & \displaystyle\prod_{i \in \mathbb{Z}/N\mathbb{Z}} k, \\ \cup & & \\ \boldsymbol{\mu}_N & & \cup \\ \cup & & \\ \zeta & \mapsto & (\zeta^i)_{i \in \mathbb{Z}/N\mathbb{Z}}. \end{array} \tag{3.1}$$

Corresponding to this decomposition, each $k[\boldsymbol{\mu}_N]$-module M admits a canonical decomposition $M = \bigoplus_{i \in \mathbb{Z}/N\mathbb{Z}} M_i$, where $\zeta \in \boldsymbol{\mu}_N$ acts on M_i as the ζ^i-multiplication. We shall denote by $\gamma_i(M)$ the dimension of the k-vector space M_i. Moreover, for an $\mathbb{F}_p[\boldsymbol{\mu}_N]$-module M, we shall write $\gamma_i(M)$ instead of $\gamma_i(M \otimes_{\mathbb{F}_p} k)$. In the latter case, $\gamma_{p^a i}(M) = \gamma_i(M)$ holds for each integer a. (Observe that the p-th power map of k maps $(M \otimes k)_i$ isomorphically onto $(M \otimes k)_{pi}$.)

Now, since $\boldsymbol{\mu}_N$ naturally acts on the $\mathbb{F}_p$-vector space $H^1_{\text{ét}}(Y, \mathbb{F}_p)$, we can define as follows:

Definition. $\gamma_{[V],i} \overset{\text{def}}{=} \gamma_i(H^1_{\text{ét}}(Y, \mathbb{F}_p))$.

These invariants essentially coincide with the so-called generalized Hasse–Witt invariants (see [Ka], [Na], and [B]). Of course, we have

$$\gamma_{[V]} = \sum_{i \in \mathbb{Z}/N\mathbb{Z}} \gamma_{[V],i}.$$

We shall present another description of these invariants, which is also well-known. Let ψ denote the structure morphism $Y \to X$. Corresponding to the decomposition (3.1), we obtain a decomposition of the sheaf $\psi_*(\mathcal{O}_Y)$ on X:

$$\psi_*(\mathcal{O}_Y) = \bigoplus_{i \in \mathbb{Z}/N\mathbb{Z}} L_i. \tag{3.2}$$

Let f be the order of $p \bmod N$ in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$. The p-th power map of $\mathcal{O}_Y$ sends L_i into L_{pi}, hence the p^f-th power map of $\mathcal{O}_Y$ sends L_i into itself, which induces a p^f-linear map

$$\varphi_{[V],i} : H^1(X, L_i) \to H^1(X, L_i)$$

on the Zariski cohomology group $H^1(X, L_i)$. We denote by $\gamma'_{[V],i}$ the dimension of the k-vector space $\bigcap_{r\geq 1} \mathrm{Im}((\varphi_{[V],i})^r)$. Then, Artin–Schreier theory, together with the well-known properties of p^f-linear maps, implies $\gamma'_{[V],i} = \gamma_{[V],i}$

Cyclic coverings and line bundles. Next, in order to apply the results of Section 2, we shall give a description of $\boldsymbol{\mu}_N$-torsors of U in terms of line bundles and divisors on X, which is essentially widely known (possibly in slightly different forms).

We denote by $\mathrm{Pic}(X)$ the Picard group of X and by $\mathbb{Z}[S]$ the group of divisors whose supports are contained in S, which can be identified with the free $\mathbb{Z}$-module with basis S. We denote by $\mathbb{Z}/N\mathbb{Z}[S]$ the free $\mathbb{Z}/N\mathbb{Z}$-module with basis S, hence $\mathbb{Z}/N\mathbb{Z}[S] = \mathbb{Z}[S]/N\mathbb{Z}[S]$. Let $(\mathbb{Z}/N\mathbb{Z})^\sim$ denote the set $\{0, 1, \ldots, N-1\}$, and $(\mathbb{Z}/N\mathbb{Z})^\sim[S]$ the subset of $\mathbb{Z}[S]$ consisting of the elements whose 'coefficients' are contained in $(\mathbb{Z}/N\mathbb{Z})^\sim$.

Consider the following (short) complex of abelian groups:

$$\mathbb{Z}[S] \stackrel{\alpha_N}{\to} \mathrm{Pic}(X) \oplus \mathbb{Z}[S] \stackrel{\beta_N}{\to} \mathrm{Pic}(X), \tag{3.3}$$

where $\alpha_N(D) = ([\mathcal{O}_X(-D)], ND)$ and $\beta_N(([L], D)) = [L^{\otimes N} \otimes \mathcal{O}_X(D)]$.

Definition. We define the abelian group $P_N = P_N(X, S)$ to be the homology group $\mathrm{Ker}(\beta_N)/\mathrm{Im}(\alpha_N)$ of the complex (3.3).

We can easily see that the following exact sequence exists:

$$0 \to \mathrm{Pic}(X)[N] \stackrel{a_N}{\to} P_N \stackrel{b_N}{\to} \mathbb{Z}/N\mathbb{Z}[S] \stackrel{c_N}{\to} \mathbb{Z}/N\mathbb{Z}, \tag{3.4}$$

where $[N]$ means the N-torsion subgroup, and

$$a_N([L]) = ([L], 0) \bmod \mathrm{Im}(\alpha_N),$$

$$b_N(([L], D) \bmod \mathrm{Im}(\alpha_N)) = D \bmod N,$$

$$c_N(D \bmod N) = \deg(D) \bmod N.$$

From this, P_N turns out to be isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2g+n-1+b^{(2)}}$, where

$$b^{(2)} \stackrel{\mathrm{def}}{=} \begin{cases} 1, & \text{if } n = 0, \\ 0, & \text{if } n > 0, \end{cases}$$

is the second Betti number of U.

We shall define two maps

$$i_N : P_N \to H^1_{\text{ét}}(U, \boldsymbol{\mu}_N), \ j_N : H^1_{\text{ét}}(U, \boldsymbol{\mu}_N) \to P_N.$$

To do this, we need some more notations. First, we denote by $\mathbb{Z}/N\mathbb{Z}[S]^0$ the kernel of c_N in (3.4) and by $(\mathbb{Z}/N\mathbb{Z})^\sim[S]^0$ the subset of $(\mathbb{Z}/N\mathbb{Z})^\sim[S]$ corresponding to $\mathbb{Z}/N\mathbb{Z}[S]^0$ under the natural bijection $(\mathbb{Z}/N\mathbb{Z})^\sim[S] \tilde{\to} \mathbb{Z}/N\mathbb{Z}[S]$. We define $\tilde{P}_N$ to be the inverse image of $(\mathbb{Z}/N\mathbb{Z})^\sim[S]^0$ under the projection $\mathrm{Ker}(\beta_N) \to \mathbb{Z}[S]$ (see (3.3)). Then we can easily see that the modulo-$\mathrm{Im}(\alpha_N)$ map $\tilde{P}_N \to P_N$ is a bijection. We denote by $\tilde{b}_N$ the projection $\tilde{P}_N \to (\mathbb{Z}/N\mathbb{Z})^\sim[S]^0$.

Now, first, take $([L], D)$ in $\tilde{P}_N$. We have $L^{\otimes N} \otimes \mathcal{O}_X(D) \simeq \mathcal{O}_X$, or, equivalently, $L^{\otimes N} \simeq \mathcal{O}_X(-D)$. These isomorphisms are unique up to multiplication by an element of $k^\times$. We fix such an isomorphism $L^{\otimes N} \tilde{\to} \mathcal{O}_X(-D)$, which induces an isomorphism $(L|_U)^{\otimes N} \tilde{\to} \mathcal{O}_X(-D)|_U = \mathcal{O}_U$. Then, by using this isomorphism, we can equip the locally free $\mathcal{O}_U$-module $\bigoplus_{i \in (\mathbb{Z}/N\mathbb{Z})^\sim} (L|_U)^{\otimes i}$ with a structure of étale $\mathcal{O}_U$-algebra, as usual. This $\mathcal{O}_U$-algebra admits a $\boldsymbol{\mu}_N$-action: $\zeta \in \boldsymbol{\mu}_N$ acts on $(L|_U)^{\otimes i}$ as the ζ^i-multiplication. The finite U-scheme corresponding to this $\mathcal{O}_U$-algebra, together with this $\boldsymbol{\mu}_N$-action, defines an étale $\boldsymbol{\mu}_N$-torsor of U. It is easy to check (by using the surjectivity of the N-th power map $k^\times \to k^\times$) that the isomorphism class of the $\boldsymbol{\mu}_N$-torsor we have just constructed is independent of the choice of the isomorphism $L^{\otimes N} \tilde{\to} \mathcal{O}_X(-D)$. This gives the definition of a map $\tilde{\imath}_N : \tilde{P}_N \to H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$. Composing this with the canonical bijection $P_N \tilde{\leftarrow} \tilde{P}_N$, we obtain $i_N : P_N \to H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$.

Next, take a $\boldsymbol{\mu}_N$-torsor V/U, and let $\psi : Y \to X$ be the normalization of $V \to U$, as above. Then, as we have seen, the locally free $\mathcal{O}_X$-module $\psi_*(\mathcal{O}_Y)$ can be canonically decomposed as a direct sum $\bigoplus_{i \in \mathbb{Z}/N\mathbb{Z}} L_i$. Using the fact that V is a $\boldsymbol{\mu}_N$-torsor of U, we can see that each L_i is a line bundle on X and that $L_0 = \mathcal{O}_X$. Since $\boldsymbol{\mu}_N$ acts on $\psi_*(\mathcal{O}_Y)$ as an $\mathcal{O}_X$-algebra, the multiplication of L_i and $L_{i'}$ is contained in $L_{i+i'}$. In particular, we are given an $\mathcal{O}_X$-linear map $L_1^{\otimes N} \to L_0 = \mathcal{O}_X$. Since V is a $\boldsymbol{\mu}_N$-torsor of U, the restriction $(L_1|_U)^{\otimes N} \to \mathcal{O}_U$ is an isomorphism. Therefore the map $L_1^{\otimes N} \to \mathcal{O}_X$ is injective, and it factors as $L_1^{\otimes N} \tilde{\to} \mathcal{O}_X(-D) \subset \mathcal{O}_X$ for some (uniquely determined) effective divisor $D \in \mathbb{Z}[S]$. We claim that the effective divisor D belongs to $(\mathbb{Z}/N\mathbb{Z})^\sim[S]$. This comes from the fact that Y is the normalization of X. In fact, the N-th power of a (local) section of $L_1([D/N])$ belongs to $\mathcal{O}_X(N[D/N] - D) \subset \mathcal{O}_X$, hence should belong to $\psi_*(\mathcal{O}_Y)$. (See Section 2 for the definition of the divisor $[D/N]$.) Considering the $\boldsymbol{\mu}_N$-action, we have $L_1([D/N]) \subset L_1$, which implies $[D/N] = 0$, or, equivalently, $D \in (\mathbb{Z}/N\mathbb{Z})^\sim[S]$. Now, since $([L_1], D)$ falls in the kernel of β_N by definition, $([L_1], D)$ is an element of $\tilde{P}_N$. This gives the definition of a map $\tilde{\jmath}_N : H^1_{\text{ét}}(U, \boldsymbol{\mu}_N) \to \tilde{P}_N$. Composing this with the canonical bijection $\tilde{P}_N \tilde{\to} P_N$, we obtain $j_N : H^1_{\text{ét}}(U, \boldsymbol{\mu}_N) \to P_N$.

PROPOSITION (3.5). *The canonical maps i_N, j_N are group isomorphisms, which are inverse to each other.*

PROOF. By the definition of multiplication of two torsors, we see that i_N is a group homomorphism. (See, for example, [Mi1], III, Remark 4.8(b).)

In the above construction concerning j_N, the canonical map $L_1^{\otimes i} \to L_i$ ($i \in (\mathbb{Z}/N\mathbb{Z})^\sim$) becomes an isomorphism after restricting to U: $(L_1|_U)^{\otimes i} \xrightarrow{\sim} L_i|_U$, since V is a $\boldsymbol{\mu}_N$-torsor of U. Using this fact, we can check that $i_N \circ j_N = \mathrm{id}$.

Finally, for $([L], D) \in \tilde{P}_N$, let V be the corresponding $\boldsymbol{\mu}_N$-torsor of U, and $\psi : Y \to X$ its normalization. Then, since the N-th power of each (local) section of L belongs to $\mathcal{O}_X(-D) \subset \mathcal{O}_X$, $\psi_*(\mathcal{O}_Y)$ should contain L, by the definition of normalization. Moreover, observing the $\boldsymbol{\mu}_N$-action, we can conclude that L should be contained in $L_1 \subset \psi_*(\mathcal{O}_Y)$. Now, the N-th power map induces a commutative diagram

$$\begin{array}{ccc} L^{\otimes N} & \xrightarrow{\sim} & \mathcal{O}_X(-D) \\ \cap & & \cap \\ L_1^{\otimes N} & \to & \mathcal{O}_X. \end{array}$$

Since $D \in (\mathbb{Z}/N\mathbb{Z})^\sim[S]$, this implies that $L = L_1$, hence that $\tilde{j}_N \circ \tilde{i}_N = \mathrm{id}$, or, equivalently $j_N \circ i_N = \mathrm{id}$. From this j_N is also a group isomorphism. (To prove $j_N \circ i_N = \mathrm{id}$, we may also resort to the fact $\#(P_N) = \#(H^1_{\text{ét}}(U, \boldsymbol{\mu}_N))$, which equals $N^{2g+n-1+b^{(2)}}$. $\square$

Generalized Hasse–Witt invariants via line bundles. Now, we can describe the "generalized Hasse–Witt invariants" in terms of P_N, as follows. For an element $([L], D)$ of $\tilde{P}_N$, fix an isomorphism $L^{\otimes N} \xrightarrow{\sim} \mathcal{O}_X(-D)$ (unique up to $k^\times$-multiplication). Taking the composite of the p^f-th power map $L \to L^{\otimes p^f}$ and

$$L^{\otimes p^f} = L \otimes L^{\otimes (p^f - 1)} \xrightarrow{\sim} L \otimes \mathcal{O}_X\left(-\frac{p^f - 1}{N} D\right) \hookrightarrow L,$$

we get a map $L \to L$, which induces a p^f-linear map

$$\varphi_{([L],D)} : H^1(X, L) \to H^1(X, L).$$

We denote by $\gamma_{([L],D)}$ the dimension of the k-vector space $\bigcap_{r \geq 1} \mathrm{Im}((\varphi_{([L],D)})^r)$. Then, by the various definitions, we see

$$\gamma_{([L],D)} = \gamma_{[V],1}, \tag{3.6}$$

where $[V] = \tilde{\imath}_N(([L], D))$.

Remark (3.7). By the Riemann–Roch theorem, we have

$$\begin{aligned} \dim_k(H^1(X, L)) &= g - 1 - \deg(L) + \dim_k(H^0(X, L)) \\ &= g - 1 + \frac{1}{N} \deg(D) + \dim_k(H^0(X, L)) \\ &\leq g - 1 + \left[\frac{n(N-1)}{N}\right] + \dim_k(H^0(X, L)) \\ &= g + n - 1 + \left[-\frac{n}{N}\right] + \dim_k(H^0(X, L)). \end{aligned}$$

From this, we obtain the following rough estimate:

$$\gamma_{([L],D)} \leq \begin{cases} g, & \text{if } ([L],D) = ([\mathcal{O}_X],0), \\ g+n-2+b^{(2)}, & \text{otherwise.} \end{cases}$$

More generally, we can describe $\gamma_{[V],i}$ in terms of line bundles and divisors. First, we shall determine the $\mathbb{Z}$-action on $\tilde{P}_N$ induced by the natural $\mathbb{Z}$-action on the abelian group P_N. In P_N, i times $([L],D)$ is $([L^{\otimes i}],iD)$ (mod $\mathrm{Im}(\alpha_N)$) for each $i \in \mathbb{Z}$. Since the element of $(\mathbb{Z}/N\mathbb{Z})^{\sim}[S]$ that is equivalent to iD modulo N is $iD - N[iD/N]$, we can see that the i-action on $\tilde{P}_N$ is given by

$$([L],D) \mapsto (L^{\otimes i}([iD/N]), iD - N[iD/N]).$$

We shall denote $L^{\otimes i}([iD/N])$ and $iD - N[iD/N]$ by $L(i)$ and $D(i)$, respectively.

Now, let V be the $\boldsymbol{\mu}_N$-torsor of U corresponding to $([L],D)$. Then we have the following generalization of (3.6):

Claim (3.8). $\gamma_{([L(i)],D(i))} = \gamma_{[V],i}$.

In fact, consider the decomposition (3.2). By the definition of i_N, Y is the normalization of X in the finite X-scheme corresponding to the $\mathcal{O}_X$-algebra $\bigoplus_{i\in(\mathbb{Z}/N\mathbb{Z})^{\sim}} L^{\otimes i}$, hence we have the canonical injection $L^{\otimes i} \hookrightarrow L_i$, for each $i \in (\mathbb{Z}/N\mathbb{Z})^{\sim}$. We have more: $L(i) = L^{\otimes i}([iD/N]) \hookrightarrow L_i$, since the N-th power of a (local) section of $L^{\otimes i}([iD/N])$ is contained in $\mathcal{O}_X(N[iD/N] - iD) = \mathcal{O}_X(-D(i)) \subset \mathcal{O}_X$. (Note that Y is normal.) In fact, we have $L(i) = L_i$. Otherwise, L_i would be strictly bigger than $L(i)$, hence we could find a (local) section of L_i whose N-th power would not belong to $\mathcal{O}_X$. This is absurd. Thus, we can identify $\varphi_{([L(i)],D(i))}$ with $\varphi_{[V],i}$, which implies our claim.

Digression: Torsion points on divisors of abelian varieties. As in [R1], we need some inputs from intersection theory to deduce our main (numerical) results concerning p-ranks of cyclic coverings from the results of Section 2.

Lemma (3.9). *Let A be an abelian variety of dimension $d > 0$ over an algebraically closed field k, and D an effective divisor on A. For each natural number N not divisible by* $\mathrm{char}(k)$, *we put*

$$c^{\mathrm{fin}}(D,N) = \min\{(D\ .\ C)\ |C\text{: } \textit{irreducible, reduced curve in } A, \\ \textit{such that } C \ni 0 \textit{ and } D \cap N_A^{-1}(C) \textit{ is finite.}\}$$

and

$$c^{\mathrm{irr}}(D,N) = \min\{(D\ .\ C)\ |C\text{: } \textit{irreducible, reduced curve in } A, \\ \textit{such that } C \ni 0 \textit{ and } N_A^{-1}(C) \textit{ is irreducible.}\}$$

Then:

(i) *For each irreducible, smooth curve C in A such that $\pi_1(C)$ surjects onto $\pi_1(A)$, we have $c^{\mathrm{irr}}(D,N) \leq (D\ .\ C)$.*

(ii) *For each very ample divisor H on A, we have $c^{\mathrm{fin}}(D,N) \leq (D \,.\, H^{d-1})$, where H^r denotes the r-th self-intersection product $\underbrace{H \,.\, \ldots \,.\, H}_{r\,\mathrm{times}}$.*

(iii) *We have $\#(\mathrm{Supp}(D) \cap A[N]) \leq c^{\mathrm{fin}}(D,N)N^{2d-2}$.*

(iv) *If $c^{\mathrm{fin}}(D,N) < N^2$, then we have $c^{\mathrm{fin}}(D,N) \leq c^{\mathrm{irr}}(D,N)$.*

Proof. (See [R1], Lemme 4.3.5 and the proof of [R1], Théorème 4.3.1.)

(i) The condition $\pi_1(C) \twoheadrightarrow \pi_1(A)$ and the number $(D \,.\, C)$ do not change if C is translated by an element of A. So, we may assume that C passes through 0. Now, since $\pi_1(C) \twoheadrightarrow \pi_1(A)$, $N_A^{-1}(C)$ must be irreducible. Thus the inequality holds.

(ii) Since H is very ample, a general member C_1 of H^{d-1} that passes through 0 has finite intersection with $N_A(D)$, hence $D \cap N_A^{-1}(C_1)$ is also finite. Let C be an irreducible component of C_1 that passes through 0. Then, regarding C as a reduced scheme, we obtain

$$c^{\mathrm{fin}}(D,N) \leq (D \,.\, C) \leq (D \,.\, C_1) = (D \,.\, H^{d-1}).$$

(iii) Take an irreducible, reduced curve C in A with $(D \,.\, C) = c^{\mathrm{fin}}(D,N)$ such that $C \ni 0$ and that $N_A^{-1}(C) \cap D$ is finite. Then we have

$$\#(\mathrm{Supp}(D) \cap A[N]) \leq (D \,.\, N_A^{-1}(C)) = N^{2d-2}(D \,.\, C) = c^{\mathrm{fin}}(D,N)N^{2d-2}.$$

Here, The inequality follows from the fact that $C \ni 0$ and that $N_A^{-1}(C) \cap D$ is finite, and the first equality follows from intersection theory as in the proof of [R1], Lemme 4.3.5.

(iv) Take an irreducible, reduced curve C in A with $(D \,.\, C) = c^{\mathrm{irr}}(D,N)$ such that $C \ni 0$ and that $N_A^{-1}(C)$ is irreducible. By (iii) and the assumption $c^{\mathrm{fin}}(D,N) < N^2$, we have $\#(\mathrm{Supp}(D) \cap A[N]) < N^{2d}$, hence $A[N] \not\subset D$, and, a fortiori, $N_A^{-1}(C) \not\subset D$. Since $N_A^{-1}(C)$ is irreducible by assumption, this implies that $D \cap N_A^{-1}(C)$ is finite. Thus we have $c^{\mathrm{fin}}(D,N) \leq (D \,.\, C) = c^{\mathrm{irr}}(D,N)$. □

Corollary (3.10). *Let X be a proper, smooth, connected curve of genus g over k and J the Jacobian variety of X. Let E be a vector bundle on X with $\chi(E) = 0$, and assume that E satisfies ($\star$) of page 59. Then, Θ_E is a divisor on J, and:*

(i) *If $g > 0$, we have $c^{\mathrm{irr}}(\Theta_E,N) \leq g\,\mathrm{rk}(E)$.*

(ii) *If $g > 0$, we have $c^{\mathrm{fin}}(\Theta_E,N) \leq 3^{g-1}g!\,\mathrm{rk}(E)$.*

(iii) *We have $\#(\mathrm{Supp}(\Theta_E) \cap J[N]) \leq 3^{g-1}g!\,\mathrm{rk}(E)N^{2g-2}$.*

(iv) *If $3^{g-1}g!\,\mathrm{rk}(E) < N^2$, we have $\#(\mathrm{Supp}(\Theta_E) \cap J[N]) \leq g\,\mathrm{rk}(E)N^{2g-2}$.*

Proof. First, we note that, by [R1], Proposition 1.8.1 (2), Θ_E is algebraically equivalent to $\mathrm{rk}(E)\Theta$, where Θ is the classical theta divisor (the image of $X^{(g-1)}$ in J).

(i) This is obtained by applying (3.9)(i) to $C = X$, which is embedded into $A = J$ by means of an Albanese morphism. In fact, then $\pi_1(X) \twoheadrightarrow \pi_1(J)$ is well-known, and we have

$$(\Theta_E \,.\, X) = \mathrm{rk}(E)(\Theta \,.\, X) = \mathrm{rk}(E)g.$$

(ii) We first note that 3Θ is very ample by [Mu], Section 17, Theorem, since Θ is ample. Now, (ii) is obtained by applying (3.9)(ii) to $H = 3\Theta$. In fact, then we have

$$(\Theta_E \,.\, (3\Theta)^{g-1}) = \mathrm{rk}(E)3^{g-1}(\Theta^g) = \mathrm{rk}(E)3^{g-1}g!.$$

(iii) We may assume $g > 0$, since $\Theta_E = \varnothing$ for $g = 0$. Then, (iii) follows from (ii) and (3.9)(iii).

(iv) We may assume $g > 0$, as in (iii). Then, (iv) follows from (i), (ii) and (3.9)(iii)(iv). □

Remark (3.11). In [R1], Lemme 4.3.5, it was necessary to assume that $D \cap l_A^{-1}(C)$ is finite. (Counterexample: C: a one-dimensional abelian subvariety of A, D: the inverse image in A of a divisor of A/C that contains the whole $(A/C)[l]$.) Accordingly, in Théorème 4.3.1, loc. cit., the condition $l + 1 \geq (p-1)g$ had to be modified. (For example, $l + 1 \geq (p-1)3^{g-1}g!$ is sufficient.) Similarly, in [T1], Lemma (1.9), the condition $l^m > \frac{l^{2g}-l^{2g-1}}{l^{2g}-1}(p-1)g$ had to be modified as $l^m > \frac{l^{2g}-l^{2g-1}}{l^{2g}-1}(p-1)3^{g-1}g!$, and, in its proof, we should have assumed that $D \cap (l_A^m)^{-1}(C)$ is finite.

Main numerical consequences. Until the end of this section, with the exception of (3.17), we restrict ourselves to the case that $N = q - 1$, where q is a (positive) power of p. (Note that, in this case, we have $p^f = q$.) Then, we get some numerical consequences of the results of Section 2, as follows.

We note that, for each element D of $(\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0$, $\deg(D) = s(D)N$ for some integer $s(D)$ with $0 \leq s(D) \leq n - 1 + b^{(2)}$, and that the cardinality of $\tilde{b}_N^{-1}(D)$ is N^{2g}.

Theorem (3.12). *Put*

$$C(g) \overset{\text{def}}{=} \begin{cases} 0, & \text{if } g = 0, \\ 3^{g-1}g!, & \text{if } g > 0. \end{cases} \tag{3.13}$$

Then, for each $D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0$ with $s(D) \leq 1$, the following statements hold.

(i) *We have*

$$\#\{[L] \in \mathrm{Pic}(X) \mid ([L], D) \in \tilde{P}_N \text{ and } \varphi_{([L],D)} \text{ is bijective}\} \geq N^{2g} - C(g)N^{2g-1}.$$

(ii) *We have*

$$\#\{[L] \in \mathrm{Pic}(X) \mid ([L], D) \in \tilde{P}_N \text{ and } \gamma_{([L],D)} \geq g - 1 + s(D)\} \geq N^{2g} - C(g)N^{2g-1}$$

and

$$\#\{[L] \in \mathrm{Pic}(X) \mid ([L], D) \in \tilde{P}_N \text{ and } \gamma_{([L],D)} = g - 1 + s(D)\} \geq \begin{cases} N^{2g} - C(g)N^{2g-1} - 1, & \text{if } s(D) = 0, \\ N^{2g} - C(g)N^{2g-1}, & \text{if } s(D) = 1. \end{cases}$$

Proof. For simplicity, we shall write s instead of $s(D)$. Since the degree of $L \in \tilde{b}_N^{-1}(D)$ is $-s$, we see that

$$\gamma_{([L],D)} \leq \dim_k(H^1(X, L)) = \begin{cases} g, & \text{if } s = 0 \text{ and } L \simeq \mathcal{O}_X, \\ g - 1 + s, & \text{otherwise,} \end{cases} \tag{3.14}$$

as in (3.7). In particular, the statements clearly hold for $g = 0$. From now on, we shall assume $g > 0$.

(i) First, recall the following commutative diagram (see Section 2):

$$\begin{array}{ccc} X & = & X \\ F^f_{X/k} \downarrow & \circlearrowleft & \downarrow F^f_X \\ X_f & \stackrel{\sim}{\to} & X \\ \downarrow & \underset{(F_{\mathrm{Spec}(k)})^f}{\square} & \downarrow \\ \mathrm{Spec}(k) & \stackrel{\sim}{\to} & \mathrm{Spec}(k). \end{array}$$

We shall denote by ι the q-linear isomorphism $X_f \stackrel{\sim}{\to} X$ in this diagram. Note that the pullback by F^f_X of a line bundle L on X is canonically isomorphic to $L^{\otimes q}$. In fact, we can easily check that the $\mathcal{O}_X$-linear map $(F^f_X)^*(L) \to L^{\otimes q}$ induced by the q-th power map $L \to L^{\otimes q}$ is an isomorphism.

Take any $[L'_{-s}] \in \tilde{b}_N^{-1}(D)$. Then we have

$$(L'_{-s})^{\otimes N} \simeq \mathcal{O}_X(-D) \text{ (hence } \deg(L'_{-s}) = -s)$$

and

$$\tilde{b}_N^{-1}(D) = \{[L' \otimes L'_{-s}] \mid [L'] \in \mathrm{Pic}(X)[N]\}. \tag{3.15}$$

We put $L_{-s} \stackrel{\mathrm{def}}{=} \iota^*(L'_{-s})$. Then we have $\deg(L_{-s}) = -s$ and

$$(F^f_{X/k})^*(L_{-s}) = (L'_{-s})^{\otimes q} \simeq \mathcal{O}_X(-D) \otimes L'_{-s}.$$

Now, by (2.6), the vector bundle $E \stackrel{\mathrm{def}}{=} B^f_D \otimes L_{-s}$ on X_f satisfies condition ($\star$) of page 59. So, applying (3.10), we get

$$\#\{[L] \in \mathrm{Pic}(X_f)[N] \mid h^0(E \otimes L) = h^1(E \otimes L) = 0\} \geq N^{2g} - C(g)N^{2g-1}.$$

By the definition of B^f_D, the condition

$$h^0(E \otimes L) = h^1(E \otimes L) = 0$$

implies

$$\begin{array}{rcl} H^1(X_f, L_{-s} \otimes L) & \xrightarrow{\sim} & H^1(X_f, (F^f_{X/k})_*(\mathcal{O}_X(D)) \otimes L_{-s} \otimes L) \\ & & \| \\ & & H^1(X, \mathcal{O}_X(D) \otimes (F^f_{X/k})^*(L_{-s} \otimes L)). \end{array}$$

In terms of $L' = \iota_*(L)$ (hence $L = \iota^*(L')$), this is equivalent to:

$$H^1(X, L'_{-s} \otimes L') \xrightarrow{\sim} H^1(X, \mathcal{O}_X(D) \otimes (L'_{-s} \otimes L')^{\otimes q}).$$

Considering (3.15), these imply the inequality in (i).

(ii) Immediate from (i) and (3.14). (The term -1 in the case $s = 0$ comes from the trivial line bundle.) □

We have the following slight generalization of (3.12). See Section 2 for the definition of the divisor $D^{(i)}$.

COROLLARY (3.16). *Let $N = p^f - 1$ and $D \in (\mathbb{Z}/N\mathbb{Z})^\sim[S]^0$. Assume that there exists $i \in \{0, 1, \ldots, f-1\}$ such that $s(D^{(i)}) = 1$. Then we have*

$$\#\{[L] \in \mathrm{Pic}(X) \mid ([L], D) \in \tilde{P}_N \text{ and } \gamma_{([L],D)} = g\} \geq N^{2g} - C(g)N^{2g-1}.$$

PROOF. Notations being as in (3.8), we can deduce

$$\gamma_{([L(p^i)],D(p^i))} = \gamma_{[V],p^i} = \gamma_{[V],1} = \gamma_{([L],D)},$$

where the first and the third equalities follows from (3.8) and the second from the remark just before the definition of $\gamma_{[V],i}$.

Since $N = p^f - 1$, we have the coincidence $D^{(i)} = D(p^i)$. Thus, we obtain (3.16) by applying (3.12) to $D^{(i)} = D(p^i)$. (Note that the p^i-action on $\tilde{P}_N$ is bijective.) □

REMARK (3.17). In this remark, we do not assume $N = p^f - 1$.

(i) For general N, the same argument as in the proof of (3.12) shows that (3.12) holds if we replace $N^{2g} - C(g)N^{2g-1}$ by $N^{2g} - C(g)(p^f - 1)N^{2g-2}$. (Apply (2.6) to $\frac{p^f-1}{N}D$.) Similarly, (3.16) holds if we replace $D^{(i)}$ by $D(p^i)$, and $N^{2g} - C(g)N^{2g-1}$ by $N^{2g} - C(g)(p^f - 1)N^{2g-2}$.

However, the resulting inequalities say nothing, unless $N^2 > C(g)(p^f - 1)$. For $g > 0$, the last condition forces N to be a rather big divisor of $p^f - 1$ ($N > \sqrt{p^f - 1}$).

(ii) Following [R1], we can improve the inequalities for $s(D) = 0$ in (3.12) (for N general). This can be achieved by considering the p-linear maps $L_1 \to L_p, L_p \to L_{p^2}, \ldots, L_{p^{f-1}} \to L_{p^f} = L_1$ step by step, instead of considering the whole p^f-linear map $L_1 \to L_1$ at a time. Then, the right-hand sides of both the inequality of (3.12)(i) and the first inequality of (3.12)(ii) become $N^{2g} - C(g)(p-1)fN^{2g-2}$.

This time, the results say something nontrivial, if $N^2 > C(g)(p-1)f$. The last condition is satisfied for $N > C(g)(p-1)$. In particular, they say something nontrivial for almost all N.

(iii) What is the counterpart of (ii) above in the case $s(D) = 1$ (or $s(D(p^i)) = 1$)? To state it, put

$$\{a_1, \ldots, a_m\} = \{a = 0, 1, \ldots, f-1 \mid s(D(p^a)) = 1\},$$

where we assume $(0 \leq) a_1 < a_2 < \cdots < a_m (\leq f-1)$. We define the natural numbers f_i by

$$f_i \stackrel{\text{def}}{=} \begin{cases} a_{i+1} - a_i & \text{if } 1 \leq i < m, \\ a_1 + f - a_m & \text{if } i = m, \end{cases}$$

so that $\sum_{i=1}^m f_i = f$. Now, by considering the p^{f_i}-linear maps $L_{p^{a_i}} \to L_{p^{a_{i+1}}}$ step by step as in (ii), we obtain the improvement (for N general)

$$\geq N^{2g} - C(g)\left(\sum_{i=1}^m (p^{f_i} - 1)\right) N^{2g-2}$$

in the statements of (3.12)(i)(ii) and (3.16). (For (3.12), we assume $a_1 = 0$.)

The improved inequalities say something nontrivial, if N^2 is greater than $C(g)\left(\sum_{i=1}^m (p^{f_i} - 1)\right)$. However, the right-hand side of the last condition depends not only on p, g and f but also on the coefficients of $D \in \mathbb{Z}[S]$.

Assuming $N = p^f - 1$ again, we shall give a rough estimate of the number of D to which (3.12) or (3.16) can be applied. (See Appendix for a related result for general N.) Note that

$$\#((\mathbb{Z}/N\mathbb{Z})^\sim[S]^0) = N^{n-1+b^{(2)}} = \begin{cases} 1 & \text{if } n \leq 1, \\ N^{n-1} & \text{if } n > 1. \end{cases}$$

Proposition (3.18). (i) *If $n \leq 1$, the value s for the unique element of $(\mathbb{Z}/N\mathbb{Z})^\sim[S]^0$ is 0.*

(ii) *If $n > 1$, there exist $M > 0$ and $0 \leq \alpha < 1$ depending only on p and n, such that*

$$\#\left\{D \in (\mathbb{Z}/N\mathbb{Z})^\sim[S]^0 \mid s(D^{(i)}) = 1 \text{ for some } i = 0, 1, \ldots f-1\right\} \geq N^{n-1}(1 - \alpha^f) - 1$$

for all $f \geq M$.

More precisely, let k be any positive integer $\geq \log_p(n-1)$ and ε any positive real number < 1. Then we can take

$$M = \frac{k}{\varepsilon}, \quad \alpha = \left(1 - \frac{1}{p^{k(n-1)}}\binom{p^k}{n-1}\right)^{(1-\varepsilon)/k}.$$

Proof. (i) Clear. ($(\mathbb{Z}/N\mathbb{Z})^\sim[S]^0$ consists of the trivial divisor.)

(ii) We choose any $Q \in S$ and put $S' = S - \{Q\}$, whose cardinality is $n' \stackrel{\text{def}}{=} n-1$. The projection $(\mathbb{Z}/N\mathbb{Z})^\sim[S]^0 \to (\mathbb{Z}/N\mathbb{Z})^\sim[S']$, $D \mapsto D'$ is bijective. We have

$$s(D) = \frac{1}{N}\deg(D) = \left\lceil \frac{1}{N}\deg(D') \right\rceil,$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$. Therefore, we have

$$s(D) \leq 1 \iff \deg(D') \leq N.$$

When $n' = 1$, $\deg(D') \leq N$ for all D'. Then the statements clearly hold ($\alpha = 0$). (Note that the term -1 comes from the trivial divisor.) So, from now on, we shall assume $n' > 1$.

Let k be a positive integer $\geq \log_p(n')$ and ε any positive real number < 1. We assume $f \geq M \overset{\text{def}}{=} \frac{k}{\varepsilon}$. Let D' be any element of $(\mathbb{Z}/N\mathbb{Z})^{\sim}[S']$, and, for each $P \in S'$, consider the p-adic expansion

$$\mathrm{ord}_P(D') = \sum_{j=0}^{f-1} n_{P,j} p^j,$$

with $n_{P,j} \in \{0, 1, \ldots, p-1\}$.

If we have

$$\sum_{P \in S'} \sum_{j=0}^{k-1} n_{P,f-k+j} p^j \leq p^k - n',$$

then we obtain

$$\begin{aligned} \deg(D') &= \sum_{P \in S'} \left(\sum_{j=0}^{f-k-1} n_{P,j} p^j \right) + \sum_{j=f-k}^{f-1} n_{P,j} p^j \\ &\leq n'(p^{f-k} - 1) + p^{f-k}(p^k - n') \\ &= p^f - n' \leq p^f - 1 = N. \end{aligned}$$

In the same way, if we have

$$\sum_{P \in S'} \sum_{j=0}^{k-1} n_{P,f-hk+j} p^j \leq p^k - n'$$

for some $h = 1, 2, \ldots, \left[\frac{f}{k}\right]$, then we obtain

$$\deg((D')^{(-(h-1)k)}) \leq N.$$

In other words, if we suppose that $\deg((D')^{(i)}) > N$ for all $i = 0, 1, \ldots, f-1$, we must have

$$\sum_{P \in S'} \sum_{j=0}^{k-1} n_{P,f-hk+j} p^j > p^k - n' \tag{3.19}$$

for all $h = 1, \ldots, \left[\frac{f}{k}\right]$. Now, since

$$\#\{E \in (\mathbb{Z}/p^k\mathbb{Z})^{\sim}[S'] \mid \deg(E) \leq p^k - n'\} = \binom{(p^k - n') + n'}{n'} = \binom{p^k}{n'}$$

("repeated combination"), we obtain

$$\begin{aligned}&\#\{D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0 \mid s(D^{(i)}) > 1 \text{ for all } i = 0, 1, \dots, f-1\}\\ &\leq \left(p^{kn'} - \binom{p^k}{n'}\right)^{\left[\frac{f}{k}\right]} p^{(f-k[\frac{f}{k}])n'} - (p^{fn'} - (p^f-1)^{n'}).\end{aligned}$$

Here, the term $(p^{fn'} - (p^f-1)^{n'})$ is the cardinality of the set

$$(\mathbb{Z}/p^f\mathbb{Z})^{\sim}[S'] - (\mathbb{Z}/N\mathbb{Z})^{\sim}[S'].$$

(Note that each element of $(\mathbb{Z}/p^f\mathbb{Z})^{\sim}[S'] - (\mathbb{Z}/N\mathbb{Z})^{\sim}[S']$ automatically satisfies (3.19), since we have assumed $n' > 1$.) By applying the identity

$$\frac{B}{B'}A' - \{A' - (B' - B)\} = \frac{(B' - A')(B' - B)}{B'}$$

to $B = (p^f - 1)^{n'}$, $B' = p^{fn'}$ and $A' = \left(p^{kn'} - \binom{p^k}{n'}\right)^{\left[\frac{f}{k}\right]} p^{(f-k[\frac{f}{k}])n'}$, we obtain

$$\begin{aligned}&\#\{D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0 \mid s(D^{(i)}) > 1 \text{ for all } i = 0, 1, \dots f-1\}\\ &\leq \frac{(p^f-1)^{n'}}{p^{fn'}}\left(p^{kn'} - \binom{p^k}{n'}\right)^{\left[\frac{f}{k}\right]} p^{(f-k[\frac{f}{k}])n'}\\ &= N^{n'}\left(1 - \frac{1}{p^{kn'}}\binom{p^k}{n'}\right)^{\left[\frac{f}{k}\right]}\\ &\leq N^{n'}\left(1 - \frac{1}{p^{kn'}}\binom{p^k}{n'}\right)^{(1-\varepsilon)f/k},\end{aligned}$$

where the last inequality follows from our assumption $f \geq k/\varepsilon$:

$$\left[\frac{f}{k}\right] \geq \frac{f}{k} - 1 \geq \frac{(1-\varepsilon)f}{k}.$$

Now, the statements of (ii) follow immediately. □

Finally, we shall summarize (3.12), (3.16) and (3.18) in terms of $\boldsymbol{\mu}_N$-torsors, via (3.5) and (3.6). Recall that we are assuming $N = p^f - 1$.

THEOREM (3.20). *Let $C(g)$ be as in* (3.13).

(i) *If $n \leq 1$, we have*

$$\#\{[V] \in H^1_{\acute{e}t}(U, \boldsymbol{\mu}_N) \mid \gamma_{[V],1} = g-1\} \geq N^{2g} - C(g)N^{2g-1} - 1$$

(ii) *If $n > 1$, we have*

$$\#\{[V] \in H^1_{\acute{e}t}(U, \boldsymbol{\mu}_N) \mid \gamma_{[V],1} = g\} \geq (N^{2g} - C(g)N^{2g-1})\{N^{n-1}(1-\alpha^f) - 1\}$$

for $f \geq M$, where M and α are as in (3.18)(ii). □

Roughly speaking, (3.20) says that the generalized Hasse–Witt invariants for 'most' (p^f-1)-cyclic coverings are g (resp. $g-1$) if $n > 1$ (resp. $n \leq 1$).

4. A Group-Theoretic Characterization of Genera

In this section, we shall prove that the genus of a curve over an algebraically closed field of characteristic > 0 can be recovered group-theoretically from the tame fundamental group of the curve. More precisely, we shall prove the following:

THEOREM (4.1). *For each $i = 1, 2$, let p_i be a prime number, k_i an algebraically closed field of characteristic p_i, X_i a proper, smooth, connected curve of genus g_i over k_i, S_i a finite (possibly empty) set of closed points of X_i with cardinality n_i, and $U_i = X_i - S_i$. If $\pi_1^{\mathrm{t}}(U_1) \simeq \pi_1^{\mathrm{t}}(U_2)$ (as topological groups), then we have:*

(i) *$p_1 = p_2$, unless $g_i = 0$, $n_i \leq 1$ for $i = 1, 2$;*
(ii) *$g_1 = g_2$; and*
(iii) *$n_1 = n_2$, unless $\{(g_1, n_1), (g_2, n_2)\} = \{(0, 0), (0, 1)\}$.*

REMARK (4.2). To specify the notion of being recovered group-theoretically, we need to introduce two curves (see [T2], § 1, Definition). However, the following proof involves only one curve, and what we shall do is to extract its various invariants from its tame fundamental group by purely group-theoretic procedure.

Now, let p, k, X, g, S, n, U be as in Section 2 and Section 3. Recall that the i-th Betti number $b^{(i)}$ of U, defined as the $\mathbb{Z}_l$-rank of the l-adic étale cohomology group $H^i_{\text{ét}}(U, \mathbb{Z}_l)$ (l: a prime number $\neq p$), is given in terms of (g, n) as:

$$b^{(0)} = 1,\ b^{(1)} = 2g + n - 1 + b^{(2)},\ b^{(2)} = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{if } n > 0. \end{cases}$$

First, we shall settle some minor things.

LEMMA (4.3). (i) *The invariant $b^{(1)}$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$.*
(ii) *We have*

$$\left.\begin{array}{l} b^{(1)} = 0 \iff (g, n) = (0, 0), (0, 1) \\ b^{(1)} = 1 \iff (g, n) = (0, 2) \end{array}\right\} \Rightarrow g = 0.$$

(iii) *Except for the case $b^{(1)} = 0$, the invariant p can be recovered from $\pi_1^{\mathrm{t}}(U)$ group-theoretically.*

PROOF. (ii) is trivial. As is well-known, $\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}$ is isomorphic to

$$\prod_{l \neq p} \mathbb{Z}_l^{b^{(1)}} \times \mathbb{Z}_p^{\gamma},$$

where γ is the p-rank of (the Jacobian variety of) X (see [T1], Corollary (1.2)). From this, (i) follows.

Since

$$(0 \leq)\gamma \leq g \leq 2g \leq 2g + n - 1 + b^{(2)} = b^{(1)},$$

$\gamma = b^{(1)}$ holds (if and) only if $g = n-1+b^{(2)} = 0$ holds, or, equivalently, $b^{(1)} = 0$. In other words, except for the case $b^{(1)} = 0$, $\gamma < b^{(1)}$ holds, so we can extract the invariant p from the above description of $\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}$ (see [T2], Proposition (1.2)). Thus, (iii) follows. □

By this lemma, we obtain (4.1)(i). Moreover, by (i) and (ii) of this lemma, we may assume that $b^{(1)} > 1$ when we prove (4.1)(ii). In particular, we may use the invariant p freely.

The essence of (4.1)(ii) is in (3.20), which says, roughly speaking, that the generalized Hasse–Witt invariants for 'most' (p^f-1)-cyclic coverings are g (resp. $g-1$) if $n > 1$ (resp. $n \leq 1$).

However, a few problems remain. The first problem is that, strictly speaking, $\boldsymbol{\mu}_N = \boldsymbol{\mu}_N(k)$ is not a group-theoretic object. Namely, even if we are given an isomorphism $\pi_1^{\mathrm{t}}(U_1) \simeq \pi_1^{\mathrm{t}}(U_2)$, we are not given any natural isomorphism $\boldsymbol{\mu}_N(k_1) \simeq \boldsymbol{\mu}_N(k_2)$, a priori, hence we do not have any natural isomorphism

$$H^1_{\text{ét}}(U_1, \boldsymbol{\mu}_N) \simeq H^1_{\text{ét}}(U_2, \boldsymbol{\mu}_N).$$

Moreover, in order to define $\gamma_{[V],1}$ for each $[V] \in H^1_{\text{ét}}(X, \boldsymbol{\mu}_N)$, we have used not only the group $\boldsymbol{\mu}_N$ but also the natural embedding $\boldsymbol{\mu}_N \hookrightarrow k$ and the field structure of k, which are also not group-theoretic objects.

In fact, by means of (3.8), any fixed isomorphism $\boldsymbol{\mu}_N(k_1) \simeq \boldsymbol{\mu}_N(k_2)$ will turn out to work for our purpose. However, to avoid confusion and to make things clear, in this section, we will use the set of open normal subgroups H of $\pi_1^{\mathrm{t}}(U)$ such that $\pi_1^{\mathrm{t}}(U)/H$ is a cyclic group of order dividing N, instead of using $H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$, and rewrite (3.20) in purely group-theoretic terms.

The second problem is that, if $n \leq 1$, the generalized Hasse–Witt invariant for a general (p^f-1)-covering is $g-1$, and, if $n > 1$, it is g, and that we do not know, a priori, in which case we are.

We overcome this second problem by considering not only the base curve U but also suitable (tame) coverings of U.

Now, we shall start with the first problem.

Assume that a cyclic group G of order prime to p and an $\mathbb{F}_p[G]$-module M are given. As in Section 3, as soon as we are given a character $\chi : G \to k^\times$ for some field k of characteristic p, we can define $\gamma_\chi(M) \stackrel{\text{def}}{=} \dim_k((M \otimes k)(\chi))$, where

$$(M \otimes k)(\chi) \stackrel{\text{def}}{=} \{x \in M \otimes k \mid \sigma \cdot x = \chi(\sigma)x \text{ for all } \sigma \in G\}.$$

However, the case is that only G and M are given. In this situation, only certain sums of $\gamma_\chi(M)$ can be well-defined, as follows.

Definition. We define the primitive part of M by

$$M^{\mathrm{prim}} \stackrel{\text{def}}{=} M/(\sum_{\sigma \neq 1} M^{\langle\sigma\rangle}),$$

where $M^{\langle\sigma\rangle} \overset{\text{def}}{=} \{x \in M \mid \sigma \cdot x = x\}$ for each $\sigma \in G$. We put

$$\gamma^{\text{prim}}(M) \overset{\text{def}}{=} \dim_{\mathbb{F}_p}(M^{\text{prim}}).$$

REMARK (4.4). (i) Let k be a field of characteristic p containing all $\#(G)$-th roots of unity. Then we can check:

$$\gamma^{\text{prim}}(M) = \sum_{\chi: G \hookrightarrow k^\times} \gamma_\chi(M).$$

(ii) Assume that M is finite-dimensional as an $\mathbb{F}_p$-vector space. We can naturally regard the dual vector space $M^* \overset{\text{def}}{=} \text{Hom}_{\mathbb{F}_p}(M, \mathbb{F}_p)$ as a G-module by $(\sigma \cdot \phi)(x) = \phi(\sigma^{-1} \cdot x)$, where $\sigma \in G$, $\phi \in M^*$, and $x \in M$. Then we can check:

$$\gamma^{\text{prim}}(M^*) = \gamma^{\text{prim}}(M).$$

(One way to check this: $\gamma_\chi(M^*) = \gamma_{\chi^{-1}}(M)$.)

We return to the tame fundamental group $\pi_1^{\text{t}}(U)$. Let H be an open normal subgroup of $\pi_1^{\text{t}}(U)$ such that $\pi_1^{\text{t}}(U)/H$ is cyclic of order prime to p. The conjugation induces an action of $\pi_1^{\text{t}}(U)/H$ on the $\mathbb{F}_p$-vector space H^{ab}/p, whose dimension we denote by γ_H.

DEFINITION. $\gamma_H^{\text{prim}} \overset{\text{def}}{=} \gamma^{\text{prim}}(H^{\text{ab}}/p)$.

For each natural number N prime to p, we define $\mathcal{H}_N$ to be the set of open normal subgroups H of $\pi_1^{\text{t}}(U)$ such that $\pi_1^{\text{t}}(U)/H$ is cyclic of order dividing N.

DEFINITION. $\gamma_N^{\text{av}} \overset{\text{def}}{=} \dfrac{1}{N^{b^{(1)}}} \sum_{H \in \mathcal{H}_N} \gamma_H^{\text{prim}}$.

In this definition, "av" means "average". In fact, we have a reinterpretation of γ_N^{av}:

LEMMA (4.5). *We have*

$$\begin{aligned}\gamma_N^{\text{av}} &= \underset{[V] \in H^1_{\acute{e}t}(U, \boldsymbol{\mu}_N)}{\text{Average}} \gamma_{[V],1} \\ &\overset{\text{def}}{=} \frac{1}{\#(H^1_{\acute{e}t}(U, \boldsymbol{\mu}_N))} \sum_{[V] \in H^1_{\acute{e}t}(U, \boldsymbol{\mu}_N)} \gamma_{[V],1}.\end{aligned}$$

PROOF. By (4.4)(ii),

$$\begin{aligned}\gamma_H^{\text{prim}} &= \gamma^{\text{prim}}(H^{\text{ab}}/p) = \gamma^{\text{prim}}((H^{\text{ab}}/p)^*) \\ &= \gamma^{\text{prim}}(\text{Hom}(\pi_1^{\text{t}}(U_H), \mathbb{F}_p)) = \gamma^{\text{prim}}(H^1_{\text{ét}}(X_H, \mathbb{F}_p)),\end{aligned}$$

where U_H is the tame covering of U corresponding to $H \subset \pi_1^{\text{t}}(U)$ and X_H is the normalization of X in U_H, and then by (4.4)(i),

$$\gamma_H^{\text{prim}} = \sum_{\chi: \pi_1^{\text{t}}(U)/H \hookrightarrow k^\times} \gamma_\chi(H^1_{\text{ét}}(X_H, \mathbb{F}_p)).$$

On the other hand, we have the following bijection:

$$\{(H,\chi) \mid H \in \mathcal{H}_N,\ \chi : \pi_1^{\mathrm{t}}(U)/H \hookrightarrow k^\times\} \xrightarrow{\sim} \mathrm{Hom}(\pi_1^{\mathrm{t}}(U), \boldsymbol{\mu}_N), \tag{4.6}$$

where (H,χ) goes to $(\pi_1^{\mathrm{t}}(U) \twoheadrightarrow \pi_1^{\mathrm{t}}(U)/H \overset{\chi}{\hookrightarrow} \boldsymbol{\mu}_N)$. Now, let $[V]$ be the element of $H^1_{\text{ét}}(U, \boldsymbol{\mu}_N) = \mathrm{Hom}(\pi_1^{\mathrm{t}}(U), \boldsymbol{\mu}_N)$ corresponding to (H,χ). Then we claim

$$\gamma_{[V],1} = \gamma_\chi(H^1_{\text{ét}}(X_H, \mathbb{F}_p)). \tag{4.7}$$

In fact, let Y be the normalization of X in V. Then, since U_H is the $\mathrm{Im}(\chi)$-torsor of U corresponding to $(\pi_1^{\mathrm{t}}(U) \twoheadrightarrow \pi_1^{\mathrm{t}}(U)/H \overset{\chi}{\xrightarrow{\sim}} \mathrm{Im}(\chi))$, we see that Y coincides with $\boldsymbol{\mu}_N \times_{\mathrm{Im}(\chi)} X_H$, the quotient of $\boldsymbol{\mu}_N \times X_H$ by the $\mathrm{Im}(\chi)$-action $(\zeta, x)^{\zeta_0} = (\zeta_0^{-1}\zeta, x^{\zeta_0})$. From this, we can deduce that $H^1_{\text{ét}}(Y, \mathbb{F}_p)$ is the induced $\mathbb{F}_p[\boldsymbol{\mu}_N]$-module of the $\mathbb{F}_p[\mathrm{Im}(\chi)]$-module $H^1_{\text{ét}}(X_H, \mathbb{F}_p)$. Now our claim (4.7) follows immediately.

Now, bijection (4.6), identity (4.7) and the fact $H^1_{\text{ét}}(U, \boldsymbol{\mu}_N) \simeq (\mathbb{Z}/N\mathbb{Z})^{b^{(1)}}$ complete the proof. □

Remark (4.8). Here is another simple reinterpretation of γ_N^{av}. For a profinite group Π and a natural number m, we shall denote by $\Pi(m)$ the kernel of $\Pi \twoheadrightarrow \Pi^{\mathrm{ab}}/(\Pi^{\mathrm{ab}})^m$, or, equivalently, $\Pi(m)$ is the topological closure of the subgroup $[\Pi,\Pi]\Pi^m$ of Π. Moreover, we shall denote by $U(m)$ the tame covering of U corresponding to the subgroup $\pi_1^{\mathrm{t}}(U)(m)$ of $\pi_1^{\mathrm{t}}(U)$, so that $\pi_1^{\mathrm{t}}(U(m)) = \pi_1^{\mathrm{t}}(U)(m)$, and $X(m)$ the normalization of X in $U(m)$. (Note that this last notation is somewhat confusing: $X(m)$ does not coincide with the (étale) covering of X corresponding to $\pi_1(X)(m)$ in general.) Then we have

$$\gamma_N^{\mathrm{av}} = \frac{\dim_{\mathbb{F}_p}(\pi_1^{\mathrm{t}}(U)(N)/(\pi_1^{\mathrm{t}}(U)(N))(p))}{(\pi_1^{\mathrm{t}}(U) : \pi_1^{\mathrm{t}}(U)(N))}.$$

In fact, the denominator of the right-hand side is $N^{b^{(1)}}$, while the numerator is $\dim_{\mathbb{F}_p}(H^1_{\text{ét}}(X(N), \mathbb{F}_p))$. Since $\pi_1^{\mathrm{t}}(U)/\pi_1^{\mathrm{t}}(U)(N) = \pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}/N$ is abelian of order prime to p, we see that the following canonical decomposition exists:

$$H^1_{\text{ét}}(X(N), \mathbb{F}_p) = \bigoplus_{H \in \mathcal{H}_N} (H^1_{\text{ét}}(X(N), \mathbb{F}_p)^{H/\pi_1^{\mathrm{t}}(U)(N)})^{(\pi_1^{\mathrm{t}}(U)/H)\text{-prim}},$$

where $(\pi_1^{\mathrm{t}}(U)/H)$-prim means the primitive part as a $(\pi_1^{\mathrm{t}}(U)/H)$-module. Since $H^1_{\text{ét}}(X(N), \mathbb{F}_p)^{H/\pi_1^{\mathrm{t}}(U)(N)} = H^1_{\text{ét}}(X_H, \mathbb{F}_p)$ (see the proof of (4.5) for the definition of X_H), we obtain the desired equality

$$\dim_{\mathbb{F}_p}(H^1_{\text{ét}}(X(N), \mathbb{F}_p)) = \sum_{H \in \mathcal{H}_N} \gamma_H^{\mathrm{prim}}$$

(see the beginning of the proof of (4.5)).

The following is a variant of (3.20). Recall that we are assuming $b^{(1)} > 1$.

Theorem (4.9). *Assume $N = p^f - 1$. Let $C(g)$ be as in* (3.13).

(i) *If $n \leq 1$, we have*

$$g - 1 - \frac{C(b^{(1)}/2)(b^{(1)}/2 - 1)}{N} \leq \gamma_N^{\mathrm{av}} \leq g - 1 + \frac{1}{N^{b^{(1)}}}.$$

(ii) *If $n > 1$, let k be any positive integer $\geq \log_p(b^{(1)})$, ε any positive real number < 1, and put*

$$M = \frac{k}{\varepsilon},\ \alpha = \left(1 - \frac{1}{p^{kb^{(1)}}}\binom{p^k}{b^{(1)}}\right)^{(1-\varepsilon)/k}.$$

Then, we have

$$g - \left\{\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 1\right)\frac{1}{N} + \left[\frac{b^{(1)}}{2}\right]\alpha^f\right\} \leq \gamma_N^{\mathrm{av}} \leq g + (b^{(1)} - 1)\alpha^f$$

for all $f \geq M$.

Proof. (i) We first note that $b^{(1)} = 2g$ holds in this case. By (3.7)(and (3.6)), we have

$$\gamma_{[V],1} \leq \begin{cases} g, & \text{if } [V] = 0, \\ g - 1, & \text{otherwise,} \end{cases}$$

for each $[V] \in H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$. From this,

$$\sum_{[V] \in H^1_{\text{ét}}(U,\boldsymbol{\mu}_N)} \gamma_{[V],1} \leq (N^{b^{(1)}} - 1)(g - 1) + g = N^{b^{(1)}}(g - 1) + 1,$$

hence

$$\gamma_N^{\mathrm{av}} \leq g - 1 + \frac{1}{N^{b^{(1)}}}.$$

On the other hand, by (3.12)(ii) and (3.18)(i), we have

$$\sum_{[V] \in H^1_{\text{ét}}(U,\boldsymbol{\mu}_N)} \gamma_{[V],1} \geq (g - 1)(N^{b^{(1)}} - C(g)N^{b^{(1)}-1}),$$

hence

$$\gamma_N^{\mathrm{av}} \geq g - 1 - \frac{C(g)(g - 1)}{N}.$$

Since $g = b^{(1)}/2$, this completes the proof.

(ii) Dividing the sum $\sum_{[V] \in H^1_{\text{ét}}(U,\boldsymbol{\mu}_N)} \gamma_{[V],1}$ into the three parts: (0) $D = 0$; (1) $s(D^{(i)}) = 1$ for some $i = 0, 1, \ldots, f - 1$; (2) otherwise, we obtain

$$\begin{aligned} &\sum_{[V] \in H^1_{\text{ét}}(U,\boldsymbol{\mu}_N)} \gamma_{[V],1} \\ &\leq ((g - 1)N^{2g} + 1) + gN^{2g}(N^{n-1}(1 - \alpha^f) - 1) + (g + n - 2)N^{2g}N^{n-1}\alpha^f \\ &= gN^{b^{(1)}} - (N^{2g} - 1) + (n - 2)N^{b^{(1)}}\alpha^f \\ &\leq gN^{b^{(1)}} + (b^{(1)} - 1)N^{b^{(1)}}\alpha^f \end{aligned}$$

for $f \geq M$, by (3.7) and (3.18)(ii). (Here, note that

$$k \geq \log_p(b^{(1)}) \geq \log_p(n-1)$$

and

$$\alpha = \left(1 - \frac{1}{p^{kb^{(1)}}}\binom{p^k}{b^{(1)}}\right)^{(1-\varepsilon)/k} \leq \left(1 - \frac{1}{p^{k(n-1)}}\binom{p^k}{n-1}\right)^{(1-\varepsilon)/k},$$

since $n-1 \leq b^{(1)}$.) Therefore

$$\gamma_N^{\mathrm{av}} \leq g + (b^{(1)} - 1)\alpha^f.$$

Similarly, considering the cases (0) and (1), we have

$$\begin{aligned}
&\sum_{[V] \in H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)} \gamma_{[V],1} \\
&\geq (g-1)(N^{2g} - C(g)N^{2g-1}) + g(N^{2g} - C(g)N^{2g-1})(N^{n-1}(1-\alpha^f) - 1) \\
&= gN^{b^{(1)}} - C(g)gN^{b^{(1)}-1} - gN^{b^{(1)}}\alpha^f + C(g)gN^{b^{(1)}-1}\alpha^f - N^{2g} + C(g)N^{2g-1} \\
&\geq gN^{b^{(1)}} - C(g)gN^{b^{(1)}-1} - gN^{b^{(1)}}\alpha^f - N^{2g} \\
&\geq gN^{b^{(1)}} - (C(g)g+1)N^{b^{(1)}-1} - gN^{b^{(1)}}\alpha^f \\
&\geq gN^{b^{(1)}} - \left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 1\right)N^{b^{(1)}-1} - \left[\frac{b^{(1)}}{2}\right]N^{b^{(1)}}\alpha^f
\end{aligned}$$

for $f \geq M$, by (3.16), etc. (For the last inequality, note that $g \leq \left[b^{(1)}/2\right]$ and that $C(g)$ is monotone increasing.) Therefore, we have

$$\gamma_N^{\mathrm{av}} \geq g - \left\{\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 1\right)\frac{1}{N} + \left[\frac{b^{(1)}}{2}\right]\alpha^f\right\}$$

for all $f \geq M$. □

Definition. We define

$$g' \overset{\text{def}}{=} \begin{cases} g-1, & \text{if } n \leq 1, \\ g, & \text{if } n > 1. \end{cases}$$

The following (together with (4.3)) gives a group-theoretic characterization of the invariant g'.

Corollary (4.10). (We are assuming $b^{(1)} > 1$.) *Let M and α be as in* (4.9), *and $C(g)$ as in* (3.13). *Then*

$$\begin{aligned}
g' - \left\{\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right]+1\right)\frac{1}{N} + \left[\frac{b^{(1)}}{2}\right]\alpha^f\right\} &\leq \gamma_N^{\mathrm{av}} \\
&\leq g' + \max\left(\frac{1}{N^{b^{(1)}}}, (b^{(1)}-1)\alpha^f\right)
\end{aligned}$$

for all $f \geq M$.

In particular, if f is sufficiently large (e.g., if

$$f \geq \max\left(M, \frac{\log(3b^{(1)})}{\log(\alpha^{-1})}, \log_p\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right) b^{(1)} + 5\right)\right)$$

holds), then g' can be characterized as the unique integer in the interval

$$\left[\gamma_N^{\mathrm{av}} - \max\left(\frac{1}{N^{b^{(1)}}}, (b^{(1)}-1)\alpha^f\right), \right.$$
$$\left. \gamma_N^{\mathrm{av}} + \left\{\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 1\right)\frac{1}{N} + \left[\frac{b^{(1)}}{2}\right]\alpha^f\right\}\right].$$

Proof. By (4.9), g' falls in the interval for $f \geq M$.

Assume $f \geq \max\left(M, \frac{\log(3b^{(1)})}{\log(\alpha^{-1})}, \log_p\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right) b^{(1)} + 5\right)\right)$. Then the length λ of the interval satisfies:

$$\begin{aligned}
\lambda = \max\Bigg(&\frac{1}{N^{b^{(1)}}} + \left\{\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 1\right)\frac{1}{N} + \left[\frac{b^{(1)}}{2}\right]\alpha^f\right\}, \\
&(b^{(1)}-1)\alpha^f + \left\{\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 1\right)\frac{1}{N} + \left[\frac{b^{(1)}}{2}\right]\alpha^f\right\}\Bigg) \\
< &\frac{1}{N^{b^{(1)}}} + (b^{(1)}-1)\alpha^f + \left\{\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 1\right)\frac{1}{N} + \left[\frac{b^{(1)}}{2}\right]\alpha^f\right\} \\
< &\left(C\left(\left[\frac{b^{(1)}}{2}\right]\right)\left[\frac{b^{(1)}}{2}\right] + 2\right)\frac{1}{N} + \frac{3b^{(1)}}{2}\alpha^f \\
\leq &\tfrac{1}{2} + \tfrac{1}{2} = 1.
\end{aligned}$$

This implies the desired uniqueness. □

At the cost of sacrificing effectivity, we also obtain the following more impressive characterization of g'.

Corollary (4.11). $\lim_{f\to\infty} \gamma_{p^f-1}^{\mathrm{av}} = g'$. □

Remark (4.12). It is easy to see that (4.11) is also valid for $b^{(1)} = 1$. In order to include the case that $b^{(1)} = 0$, the formula should be modified as

$$\lim_{f\to\infty} \gamma_{p^f-1}^{\mathrm{av}} = (g')^+,$$

where $x^+ \stackrel{\mathrm{def}}{=} \max(x, 0)$.

Now, we shall treat the second problem: the group-theoretic characterization above is not for g but for g'.

First, we introduce the following temporary invariant, which can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$ (assuming $b^{(1)} > 0$):

$$n^{\mathrm{temp}} \stackrel{\mathrm{def}}{=} b^{(1)} - 2g' + 1.$$

Next, let m be a natural number prime to p, and $U(m)$ the tame covering of U as in (4.8). We define $n(m)$ (resp. $n^{\mathrm{temp}}(m)$) to be the invariant n (resp. n^{temp}) for the curve $U(m)$. Note that $n^{\mathrm{temp}}(m)$ can also be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$.

LEMMA (4.13). *Assume* $b^{(1)} > 0$.

(i) *We have*

$$n^{\mathrm{temp}} = \begin{cases} 3, & \text{if } n \leq 1, \\ n, & \text{if } n > 1. \end{cases}$$

(ii) *If* $m > 1$, *we have*

$$n^{\mathrm{temp}}(m) = \begin{cases} 3, & \text{if } n = 0, \\ m^{b^{(1)}}, & \text{if } n = 1, \\ m^{b^{(1)}-1}n, & \text{if } n > 1. \end{cases}$$

PROOF. (i) Immediate from the definitions.

(ii) By (i), we have

$$n^{\mathrm{temp}}(m) = \begin{cases} 3, & \text{if } n(m) \leq 1, \\ n(m), & \text{if } n(m) > 1. \end{cases}$$

On the other hand, we have

$$n(m) = \begin{cases} m^{b^{(1)}}n, & \text{if } n \leq 1, \\ m^{b^{(1)}-1}n, & \text{if } n > 1. \end{cases}$$

These give the desired equality. □

Finally, we can prove the following:

THEOREM (4.14). *Assume* $b^{(1)} > 0$. *Fix any natural number* $m \neq 1, 3$ *prime to* p. *Then*

$$n = \begin{cases} n^{\mathrm{temp}}, & \text{if } n^{\mathrm{temp}} \neq 3, \\ 0, & \text{if } n^{\mathrm{temp}} = 3 \text{ and } n^{\mathrm{temp}}(m) = 3, \\ 1, & \text{if } n^{\mathrm{temp}} = 3 \text{ and } n^{\mathrm{temp}}(m) = m^{b^{(1)}}, \\ 3, & \text{if } n^{\mathrm{temp}} = 3 \text{ and } n^{\mathrm{temp}}(m) = 3m^{b^{(1)}-1}. \end{cases}$$

In particular, the invariant n *can be recovered group-theoretically from* $\pi_1^{\mathrm{t}}(U)$ (*except for the case* $b^{(1)} = 0$).

PROOF. The first statement follows from (4.13). Since n^{temp}, $n^{\mathrm{temp}}(m)$ and $b^{(1)}$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$, the second statement follows. (More precisely, we have to consider two cases separately. If $b^{(1)} = 1$, then we have $n = n^{\mathrm{temp}} = 2$. Otherwise, i.e. if $b^{(1)} > 1$, then the numbers 3, $m^{b^{(1)}}$ and $3m^{b^{(1)}-1}$ are distinct from one another.) □

End of proof of (4.1). As we have already seen, (4.3) implies (4.1)(i) and that we may assume $b^{(1)} > 0$ when we prove (4.1)(ii)(iii). Now, (4.14) implies (4.1)(iii). Since $b^{(2)}$ is determined by n, (4.14) and (4.3), together with the equality

$$b^{(1)} = 2g + n - 1 + b^{(2)},$$

implies (4.1)(ii). This completes the proof of (4.1). □

Remark (4.15). We might hope for the more general limit formula

$$\lim_{\substack{N \to \infty \\ p \nmid N}} \gamma_N^{\mathrm{av}} = g'. \tag{4.16}$$

For the present, we can only prove 'one half' of (4.16):

$$\limsup_{\substack{N \to \infty \\ p \nmid N}} \gamma_N^{\mathrm{av}} \leq g', \tag{4.17}$$

by using a higher-dimensional version of LeVeque's inequality, due to Stegbuchner ([S]), in the theory of uniform distribution modulo 1. See Appendix for this. It may be interesting to ask if (3.17)(iii) gives an approach to the other half of (4.16).

Remark (4.18). As in [T2], Remark (1.11), not only $\pi_1^{\mathrm{t}}(U)$ but also a suitable quotient is enough to determine g (and n). For example, $\pi_1^{\mathrm{t}}(U)/D(D(D(\pi_1^{\mathrm{t}}(U))))$ is enough, where, for a profinite group G, $D(G)$ denotes the (topological) commutator subgroup of G, or, equivalently, the kernel of $G \twoheadrightarrow G^{\mathrm{ab}}$.

Finally, as a direct consequence of (4.1), we have:

Corollary (4.19). *The quotient $\pi_1(X)$ of $\pi_1^{\mathrm{t}}(U)$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$.*

Proof. As in [T2], Corollary 1.10, this follows from (4.1)(ii) and the Hurwitz formula. □

5. Applications

(A) A group-theoretic characterization of inertia groups. Since we have established (4.1), we can prove, as in [T2], that the set of inertia subgroups of $\pi_1^{\mathrm{t}}(U)$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$ for U hyperbolic. (We say that the curve U is hyperbolic, if the Euler–Poincaré characteristic $b^{(0)} - b^{(1)} + b^{(2)} = 2 - 2g - n$ of U is negative.)

Let K be the function field $k(U) = k(X)$, and define $\tilde{K}^{\mathrm{t}}$ to be the maximal Galois extension of K in a fixed separable closure K^{sep}, unramified over U and at most tamely ramified over S. We may and shall identify $\pi_1^{\mathrm{t}}(U)$ with $\mathrm{Gal}(\tilde{K}^{\mathrm{t}}/K)$. We define $\tilde{X}^{\mathrm{t}}$ to be the normalization of X in $\tilde{K}^{\mathrm{t}}$ and $\tilde{S}^{\mathrm{t}}$ to be the inverse image of S in $\tilde{X}^{\mathrm{t}}$. For each $\tilde{P} \in \tilde{S}^{\mathrm{t}}$, we denote by $I_{\tilde{P}}$ the inertia subgroup of $\pi_1^{\mathrm{t}}(U)$

associated to $\tilde{P}$, i.e. the stabilizer of $\tilde{P}$. We have $I_{\tilde{P}} \neq \{1\}$ if and only if ($n > 0$ and) $(g, n) \neq (0, 1)$ (see [T1], Lemma (2.2)).

LEMMA (5.1). *Assume that U is hyperbolic.*

(i) *Let $\tilde{P}$ and $\tilde{Q}$ be two points of $\tilde{S}^{\mathrm{t}}$ distinct from each other. Then the intersection of $I_{\tilde{P}}$ and $I_{\tilde{Q}}$ is trivial in $\pi_1^{\mathrm{t}}(U)$. In particular, for any $\sigma \in \pi_1^{\mathrm{t}}(U) - I_{\tilde{P}}$, the intersection of $I_{\tilde{P}}$ and $\sigma I_{\tilde{P}} \sigma^{-1}$ is trivial.*

(ii) *The map $\tilde{S}^{\mathrm{t}} \to \mathrm{Sub}(\pi_1^{\mathrm{t}}(U))$, $\tilde{P} \mapsto I_{\tilde{P}}$ is injective, where, for a profinite group G, $\mathrm{Sub}(G)$ denotes the set of closed subgroups of G. Moreover, for each $\tilde{P} \in \tilde{S}^{\mathrm{t}}$, the normalizer of $I_{\tilde{P}}$ in $\pi_1^{\mathrm{t}}(U)$ is $I_{\tilde{P}}$ itself.*

PROOF. (i) [T2], Lemma (2.1). (ii) [T2], Corollary (2.2). □

Let $\mathcal{I}^{\mathrm{t}}$ be the set of inertia subgroups in $\pi_1^{\mathrm{t}}(U)$, namely the image of the map $\tilde{S}^{\mathrm{t}} \to \mathrm{Sub}(\pi_1^{\mathrm{t}}(U))$, $\tilde{P} \mapsto I_{\tilde{P}}$.

THEOREM (5.2). *If U is hyperbolic, then the set $\mathcal{I}^{\mathrm{t}}$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$. More precisely, let the notations and the assumptions be as in (4.1), and assume further that $2 - 2g_i - n_i < 0$ for some $i = 1, 2$. Then, if an isomorphism $\pi_1^{\mathrm{t}}(U_1) \simeq \pi_1^{\mathrm{t}}(U_2)$ (as topological groups) is given, the induced bijection $\mathrm{Sub}(\pi_1^{\mathrm{t}}(U_1)) \simeq \mathrm{Sub}(\pi_1^{\mathrm{t}}(U_2))$ induces a bijection $\mathcal{I}_1^{\mathrm{t}} \simeq \mathcal{I}_2^{\mathrm{t}}$, where $\mathcal{I}_i^{\mathrm{t}}$ denotes the set $\mathcal{I}^{\mathrm{t}}$ for the curve U_i, for each $i = 1, 2$.*

PROOF. See [T2], Proposition (2.4) and Remark (2.6). (Use (4.1)(iii).) □

(B) A group-theoretic characterization of 'additive structures' of inertia groups. Let $\tilde{P} \in \tilde{S}^{\mathrm{t}}$. As is well-known, $I_{\tilde{P}}$ can be canonically identified with the Tate module

$$\widehat{\mathbb{Z}}'(1) \stackrel{\mathrm{def}}{=} \varprojlim_{p \nmid m} \boldsymbol{\mu}_m(k)$$

of the multiplicative group $k^{\times}$, where $\boldsymbol{\mu}_m(k)$ is the group of m-th roots of unity in k. So, $I_{\tilde{P}} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})'$, where $(\mathbb{Q}/\mathbb{Z})'$ denotes the prime-to-p part of $\mathbb{Q}/\mathbb{Z}$, can be canonically identified with

$$(\mathbb{Q}/\mathbb{Z})'(1) \stackrel{\mathrm{def}}{=} \bigcup \boldsymbol{\mu}_m(k) = F^{\times},$$

where F denotes the algebraic closure of the prime field $\mathbb{F}_p$ in k. Thus, $F_{\tilde{P}} \stackrel{\mathrm{def}}{=} (I_{\tilde{P}} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})') \coprod \{*\}$ (where $\{*\}$ means a one-point set) can be identified with F, hence carries a structure of field, whose multiplicative group is $I_{\tilde{P}} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})'$ and whose zero element is $*$.

Now, we have the following proposition. Unlike in (A) above, the proof here is quite different from [T2], Proposition 2.8, even after we have established (4.1) and (5.2). (See [T2], Remark 2.10(ii).)

PROPOSITION (5.3). *Assume that U is hyperbolic. Then the field structure of $F_{\tilde{P}} = I_{\tilde{P}} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})' \coprod \{*\}$ can be recovered group-theoretically from $\pi_1^{\mathrm{t}}(U)$.*

PROOF. We may assume $n > 0$.

First, we shall reduce the problem to the case $n \geq 3$. If $g = 0$, this follows automatically from the hyperbolicity condition. For $g > 0$, take any natural number m prime to p such that $m^{2g}n \geq 3$. Then, replacing $\pi_1^{\mathrm{t}}(U)$ by the kernel of $\pi_1^{\mathrm{t}}(U) \to \pi_1(X)^{\mathrm{ab}}/m$ (whose index in $\pi_1^{\mathrm{t}}(U)$ is m^{2g}), we have $n \geq 3$. (Note that $I_{\tilde{P}}$ is contained in the kernel.) Next, by (5.1)(i), the set $\mathcal{I}^{\mathrm{t}}$ divided by the conjugacy action of $\pi_1^{\mathrm{t}}(U)$ consists of n orbits. Choosing any 3 orbits among these n orbits such that one of them is the conjugacy class of the given $I_{\tilde{P}}$, and dividing $\pi_1^{\mathrm{t}}(U)$ by the subgroup (topologically) generated by all members I of $\mathcal{I}^{\mathrm{t}}$ whose conjugacy class is among the other $n-3$ orbits, we may reduce the problem to the case $n = 3$. (Observe that these reduction steps are purely group-theoretic, by (4.1), (4.19) and (5.2).)

From now on, we assume $n = 3$ and we shall use (2.21). For each natural number f, let $\mathbb{F}_{p^f,\tilde{P}}$ denote the unique subfield of $F_{\tilde{P}}$ with cardinality p^f. Since $\mathbb{F}_{p^f,\tilde{P}}{}^{\times} = I_{\tilde{P}}/(p^f - 1)$, the subfield $\mathbb{F}_{p^f,\tilde{P}}$ can be recovered group-theoretically as a (multiplicative) submonoid. Fix any field $\mathbb{F}_{p^f}$ with cardinality p^f (unrelatedly to $\mathbb{F}_{p^f,\tilde{P}}$). Then the set $\mathrm{Hom}(\mathbb{F}_{p^f,\tilde{P}}{}^{\times}, \mathbb{F}_{p^f}{}^{\times}) = \mathrm{Hom}_{(\mathrm{groups})}(\mathbb{F}_{p^f,\tilde{P}}{}^{\times}, \mathbb{F}_{p^f}{}^{\times})$ is group-theoretic; recovering the field structure of $\mathbb{F}_{p^f,\tilde{P}}$ is equivalent to recovering $\mathrm{Hom}(\mathbb{F}_{p^f,\tilde{P}}, \mathbb{F}_{p^f}) = \mathrm{Hom}_{(\mathrm{fields})}(\mathbb{F}_{p^f,\tilde{P}}, \mathbb{F}_{p^f})$ as a subset of $\mathrm{Hom}(\mathbb{F}_{p^f,\tilde{P}}{}^{\times}, \mathbb{F}_{p^f}{}^{\times})$. Moreover, it is sufficient to recover this subset for f in a cofinal subset of $\mathbb{Z}_{>0}$ with respect to division.

To do this, we shall consider the two maps

$$\mathrm{Res}_f : \mathrm{Hom}(\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}/(p^f - 1), \mathbb{F}_{p^f}{}^{\times}) \to \mathrm{Hom}(\mathbb{F}_{p^f,\tilde{P}}{}^{\times}, \mathbb{F}_{p^f}{}^{\times})$$

and

$$\Gamma_f : \mathrm{Hom}(\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}/(p^f - 1), \mathbb{F}_{p^f}{}^{\times}) \to \mathbb{Z}_{\geq 0}.$$

The first map Res_f is the restriction with respect to the canonical inclusion $\mathbb{F}_{p^f,\tilde{P}}{}^{\times} = I_{\tilde{P}}/(p^f - 1) \hookrightarrow \pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}/(p^f - 1)$. The second map Γ_f is defined to send $\chi \in \mathrm{Hom}(\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}/(p^f - 1), \mathbb{F}_{p^f}{}^{\times})$ to $\gamma_\chi(H^1_{\text{ét}}(X_H, \mathbb{F}_p))$, where $H \overset{\text{def}}{=} \mathrm{Ker}(\chi)$. (For the definitions of γ_χ and X_H, see Section 4, especially (4.5) and its preceding paragraphs. Strictly speaking, in Section 4, we use the notation γ_χ only for a character χ of a cyclic group. However, the same definition goes well for characters of general finite groups, or we can replace $\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}/(p^f - 1)$ by $\mathrm{Im}(\chi)$. See the proof of (4.5).)

Now we can state the following claim, which completes the proof of (5.3).

CLAIM (5.4). Let m_0 be the product of all prime numbers $\leq p-2$. (For $p = 2, 3$, $m_0 = 1$.) Let f_0 be the order of p mod m_0 in the multiplicative group $(\mathbb{Z}/m_0\mathbb{Z})^{\times}$. For each $f > \log_p(C(g) + 1)$ divisible by f_0, we have

$$\mathrm{Hom}(\mathbb{F}_{p^f,\tilde{P}}, \mathbb{F}_{p^f}) = \mathrm{Surj}(\mathbb{F}_{p^f,\tilde{P}}{}^{\times}, \mathbb{F}_{p^f}{}^{\times}) - \mathrm{Res}_f(\Gamma_f^{-1}(\{g+1\}))$$
$$\big(\subset \mathrm{Hom}(\mathbb{F}_{p^f,\tilde{P}}{}^{\times}, \mathbb{F}_{p^f}{}^{\times}) \big).$$

To prove this claim, we fix any embedding $\mathbb{F}_{p^f} \to k$ as fields. Then we have

$$\mathrm{Hom}(\pi_1^{\mathrm{t}}(U)^{\mathrm{ab}}/(p^f-1), {\mathbb{F}_{p^f}}^{\times}) = H^1_{\text{ét}}(U, \boldsymbol{\mu}_N),$$

where $N \overset{\text{def}}{=} p^f - 1$. By (3.5), this can be identified with P_N (or $\tilde{P}_N$), in the notation of Section 3. On the other hand, $F_{\tilde{P}}$ can be canonically identified with the algebraic closure of $\mathbb{F}_p$ in k. This identification, together with the fixed embedding $\mathbb{F}_{p^f} \to k$, specifies one identification $\mathbb{F}_{p^f, \tilde{P}} = \mathbb{F}_{p^f}$. By using this, we obtain

$$\mathrm{Hom}({\mathbb{F}_{p^f, \tilde{P}}}^{\times}, {\mathbb{F}_{p^f}}^{\times}) = \mathbb{Z}/N\mathbb{Z}.$$

By using various definitions, we see that the map $P_N \to \mathbb{Z}/N\mathbb{Z}$ coming from Res_f is nothing but the composite of $b_N : P_N \to \mathbb{Z}/N\mathbb{Z}[S]$ (see (3.4)) and $\mathbb{Z}/N\mathbb{Z}[S] \to \mathbb{Z}/N\mathbb{Z}$, $D \bmod N \mapsto \mathrm{ord}_P(D)$. Thus we can reformulate (5.4) as follows: For each $n \in (\mathbb{Z}/N\mathbb{Z})^{\sim}$,

$$n \in \{p^b \mid b = 0, 1, \ldots, f-1\} \iff$$
$$(n, N) = 1 \text{ and } \nexists ([L], D) \in \tilde{P}_N \text{ s.t. } \mathrm{ord}_P(D) = n \text{ and } \gamma_{([L],D)} = g+1. \quad (5.5)$$

First, by (3.7), we see that $\gamma_{([L],D)} \leq g+1$ always holds and that $\gamma_{([L],D)} = g+1$ holds if and only only if $\gamma_{([L],D)} = \dim_k(H^1(X, L))$ (or, equivalently, $\varphi_{([L],D)}$ is bijective) and $\deg(D) = 2N$. Moreover, if $\varphi_{([L],D)}$ is bijective, then B_D^f should satisfy condition $(\star)$ of page 59, and, in particular, it should be a semi-stable vector bundle.

By this observation, the '$\Rightarrow$' part of (5.5) follows from (2.21)(iv–a). More specifically, let us denote by $P_1 = P, P_2, P_3$ the three points of S. Then (2.21)(iv–a) implies that either $\mathrm{ord}_{P_2}(D) = N$ or $\mathrm{ord}_{P_3}(D) = N$ holds, which is impossible as $D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]$.

To prove the '$\Leftarrow$' part of (5.5), let n be a natural number $\in (\mathbb{Z}/N\mathbb{Z})^{\sim}$ such that $(n, N) = 1$, and suppose that $n \notin \{p^b \mid b = 0, 1, \ldots, f-1\}$. Then we have to prove that there exists $([L], D) \in \tilde{P}_N$ such that $\mathrm{ord}_P(D) = n$ and $\gamma_{([L],D)} = g+1$. Since f is assumed to be divisible by f_0, N is divisible by all prime numbers $\leq p-2$. Therefore, by the assumption $(n, N) = 1$, we must have $n \notin I_{p-1}p^{I_f} = \{ap^b \mid a = 0, 1, \ldots, p-2,\ b = 0, 1, \ldots, f-1\}$. Now, by (2.21)(iv–c), there exists $D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]$ with degree $2N$ which satisfies (2.14) and to which (2.13) can be applied. Then, as in the proof of (3.12), we obtain

$$\#\{[L] \in \mathrm{Pic}(X) \mid ([L], D) \in \tilde{P}_N \text{ and } \gamma_{([L],D)} = g+1\} \geq N^{2g} - C(g)N^{2g-1} > 0,$$

where the last inequality comes from the assumption $f > \log_p(C(g)+1)$. This completes the proof. □

Remark (5.6). A similar technique as in the proof of (5.4) gives an alternative proof of (4.1). More precisely, fix an algebraic closure $\overline{\mathbb{F}}_p$ of the prime field $\mathbb{F}_p$, and put

$$\gamma^{\max} \overset{\text{def}}{=} \max\{\gamma_\chi(H^1_{\text{ét}}(X_{\mathrm{Ker}(\chi)}, \mathbb{F}_p)) \mid \chi \in \mathrm{Hom}(\pi_1^{\mathrm{t}}(U), \overline{\mathbb{F}}_p^{\times}),\ \chi \neq 1\}.$$

(For the sake of convenience, we shall define $\max \varnothing = -1$.) Then:

CLAIM (5.7). We have

$$\gamma^{\max} = g + n - 2 + b^{(2)}.$$

If we assume (5.7),

$$g = b^{(1)} - \gamma^{\max} - 1,\ n' \stackrel{\text{def}}{=} n + b^{(2)} = 2\gamma^{\max} - b^{(1)} + 3$$

can be recovered group-theoretically. Moreover, to recover n (assuming $b^{(1)} > 0$), we have only to note that

$$n = \begin{cases} n', & \text{if } n'(m) > 1, \\ 0, & \text{if } n'(m) \leq 1, \end{cases}$$

where m is an arbitrary natural number > 1 prime to p and $n'(m)$ is the invariant n' for the curve $U(m)$. (See the paragraph preceding (4.13).)

For the proof of (5.7), first, the inequality $\gamma^{\max} \leq g + n - 2 + b^{(2)}$ follows from (3.7) (together with (3.6) and (4.7)). For the opposite inequality, let f be a natural number $> \max(n-1, \log_p(C(g)+1))$ and put $N = p^f - 1$. Write the set S of cardinality n as $\{P_{-1}, P_0, P_1, \ldots, P_{n-2}\}$ and define $D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]$ by

$$D \stackrel{\text{def}}{=} \sum_{i=-1}^{n-2} n_i P_i,\ n_i = \begin{cases} \sum_{j=0}^{n-2} p^j, & \text{if } i = -1, \\ N - p^i, & \text{if } i = 0, 1, \ldots, n-2. \end{cases}$$

($D = 0$ for $n \leq 1$.) Then, we see that D satisfies (2.14) (with $s = n - 1 + b^{(2)}$). Now, as in the proof of (3.12), we deduce that

$$\begin{aligned} &\#\{[L] \in \mathrm{Pic}(X) \mid ([L], D) \in \tilde{P}_N \text{ and } \gamma_{([L],D)} = g + n - 2 + b^{(2)}\} \\ &\geq N^{2g} - C(g) N^{2g-1} > 0, \end{aligned}$$

where the last inequality comes from the assumption $f > \log_p(C(g)+1)$. This completes the proof.

(C) The genus 0 case. By means of the above results, we can prove that the isomorphism class of the scheme U can be recovered group-theoretically from the tame fundamental group $\pi_1^{\mathrm{t}}(U)$ in the case where $g = 0$ and $k = \overline{\mathbb{F}}_p$. More precisely, we have:

THEOREM (5.8). *Let k be an algebraically closed field of characteristic > 0 and F the algebraic closure of $\mathbb{F}_p$ in k. Let U be a smooth, connected curve over k. For each given smooth, connected curve U_0 over F whose smooth compactification is of genus 0 and whose number of punctures is greater than 1, we can detect whether U is isomorphic to $U_0 \otimes_F k$ as a scheme or not, group-theoretically from $\pi_1^{\mathrm{t}}(U)$.*

COROLLARY (5.9). *For each $i = 1, 2$, let k_i be an algebraically closed field of characteristic > 0 and U_i a smooth, connected curve over k_i. Let (g_i, n_i) denote (g, n) for U_i. Assume $k_1 \simeq k_2$. For some $i = 1, 2$, assume that $g_i = 0$, $n_i > 1$,*

and either (a) U_i *is defined over* F_i, *the algebraic closure of* $\mathbb{F}_p$ *in* k_i *or* (b) $n_i \leq 4$. *Then* $\pi_1^{\mathrm{t}}(U_1)$ *and* $\pi_1^{\mathrm{t}}(U_2)$ *are isomorphic as topological groups if and only if* U_1 *and* U_2 *are isomorphic as schemes.*

Proof of (5.8) and (5.9). With (4.1), (5.2), (5.3), etc., the same proofs as those of [T2], Theorem 3.5 and Corollary 3.6 work for $\pi_1^{\mathrm{t}}(U)$. □

Appendix: Proof of (4.17)

First, we recall some notations in the text. Let k be an algebraically closed field of characteristic $p > 0$, and let U be a smooth, connected curve over k. We denote by X the smooth compactification of U and put $S = X - U$. We define non-negative integers g and n to be the genus of X and the cardinality of the point set S, respectively. We put

$$g' \stackrel{\text{def}}{=} \begin{cases} g-1, & \text{if } n \leq 1, \\ g, & \text{if } n > 1. \end{cases}$$

Moreover, see Section 4 for the definition of the i-th Betti number $b^{(i)}$ of U.

In Section 4, we introduced the invariant γ_N^{av} of U for each natural number N prime to p, as a certain average of generalized Hasse–Witt invariants of N-cyclic étale coverings of U. Now, the following is the main result of this Appendix.

Theorem (A.1). *Assume* $b^{(1)} > 0$ (*or, equivalently,* $(g,n) \neq (0,0),(0,1)$). *Then* (4.17) *holds, that is, we have*

$$\limsup_{\substack{N \to \infty \\ p \nmid N}} \gamma_N^{\mathrm{av}} \leq g'.$$

We devote the rest of this Appendix to proving (A.1).

Let N be a natural number prime to p. Recall that for each divisor D in $(\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0$, $s(D) \stackrel{\text{def}}{=} \deg(D)/N$ is an integer with $0 \leq s(D) \leq n - 1 + b^{(2)}$. Moreover, for each integer a, we denote by $D(a)$ the element of $(\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0$ that is equivalent to aD modulo N. Let f be the order of $p \bmod N$ in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^{\times}$. We put

$$M_N \stackrel{\text{def}}{=} \#\{D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0 \mid s(D(p^j)) \leq 1 \text{ for some } j = 0, 1, \ldots f-1\}$$

and $E_N \stackrel{\text{def}}{=} \#((\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0) - M_N = N^{n-1+b^{(2)}} - M_N$. ($M$ and E mean "main term" and "error term".)

Now, we have the following:

Lemma (A.2). (i) *If* $n \leq 1$, *we have*

$$\gamma_N^{\mathrm{av}} \leq g - 1 + \frac{1}{N^{b^{(1)}}}.$$

(ii) *If* $n > 1$, *we have*

$$\gamma_N^{\mathrm{av}} \leq g + (b^{(1)} - 1)\frac{E_N}{N^{n-1}}.$$

PROOF. (i) Just the same as the first half of the proof of (4.9)(i).

(ii) Let $[V]$ be an element of $H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)$, and $([L], D)$ the element of $\tilde{P}_N$ corresponding to $[V]$. (See Section 3, especially (3.5) and paragraphs preceding it.) Then, as in the proof of (3.16), the remark just before the definition of $\gamma_{[V],i}$ (at the beginning of Section 3) and (3.8) imply

$$\gamma_{[V],1} = \gamma_{[V],p^j} = \gamma_{([L(p^j)],D(p^j))}$$

for each i. So, if $s(D(p^j)) \leq 1$ for some $j = 0, 1, \ldots, f-1$, we have $\gamma_{[V],1} \leq g$, as in (3.7). From this, we obtain

$$\sum_{[V] \in H^1_{\text{ét}}(U, \boldsymbol{\mu}_N)} \gamma_{[V],1} \leq gN^{2g}M_N + (g+n-2)N^{2g}E_N = gN^{b^{(1)}} + (n-2)N^{2g}E_N$$

by (3.4) and (3.7). Thus we have

$$\gamma_N^{\text{av}} \leq g + (n-2)\frac{E_N}{N^{n-1}} \leq g + (b^{(1)} - 1)\frac{E_N}{N^{n-1}},$$

as desired. □

(A.2)(i) settles the proof of (A.1) for $n \leq 1$, while (A.2)(ii) reduces the proof of (A.1) for $n > 1$ to

$$E_N = o(N^{n-1}), \quad \text{that is,} \quad \lim_{\substack{N \to \infty \\ p \nmid N}} \frac{E_N}{N^{n-1}} = 0. \tag{A.3}$$

Note that (A.3) depends only on the finite set S, so it no longer involves the geometry of U.

To prove (A.3), we need some knowledge of the theory of uniform distribution modulo 1, which we shall recall here. (For more details, see [KN].)

DEFINITION. (i) $I \overset{\text{def}}{=} [0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$. For each $x \in \mathbb{R}$, we denote by $\{x\}$ the fractional part $x - [x] \in I$ of x.

(ii) Let s be a positive integer. Let $\mathbf{a} = (a_1, \ldots, a_s)$ and $\mathbf{b} = (b_1, \ldots, b_s)$ be elements of $\mathbb{R}^s$. We say that $\mathbf{a} < \mathbf{b}$ (resp. $\mathbf{a} \leq \mathbf{b}$) if $a_i < b_i$ (resp. $a_i \leq b_i$) for each $i = 1, \ldots, s$. We put

$$[\mathbf{a}, \mathbf{b}) \overset{\text{def}}{=} \{\mathbf{x} \in \mathbb{R}^s \mid \mathbf{a} \leq \mathbf{x} < \mathbf{b}\}.$$

If $\mathbf{a} \leq \mathbf{b}$, the Lebesgue measure $\lambda([\mathbf{a}, \mathbf{b}))$ of $[\mathbf{a}, \mathbf{b})$ is given by $(b_1 - a_1) \ldots (b_s - a_s)$. Note that $I^s = [\mathbf{0}, \mathbf{1})$, where $\mathbf{0} = (0, \ldots, 0), \mathbf{1} = (1, \ldots, 1)$.

For each $\mathbf{x} = (x_1, \ldots, x_s) \in \mathbb{R}^s$, we put

$$\{\mathbf{x}\} \overset{\text{def}}{=} (\{x_1\}, \ldots, \{x_s\}),$$
$$\|\mathbf{x}\| \overset{\text{def}}{=} \max_{i=1,\ldots,s} |x_i|,$$
$$r(\mathbf{x}) \overset{\text{def}}{=} \prod_{\substack{i=1,\ldots,s \\ x_i \neq 0}} |x_i| \quad (r(\mathbf{0}) = 1).$$

For each $\mathbf{x} = (x_1, \ldots, x_s), \mathbf{y} = (y_1, \ldots, y_s) \in \mathbb{R}^s$, we put

$$\langle \mathbf{x}, \mathbf{y} \rangle \stackrel{\text{def}}{=} x_1 y_1 + \ldots + x_s y_s.$$

(iii) Let $\mathbf{x}_1, \ldots, \mathbf{x}_M$ be a sequence of length M of elements of $\mathbb{R}^s$. For each subset E of I^s, put

$$A(E; M; \mathbf{x}_1, \ldots, \mathbf{x}_M) \stackrel{\text{def}}{=} \#\{j = 1, \ldots, M \mid \{\mathbf{x}_j\} \in E\}.$$

Moreover, we define the discrepancy $\mathcal{D}_M$ of the sequence $\mathbf{x}_1, \ldots, \mathbf{x}_M$ by

$$\mathcal{D}_M = \mathcal{D}_M(\mathbf{x}_1, \ldots, \mathbf{x}_M) \stackrel{\text{def}}{=} \sup_J \left| \frac{A(J; M; \mathbf{x}_1, \ldots, \mathbf{x}_M)}{M} - \lambda(J) \right|,$$

where J runs over the subsets of I^s in the form $[\mathbf{a}, \mathbf{b})$ with $\mathbf{a}, \mathbf{b} \in \mathbb{R}^s$, $\mathbf{0} \leq \mathbf{a} < \mathbf{b} \leq \mathbf{1}$. (Observe that $0 \leq \mathcal{D}_M \leq 1$.)

Now, we can state the following higher-dimensional version of LeVeque's inequality, due to Stegbuchner.

THEOREM (STEGBUCHNER [S]). *Let $\mathbf{x}_1, \ldots, \mathbf{x}_M$ be a sequence of length M of elements of $\mathbb{R}^s$. Then*

$$\mathcal{D}_M(\mathbf{x}_1, \ldots, \mathbf{x}_M) \leq \left(C_s \sum_{\mathbf{h} \in \mathbb{Z}^s - \{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2} \left| \frac{1}{M} \sum_{j=1}^{M} e^{2\pi i \langle \mathbf{h}, \mathbf{x}_j \rangle} \right|^2 \right)^{1/(s+2)},$$

where C_s is a positive constant depending only on s. More precisely, we may take $C_s = s^{2(s+2)} 2^s 9^{s^2+3s+1}$. □

For various improvements of the constant C_s, see, e.g., [GT], Theorem 3 and [DT], Theorem 1.28.

As in the proof of (3.18)(ii), we choose any $Q \in S$ and put $S' = S - \{Q\}$, whose cardinality is $n' \stackrel{\text{def}}{=} n - 1 (> 0)$. The projection $(\mathbb{Z}/N\mathbb{Z})^\sim[S]^0 \to (\mathbb{Z}/N\mathbb{Z})^\sim[S'], D \mapsto D'$ is bijective. For each $a \in \mathbb{Z}$, we have $D(a)' = D'(a)$. Moreover, we see that

$$s(D) = \frac{1}{N} \deg(D) = \left\lceil \frac{1}{N} \deg(D') \right\rceil,$$

where $\lceil x \rceil$ denotes the smallest integer not less than x. Therefore, we have

$$s(D) \leq 1 \iff \deg(D') \leq N.$$

Taking S' as a basis, we may identify $(\mathbb{Z}/N\mathbb{Z})^\sim[S'] = ((\mathbb{Z}/N\mathbb{Z})^\sim)^{n'} \subset \mathbb{Z}^{n'}$.

Then, for each $D \in (\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0$, we can apply Stegbuchner's theorem to $s = n'$, $M = f$, and $\mathbf{x}_j = D(p^{j-1})'/N$ and obtain

$$\begin{aligned}\mathcal{D}_f(D) &\overset{\text{def}}{=} \mathcal{D}_f\left(\frac{D(p^0)'}{N}, \ldots, \frac{D(p^{f-1})'}{N}\right)\\ &\leq \left(C_{n'} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2}\left|\frac{1}{f}\sum_{j=0}^{f-1} e^{2\pi i\langle \mathbf{h}, \frac{D(p^j)'}{N}\rangle}\right|^2\right)^{1/(n'+2)}\\ &\leq \left(C_{n'} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2}\left|\frac{1}{f}\sum_{j=0}^{f-1} e^{2\pi i\frac{p^j\langle \mathbf{h}, D'\rangle}{N}}\right|^2\right)^{1/(n'+2)}.\end{aligned}$$

So

$$\begin{aligned}\sum_{D\in(\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0} \mathcal{D}_f(D)^{n'+2} &\leq C_{n'} \sum_{D'\in((\mathbb{Z}/N\mathbb{Z})^{\sim})^{n'}} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2}\left|\frac{1}{f}\sum_{j=0}^{f-1} e^{2\pi i\frac{p^j\langle \mathbf{h}, D'\rangle}{N}}\right|^2\\ &= C_{n'} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2} \sum_{D'\in((\mathbb{Z}/N\mathbb{Z})^{\sim})^{n'}} \left|\frac{1}{f}\sum_{j=0}^{f-1} e^{2\pi i\frac{p^j\langle \mathbf{h}, D'\rangle}{N}}\right|^2.\end{aligned}$$

Here, we have

$$\begin{aligned}\left|\frac{1}{f}\sum_{j=0}^{f-1} e^{2\pi i\frac{p^j\langle \mathbf{h}, D'\rangle}{N}}\right|^2 &= \left(\frac{1}{f}\sum_{j=0}^{f-1} e^{2\pi i\frac{p^j\langle \mathbf{h}, D'\rangle}{N}}\right)\overline{\left(\frac{1}{f}\sum_{j=0}^{f-1} e^{2\pi i\frac{p^j\langle \mathbf{h}, D'\rangle}{N}}\right)}\\ &= \frac{1}{f^2}\sum_{j,j'=0}^{f-1} e^{2\pi i\frac{(p^j-p^{j'})\langle \mathbf{h}, D'\rangle}{N}}.\end{aligned}$$

Now, since

$$\chi_{\mathbf{h},j,j'} : D' \bmod N \mapsto e^{2\pi i\frac{(p^j-p^{j'})\langle \mathbf{h}, D'\rangle}{N}}$$

is a character of the abelian group $(\mathbb{Z}/N\mathbb{Z})^{n'}$, we have

$$\sum_{D'\in((\mathbb{Z}/N\mathbb{Z})^{\sim})^{n'}} \chi_{\mathbf{h},j,j'}(D') = \begin{cases} 0, & \text{if } \chi_{\mathbf{h},j,j'} \neq 1,\\ N^{n'}, & \text{if } \chi_{\mathbf{h},j,j'} = 1.\end{cases}$$

Moreover, we have

$$\chi_{\mathbf{h},j,j'} = 1 \iff (p^j - p^{j'})\mathbf{h} \equiv \mathbf{0} \pmod N \iff f_{\mathbf{h}} \mid (j - j').$$

Here, $f_{\mathbf{h}}$ is the order of $p \bmod N_{\mathbf{h}}$ in the multiplicative group $(\mathbb{Z}/N_{\mathbf{h}}\mathbb{Z})^{\times}$, where $N_{\mathbf{h}}$ is the order of $\mathbf{h} \bmod N \in (\mathbb{Z}/N\mathbb{Z})^{n'}$. Thus, in summary, we get

$$\sum_{D\in(\mathbb{Z}/N\mathbb{Z})^{\sim}[S]^0} \mathcal{D}_f(D)^{n'+2}$$

$$\begin{aligned}
&\leq C_{n'} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2}\frac{1}{f^2}\sum_{j,j'=0}^{f-1}\sum_{D'\in((\mathbb{Z}/N\mathbb{Z})^\sim)^{n'}} \chi_{\mathbf{h},j,j'}(D')\\
&= C_{n'} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2}\frac{1}{f^2}\#(\{(j,j') \mid j,j'=0,\dots,f-1, f_{\mathbf{h}} \mid (j-j')\})N^{n'}\\
&= C_{n'} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2}\frac{1}{f^2}\frac{f^2}{f_{\mathbf{h}}}N^{n'}\\
&= C_{n'}N^{n'} \sum_{\mathbf{h}\in\mathbb{Z}^{n'}-\{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2 f_{\mathbf{h}}}.
\end{aligned}$$

Taking a positive integer K (which we fix later), we divide the last infinite sum into the sum of the infinite sum with $\|\mathbf{h}\| > K$ and the finite sum with $\|\mathbf{h}\| \leq K$. For the former, we have

$$\begin{aligned}
\sum_{\|\mathbf{h}\|>K}\frac{1}{r(\mathbf{h})^2 f_{\mathbf{h}}} &\leq \sum_{\|\mathbf{h}\|>K}\frac{1}{r(\mathbf{h})^2}\\
&\leq \sum_{i=1}^{n'}\sum_{\mathbf{h}\text{ s.t. }|h_i|>K}\frac{1}{r(\mathbf{h})^2}\\
&= \sum_{i=1}^{n'}\left(\sum_{|h_i|>K}\frac{1}{|h_i|^2}\right)\prod_{j\neq i}\left(\sum_{h_j\in\mathbb{Z}}\frac{1}{\max(|h_j|,1)^2}\right)\\
&\leq \sum_{i=1}^{n'}\left(2\int_K^\infty\frac{dx}{x^2}\right)(1+2\zeta(2))^{n'-1}\\
&= 2n'(1+2\zeta(2))^{n'-1}\frac{1}{K}.
\end{aligned}$$

For the latter, we need an estimate of $f_{\mathbf{h}}$. Since $N \mid N_{\mathbf{h}}\mathbf{h}$, we have $N_{\mathbf{h}}\|\mathbf{h}\| \geq N$, unless $\mathbf{h} = \mathbf{0}$. So, if $\|\mathbf{h}\| \leq K$ and $\mathbf{h} \neq \mathbf{0}$, we have $N_{\mathbf{h}} \geq N/K$. On the other hand, since $N_{\mathbf{h}} \mid p^{f_{\mathbf{h}}} - 1 < p^{f_{\mathbf{h}}}$, we have $f_{\mathbf{h}} \geq \log(N_{\mathbf{h}})/\log(p)$. These two inequalities imply

$$f_{\mathbf{h}} \geq \frac{\log(N/K)}{\log(p)}.$$

Therefore, we have (assuming $N/K > 1$)

$$\begin{aligned}
\sum_{0<\|\mathbf{h}\|\leq K}\frac{1}{r(\mathbf{h})^2 f_{\mathbf{h}}} &\leq \frac{\log(p)}{\log(N/K)}\sum_{0<\|\mathbf{h}\|\leq K}\frac{1}{r(\mathbf{h})^2}\\
&\leq \frac{\log(p)}{\log(N/K)}\{(1+2\zeta(2))^{n'}-1\}.
\end{aligned}$$

Now, fix any real number δ with $0 < \delta < 1$ and put $K = [N^\delta]$. Then we have

$$\frac{1}{K} \leq \frac{1}{N^\delta - 1} \text{ and } \frac{1}{\log(N/K)} \leq \frac{1}{\log(N/N^\delta)} = \frac{1}{(1-\delta)\log(N)}.$$

Thus we conclude that

$$\sum_{\mathbf{h} \in \mathbb{Z}^{n'} - \{\mathbf{0}\}} \frac{1}{r(\mathbf{h})^2 f_{\mathbf{h}}} \leq 2n'(1 + 2\zeta(2))^{n'-1} \frac{1}{N^\delta - 1} + \frac{\log(p)\{(1 + 2\zeta(2))^{n'} - 1\}}{(1-\delta)\log(N)}.$$

From this, we finally obtain

$$\sum_{D \in (\mathbb{Z}/N\mathbb{Z})^\sim[S]^0} \mathcal{D}_f(D)^{n'+2} \leq \left(c_1(n') \frac{1}{N^\delta - 1} + c_2(n', p, \delta) \frac{1}{\log(N)} \right) N^{n'},$$

where $c_1(n')$ (resp. $c_2(n', p, \delta)$) is a positive constant depending only on n' (resp. n', p, and δ).

On the other hand, let D be an element of $(\mathbb{Z}/N\mathbb{Z})^\sim[S]^0$ such that $s(D(p^j)) > 1$ for all $j = 0, 1, \ldots f-1$. Then, in particular, $\frac{D(p^j)'}{N} \notin [0, 1/n')^{n'}$ for all such j. So, by the definition of discrepancy, we have

$$\mathcal{D}_f(D) \geq \lambda([0, 1/n')^{n'}) = 1/(n')^{n'}.$$

From this, we obtain

$$\sum_{D \in (\mathbb{Z}/N\mathbb{Z})^\sim[S]^0} \mathcal{D}_f(D)^{n'+2} \geq c_3(n') E_N,$$

where $c_3(n') = 1/(n')^{n'(n'+2)}$ is a positive constant depending only on n'.

Now, we can conclude that

$$0 \leq \frac{E_N}{N^{n'}} \leq d_1(n') \frac{1}{N^\delta - 1} + d_2(n', p, \delta) \frac{1}{\log(N)},$$

where $d_1(n') = c_1(n')/c_3(n')$ and $d_2(n', p, \delta) = c_2(n', p, \delta)/c_3(n')$ are positive constants independent of N. Since $\delta > 0$, this implies (A.3).

This completes the proof of (A.1).

References

[B] I. Bouw, "Tame covers of curves: p-ranks and fundamental groups", thesis, Univ. Utrecht, 1998.

[BH] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, Cambridge, 1993.

[DT] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Lecture Notes in Mathematics **1651**, Springer, Berlin, 1997.

[E] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, New York, 1994.

[EGA4] A. Grothendieck, "Éléments de Géométrie Algébrique IV: Étude locale des schémas et des morphismes de schémas", *Publications Mathématiques de l'IHES* **20, 24, 28, 32,** 1964–1967.

[FJ] M. D. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3. Folge) **11**, Springer, Berlin and New York, 1986.

[GT] P. J. Grabner and R. F. Tichy, "Remark on an inequality of Erdös–Turán–Koksma", *Anz. Österreich. Akad. Wiss. Math.-Natur. Kl.* **127** (1990), 15–22.

[GM] A. Grothendieck and J. P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Mathematics **208**, Springer, Berlin and New York, 1971.

[Ka] H. Katsurada, "On generalized Hasse–Witt invariants and unramified Galois extensions of an algebraic function field", *J. Math. Soc. Japan* **31** (1979), 101–125.

[KN] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley, New York-London-Sydney, 1974.

[Na] S. Nakajima, "On generalized Hasse–Witt invariants of an algebraic curve", pp. 69–88 in *Galois groups and their representations* (Nagoya, 1981), Advanced Studies in Pure Mathematics **2**, edited by Y. Ihara, North-Holland, Amsterdam, and Kinokuniya, Tokyo, 1983.

[Mac] F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge University Press, Cambridge, 1916.

[Mad] D. A. Madore, "Theta divisors and the Frobenius morphism", pp. 279–289 in *Courbes semi-stables et groupe fondamental en géométrie algébrique* (Luminy, 1998) Progr. Math. **187**, edited by J.-B. Bost, F. Loeser and M. Raynaud, Birkhäuser, Basel, 2000.

[Mi1] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton Univ. Press, Princeton, New Jersey, 1980.

[Mi2] ———, "Jacobian varieties", pp. 167–212 in *Arithmetic geometry* (Storrs, 1984), edited by G. Cornell and J. H. Silverman, Springer, New York-Berlin, 1986.

[Mu] D. Mumford, *Abelian varieties*, Oxford University Press, London, 1970.

[R1] M. Raynaud, "Sections des fibrés vectoriels sur une courbe", *Bull. Soc. math. France* **110** (1982), 103–125.

[R2] ———, "Revêtements des courbes en caractéristique $p > 0$ et ordinarité", *Compositio Math.* **123** (2000), 73–88.

[S] H. Stegbuchner, "Eine mehrdimensionale Version der Ungleichung von LeVeque", *Monatsh. Math.* **87** (1979), 167–169.

[SGA1] A. Grothendieck and Mme. M. Raynaud, *Revêtements étales et groupe fondamental, Séminaire de Géometrie Algébrique du Bois Marie* 1960–61 (SGA 1), Lecture Notes in Mathematics **224**, Springer, Berlin and New York, 1971.

[SGA6] P. Berthelot, A. Grothendieck and L. Illusie, *Théorie des intersections et théorème de Riemann–Roch, Séminaire de Géométrie Algébrique du Bois Marie* 1966–1967 (SGA 6), Lecture Notes in Mathematics **225**, Springer, Berlin and New York, 1971.

[SGA7I] A. Grothendieck, M. Raynaud and D. S. Rim, *Groupes de monodromie en géométrie algébrique, Séminaire de Géométrie Algébrique du Bois Marie* 1967–1969 (SGA 7I), Lecture Notes in Mathematics **288**, Springer, Berlin and New York, 1972.

[T1] A. Tamagawa, "The Grothendieck conjecture for affine curves", *Compositio Math.* **109** (1997), 135–194.

[T2] ———, "On the fundamental groups of curves over algebraically closed fields of characteristic > 0", *Internat. Math. Res. Notices* (1999), no. 16, 853–873.

[T3] ———, "Fundamental groups and geometry of curves in positive characteristic", pp. 297–333 in *Arithmetic fundamental groups and noncommutative algebra* (Berkeley, 1999), Proceedings of Symposia in Pure Mathematics **70**, edited by M. D. Fried and Y. Ihara, American Mathematical Society, Providence, 2002.

[Y] Y. Yoshino, *Cohen–Macaulay modules over Cohen–Macaulay rings*, London Mathematical Society Lecture Note Series **146**, Cambridge University Press, Cambridge, 1990.

Akio Tamagawa
Research Institute for Mathematical Sciences
Kyoto University
Kyoto 606-8502
Japan
tamagawa@kurims.kyoto-u.ac.jp