JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Evangelia GAZAKI et Toshiro HIRANOUCHI

Abelian geometric fundamental groups for curves over a p-adic field

Tome 35, nº 3 (2023), p. 905-946.

https://doi.org/10.5802/jtnb.1269

Journal de Théorie des Nombres
de Bordeaux **35** (2023), 905–946

Abelian geometric fundamental groups for curves over a p-adic field

par Evangelia GAZAKI et Toshiro HIRANOUCHI

Résumé. Pour une courbe X sur un corps p-adique k, nous étudions le groupe fondamental géométrique abélien $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ de X en utilisant la théorie du corps de classes de X due à S. Bloch et S. Saito. En particulier, nous étudions un sous-groupe de $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ qui classifie les revêtements géométriques et abéliens de X admettant une ramification au-dessus de la fibre spéciale du modèle de X. En supposant que X a un point rationnel sur k, X a bonne réduction et sa jacobienne a bonne réduction ordinaire, nous donnons un encadrement de ce sous-groupe de $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$.

Abstract. For a curve X over a p-adic field k, using the class field theory of X due to S. Bloch and S. Saito we study the abelian geometric fundamental group $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ of X. In particular, we investigate a subgroup of $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ which classifies the geometric and abelian coverings of X which allow possible ramification over the special fiber of the model of X. Under the assumptions that X has a k-rational point, X has good reduction and its Jacobian variety has good ordinary reduction, we give some upper and lower bounds of this subgroup of $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$.

1. Introduction

Let k be a *p-adic field*, that is, a finite extension of $\mathbb{Q}_p$, with residue field $\mathbb{F}_k$. In this note, we investigate the abelian fundamental group $\pi_1^{\mathrm{ab}}(X)$ for a projective smooth and geometrically connected curve X over k. The structure map $X \to \mathrm{Spec}(k)$ induces the short exact sequence

$$0 \longrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \longrightarrow \pi_1^{\mathrm{ab}}(X) \longrightarrow G_k^{\mathrm{ab}} = \pi_1^{\mathrm{ab}}(\mathrm{Spec}(k)) \longrightarrow 0, \tag{1.1}$$

where $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ is defined by the exactness and is referred to as the *geometric fundamental group* of X. Local class field theory describes G_k^{ab} sufficiently to allow us to focus on $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$. Now, we restrict our attention to the case where X has *good reduction* in the sense that the special fiber $\overline{X} := \mathscr{X} \otimes_{\mathcal{O}_k} \mathbb{F}_k$ of a regular model $\mathscr{X}$ over $\mathcal{O}_k$ of X is a smooth curve over $\mathbb{F}_k$, and also X has a k-rational point. The short exact sequence (1.1) splits.

Manuscrit reçu le 9 septembre 2022, accepté le 28 avril 2023.

2020 *Mathematics Subject Classification.* 11G45, 11G10, 11G20.

Mots-clefs. Class field theory, Fundamental groups, and Elliptic curves.

The first author was partially supported by the NSF grant DMS-2001605. The second author was supported by JSPS KAKENHI Grant Number 20K03536.

There is a map called the *specialization map* $\pi_1^{\mathrm{ab}}(X) \overset{\mathrm{sp}}{\to} \pi_1^{\mathrm{ab}}(\overline{X})$ (cf. (2.6)) and this induces

$$(1.2) \qquad 0 \longrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \longrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \xrightarrow{\mathrm{sp}} \pi_1^{\mathrm{ab}}(\overline{X})^{\mathrm{geo}} \longrightarrow 0,$$

where $\pi_1^{\mathrm{ab}}(\overline{X})^{\mathrm{geo}} := \mathrm{Ker}(\pi_1^{\mathrm{ab}}(\overline{X}) \to G_{\mathbb{F}_k})$ is the geometric fundamental group of $\overline{X}$ and $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ is defined by the exactness again. The fundamental group $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ classifies the geometric coverings of X which are *completely ramified* over the special fiber $\overline{X}$ (for the precise description and definition, see Section 2). The classical class field theory (for the curve $\overline{X}$ over the finite field $\mathbb{F}_k$) says that the reciprocity map induces an isomorphism $\rho_{\overline{X}} \colon \bar{J} \overset{\simeq}{\to} \pi_1^{\mathrm{ab}}(\overline{X})^{\mathrm{geo}}$, where $\bar{J} = \mathrm{Jac}(\overline{X})$ is the Jacobian variety of $\overline{X}$. Our main result describes the structure of the remaining part $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ by using an invariant related to the Jacobian variety $J = \mathrm{Jac}(X)$ of X.

Theorem 1.1 (cf. Corollary 4.1)**.** *Let X be a projective smooth curve over k with $X(k) \neq \emptyset$, and $J = \mathrm{Jac}(X)$ the Jacobian variety of X. We assume that X has good reduction, and the Jacobian variety $\bar{J} = \mathrm{Jac}(\overline{X})$ of $\overline{X}$ is an ordinary abelian variety. Then, we have surjective homomorphisms*

$$(\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g} \twoheadrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \twoheadrightarrow (\mathbb{Z}/p^{N_J})^{\oplus g},$$

where $N_J = \max\{n \mid J[p^n] \subset J(k)\}, M^{\mathrm{ur}} = \max\{m \mid \mu_{p^m} \subset k^{\mathrm{ur}}\}$, and $g = \dim J$. Here, we denoted by k^{ur} the maximal unramified extension of k and μ_{p^m} is the group of p^m-th roots of unity.

Remark 1.2. Put $M = \max\{m \mid \mu_{p^m} \subset k\}$. In general, we have inequalities $N_J \leq M \leq M^{\mathrm{ur}}$. Here, the first inequality follows from the Weil pairing. For the later inequality $M \leq M^{\mathrm{ur}}$, if we assume $\mu_p \subset k$, that is, $M \geq 1$ and put $e_0(k) = e_k/(p-1)$, where e_k is the absolute ramification index of k, then $M = M^{\mathrm{ur}}$ if and only if $\zeta_{p^M} \notin \mathrm{Im}(U_k^{pe_0(k)} \hookrightarrow k^\times \twoheadrightarrow k^\times/(k^\times)^p)$, where ζ_{p^M} is a primitive p^M-th root of unity, and $U_k^{pe_0(k)}$ is the higher unit group (see e.g., [19, Lemma 2.1.5]). For example, when the base field k is of the form $k = k_0(\zeta_{p^m})$ for some finite unramified extension $k_0/\mathbb{Q}_p$, we have $M = M^{\mathrm{ur}} = m$. If we additionally assume $N_J = M$ as we considered in [12] (we also give some elliptic curves satisfying this condition in Section 5), then the exact sequence (1.2) splits and we have $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \simeq (\mathbb{Z}/p^m)^{\oplus g}$. One can recover the main theorem in [12].

The above theorem enables us to construct an abelian geometric covering $\widetilde{X} \to X$ corresponding to $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ (Theorem 4.5) along the context of the geometric abelian class field theory (e.g., [33]). This can be regarded as an analogue of Yoshida's work on the modular curve $X_0(p)$ over $\mathbb{Q}_p$ ([42]). In Section 5, we give examples in genus 1, that is when $X = E$ is an elliptic curve with good ordinary reduction, to indicate that each one of the two bounds given in Theorem 1.1 can be achieved depending on the $\mathrm{Gal}(\overline{k}/k)$-action on the Tate module of X (cf. Theorem 5.3). This in particular shows that Theorem 1.1 is as general as it can be. We also consider an elliptic curve $X = E$ over k with good *supersingular reduction* and we give bounds for $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ of similar flavor as in Theorem 1.1.

Notation. Throughout this note, we use the following notation: We fix a finite extension k of $\mathbb{Q}_p$. For a finite extension K/k, we define

- O_K: the valuation ring of K with maximal ideal $\mathfrak{m}_K$,
- $\mathbb{F}_K = \mathcal{O}_K/\mathfrak{m}_K$: the residue field of K,
- $G_K := \mathrm{Gal}(\overline{k}/K)$: the absolute Galois group of K, and
- $U_K = \mathcal{O}_K^\times$: the unit group of $\mathcal{O}_K$.

For an abelian group G and $m \in \mathbb{Z}_{\geq 1}$, we write $G[m]$ and G/m for the kernel and cokernel of the multiplication by m on G respectively. We also denote by $G\{m\} := \bigcup_{n\geq 1} G[m^n]$ the m-primary part of G. For a profinite group G, and a G-module M, we denote by $M^G \subset M$ and $M \twoheadrightarrow M_G$ its G-invariant subgroup and G-coinvariant quotient, respectively. In this note, by a *variety* over k we mean an integral and separated scheme of finite type over k, and a *curve* over k is a variety over k with dimension 1.

Acknowledgements. The authors would like to give heartful thanks to Prof. Yoshiyasu Ozeki who allowed us to include his result on the invariants N_J and M^{ur} used in Theorem 1.1 (cf. Proposition 3.10). We would also like to thank Prof. Takao Yamazaki whose comments on the construction of the maximal covering in Section 4 were an enormous help to us. The authors thank the referee for careful reading, and many valuable suggestions to improve our manuscript.

2. Preliminaries

Finite by divisible. Following [28], we introduce the following notation:

Definition 2.1 ([28, Lemma 3.4.4])**.** An abelian group G is said to be *finite by divisible* if G has a decomposition $G \simeq F \oplus D$ for a finite group F and a divisible group D. In what follows, we often denote by G_{fin} and G_{div} the subgroups of G isomorphic to F and D respectively.

Lemma 2.2 ([28, Lemma 3.4.4])**.**

(i) *Let G be an abelian group. Then, G is finite by divisible if and only if $\varprojlim_{m\geq 1} G/m$ is finite. The last condition holds if G/m is finite for any $m \geq 1$, and its order is bounded independently of m.*

(ii) *If $G \to G'$ is a surjective homomorphism of abelian groups, and if G is finite by divisible, then so is G'.*

(iii) *Suppose that there is a short exact sequence* $0 \to G'' \to G \to G' \to 0$ *of abelian groups. If* G *is finite by divisible, and* G' *is finite, then* G'' *is also finite by divisible.*

Proof. The assertions (i), (ii) follow from [28, Lemma 3.4.4].

Let's now prove (iii). For any $m \geq 1$, consider the exact sequence

$$\mathrm{Tor}(G', \mathbb{Z}/m) \longrightarrow G''/m \longrightarrow G/m \longrightarrow G'/m \longrightarrow 0 \tag{2.1}$$

induced from the short exact sequence $0 \to G'' \to G \to G' \to 0$. Since G is finite by divisible, G/m is finite and its order is bounded independently of m. From $\mathrm{Tor}(G', \mathbb{Z}/m) = G'[m] \subset G'$ and G' is finite, both G'/m and $\mathrm{Tor}(G', \mathbb{Z}/m)$ are finite and their orders are bounded. From the exact sequence (2.1) the same holds for G''/m and hence G'' is finite by divisible from (i). □

Mackey products, and the Galois symbol map. We recall the definition and properties of Mackey functors following [28, (3.2)]. For properties of Mackey functors, see also [14, 15].

Definition 2.3 (cf. [28, Section 3])**.** A *Mackey functor* $\mathscr{M}$ (over k) (or a G_k*-modulation* in the sense of [25, Definition 1.5.10]) is a contravariant functor from the category of étale schemes over k to the category of abelian groups equipped with a covariant structure for finite morphisms such that $\mathscr{M}(X_1 \sqcup X_2) = \mathscr{M}(X_1) \oplus \mathscr{M}(X_2)$ and if the left diagram below is Cartesian, then the right becomes commutative:

$$\begin{tikzcd}
X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] & \mathscr{M}(X') \arrow[r, "{g'}_*"] & \mathscr{M}(X) \\
Y' \arrow[r, "g"] & Y & \mathscr{M}(Y') \arrow[r, "g_*"] \arrow[u, "f'^*"] & \mathscr{M}(Y). \arrow[u, "f^*"']
\end{tikzcd}$$

For a Mackey functor $\mathscr{M}$, we denote by $\mathscr{M}(K)$ its value $\mathscr{M}(\mathrm{Spec}(K))$ for a field extension K of k. For any finite extension $k \subset K \subset L$, the induced homomorphism from the canonical map $j\colon \mathrm{Spec}(L) \to \mathrm{Spec}(K)$ is denoted by $N_{L/K} := j_* : \mathscr{M}(L) \to \mathscr{M}(K)$ which is often referred as the *norm map*, and $\mathrm{Res}_{L/K} := j^* : \mathscr{M}(K) \to \mathscr{M}(L)$ is called the *restriction*.

Example 2.4.

(i) Let G be a commutative algebraic group over k. Then, the algebraic group G induces a Mackey functor by defining $G(K) = G(\mathrm{Spec}\, K)$ for K/k finite.

(ii) For a Mackey functor $\mathscr{M}$, and for $m \in \mathbb{Z}_{\geq 1}$, we define a Mackey functor $\mathscr{M}/m$ by

$$(\mathscr{M}/m)(K) := \mathscr{M}(K)/m$$

for any finite extension K/k.

The category of Mackey functors forms an abelian category with the following tensor product:

Definition 2.5 (cf. [14])**.** For Mackey functors $\mathscr{M}$ and $\mathscr{N}$, their *Mackey product* $\mathscr{M} \otimes \mathscr{N}$ is defined as follows: For any field extension k'/k,

$$(\mathscr{M} \otimes \mathscr{N})(k') := \left(\bigoplus_{K/k' \colon \text{finite}} \mathscr{M}(K) \otimes_{\mathbb{Z}} \mathscr{N}(K) \right) \Big/ (\mathrm{PF}),$$

where (PF) stands for the subgroup generated by elements of the following form:

(PF) For finite field extensions $k' \subset K \subset L$,

$N_{L/K}(x) \otimes y - x \otimes \mathrm{Res}_{L/K}(y)$ for $x \in \mathscr{M}(L)$ and $y \in \mathscr{N}(K)$, and

$x \otimes N_{L/K}(y) - \mathrm{Res}_{L/K}(x) \otimes y$ for $x \in \mathscr{M}(K)$ and $y \in \mathscr{N}(L)$.

For the Mackey product $\mathscr{M} \otimes \mathscr{N}$, we write $\{x, y\}_{K/k'}$ for the image of $x \otimes y \in \mathscr{M}(K) \otimes_{\mathbb{Z}} \mathscr{N}(K)$ in the product $(\mathscr{M} \otimes \mathscr{N})(k')$. For any finite field extension k'/k, the norm map $N_{k'/k} = j_* : (\mathscr{M} \otimes \mathscr{N})(k') \to (\mathscr{M} \otimes \mathscr{N})(k)$ is given by

$$N_{k'/k}(\{x, y\}_{K/k'}) = \{x, y\}_{K/k}. \tag{2.2}$$

Let G be a semi-abelian variety over k. For any $m \in \mathbb{Z}_{\geq 1}$, the connecting homomorphism associated to the short exact sequence $0 \to G[m] \to G \overset{m}{\to} G \to 0$ as G_k-modules gives, for each finite extension K/k,

$$\delta_G \colon G(K)/m \hookrightarrow H^1(K, G[m]) := H^1(G_K, G[m]), \tag{2.3}$$

which is often called the *Kummer map*.

Definition 2.6 (cf. [36, Proposition 1.5])**.** For semi-abelian varieties G_1 and G_2 over k, the *Galois symbol map*

$$s_m \colon (G_1 \otimes G_2)(k)/m \longrightarrow H^2(k, G_1[m] \otimes G_2[m])$$

is defined by the cup product and the corestriction: $s_m(\{x, y\}_{K/k}) = \mathrm{Cor}_{K/k}\,(\delta_{G_1}(x) \cup \delta_{G_2}(y))$. The map is well-defined by the functorial properties of Galois cohomology (cf. [25, Proposition 1.5.3 (iv)]).

For two semi-abelian varieties G_1, G_2 over k, the *Somekawa K-group* $K(k; G_1, G_2)$ attached to G_1, G_2 is a quotient of the Mackey product $(G_1 \otimes G_2)(k)$ (see [36] for the precise definition) by considering G_1, G_2 as Mackey functors (cf. Example 2.4). By definition, for every finite K/k there is a surjection, $(G_1 \otimes G_2)(K) \twoheadrightarrow K(K; G_1, G_2)$. The elements of $K(k; G_1, G_2)$ will also be denoted as linear combinations of symbols of the form $\{x_1, x_2\}_{K/k}$, where K/k is some finite extension and $x_i \in G_i(K)$ for $i = 1, 2$. The Galois symbol map $s_m : (G_1 \otimes G_2)(k)/m \to H^2(k, G_1[m] \otimes G_2[m])$ (Definition 2.6) factors through $K(k; G_1, G_2)$ and the induced map

$$s_m \colon K(k; G_1, G_2)/m \longrightarrow H^2(k, G_1[m] \otimes G_2[m])$$

is also called the *Galois symbol map.*

Geometric fundamental groups, and their "ramified parts". Let V be a projective and smooth variety over k. We assume that there exists a k-rational point $x \in V(k)$. From this assumption, the variety V is geometrically connected. The abelianization of the fundamental group $\pi_1(V)$ is denoted by $\pi_1^{\mathrm{ab}}(V)$. Since we always consider the abelian fundamental groups, we omit the geometric point. Furthermore, we say that $\varphi \colon W \to V$ is an *abelian covering* if φ is an étale covering (that is, finite and étale), and is Galois whose Galois group $\mathrm{Aut}(\varphi)$ is an abelian group. Let $k(V)$ be the function field of V. The map $\mathrm{Spec}(k(V)) \to V$ induces a surjective homomorphism

$$\mathrm{Gal}(k(V)^{\mathrm{ab}}/k(V)) \simeq \pi_1^{\mathrm{ab}}(\mathrm{Spec}(k(V))) \twoheadrightarrow \pi_1^{\mathrm{ab}}(V), \tag{2.4}$$

where $k(V)^{\mathrm{ab}}$ is the maximal abelian extension of $k(V)$ ([9, Exposé IX, Proposition 8.2]). Define the *maximal unramified extension* $k(V)^{\mathrm{ur,ab}}$ of $k(V)$ by the subfield of $k(V)^{\mathrm{ab}}$ generated by all finite extensions of $k(V)$ contained in $k(V)^{\mathrm{ab}}$ that are unramified over V. Here, a finite extension $F/k(V)$ is said to be *unramified over* V, if the normalization of V in F is unramified over V, or equivalently, étale over V. The kernel of the map (2.4) is $\mathrm{Gal}(k(V)^{\mathrm{ab}}/k(V)^{\mathrm{ur,ab}})$ and hence $\pi_1^{\mathrm{ab}}(V) \simeq \mathrm{Gal}(k(V)^{\mathrm{ur,ab}}/k(V))$. The structure map $V \to \mathrm{Spec}(k)$ induces a surjective homomorphism $\pi_1(V) \twoheadrightarrow \pi_1(\mathrm{Spec}(k)) = G_k$ ([9, Exposé IX, Théorème 6.1]). This map induces a short exact sequence

$$0 \longrightarrow \pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}} \longrightarrow \pi_1^{\mathrm{ab}}(V) \longrightarrow G_k^{\mathrm{ab}} \longrightarrow 0, \tag{2.5}$$

where $\pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}}$ is defined by the exactness and is called the *geometric fundamental group* of V. By the fixed k-rational point $x \in V(k)$, the above sequence splits. The fundamental group $\pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}}$ classifies (abelian) *geometric coverings* of X. Here, an abelian covering $\varphi \colon V' \to V$ is said to be *geometric* if the fiber $\varphi^{-1}(x) = V' \times_V x \to \mathrm{Spec}(k)$ of φ over x is *completely split*, in the sense that $\varphi^{-1}(x)$ is the sum of distinct $[k(V') : k(V)]$ k-rational points. (cf. [17, II Preliminaries]). More precisely, the geometric fundamental group $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ is written as

$$\pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}} \simeq \mathrm{Gal}(k(V)^{\mathrm{ur,ab}}/k(V)k^{\mathrm{ab}}) \simeq \mathrm{Gal}(k(V)^{\mathrm{geo}}/k(V)),$$

where $k(V)^{\mathrm{geo}}$ is the subfield of $k(V)^{\mathrm{ur,ab}}$ generated by all finite extensions of $k(V)$ contained in $k(V)^{\mathrm{ur,ab}}$ that are completely split over x. Here, a finite extension $k \subset F \subset k(V)^{\mathrm{ur,ab}}$ is said to be *completely split* over x if the normalization of V in F is completely split over x.

In the following, we assume that V has *good reduction*, that is, there exists a proper smooth model over $\mathcal{O}_k$ of V. We denote by $\overline{V} = \mathscr{V} \otimes_{\mathcal{O}_k} \mathbb{F}_k$ the special fiber of a smooth model $\mathscr{V}$ over $\mathcal{O}_k$ which is a smooth variety over the finite field $\mathbb{F}_k$. In this case, it is known that $\pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}}$ is finite ([43, Corollary 1.2], [27, Chapter 4]). By the valuative criterion for properness, the fixed rational point x gives rise to an $\mathcal{O}_k$-rational point of $\mathscr{V}$ and hence to an $\mathbb{F}_k$-rational point of $\overline{V}$ denoted by $\bar{x}$. In the same way as above, we have a split short exact sequence

$$0 \longrightarrow \pi_1^{\mathrm{ab}}(\overline{V})^{\mathrm{geo}} \longrightarrow \pi_1^{\mathrm{ab}}(\overline{V}) \longrightarrow G_{\mathbb{F}_k} \longrightarrow 0.$$

By [9, Exposé X, Théorèm 2.1], there is a canonical surjection

$$\mathrm{sp}\colon \pi_1^{\mathrm{ab}}(V) \longrightarrow \pi_1^{\mathrm{ab}}(\mathscr{V}) \simeq \pi_1^{\mathrm{ab}}(\overline{V}) \tag{2.6}$$

and this induces the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}} \arrow[r] \arrow[d, dashed, "\mathrm{sp}"] & \pi_1^{\mathrm{ab}}(V) \arrow[r] \arrow[d, two heads, "\mathrm{sp}"] & G_k^{\mathrm{ab}} \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & \pi_1^{\mathrm{ab}}(\overline{V})^{\mathrm{geo}} \arrow[r] & \pi_1^{\mathrm{ab}}(\overline{V}) \arrow[r] & G_{\mathbb{F}_k} \arrow[r] & 0.
\end{tikzcd}$$

As the horizontal sequences split, the specialization map $\mathrm{sp}\colon \pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}} \to \pi_1^{\mathrm{ab}}(\overline{V})^{\mathrm{geo}}$ on the geometric fundamental groups is surjective.

Definition 2.7 ([42, Definition 2.2])**.** We denote by $\pi_1^{\mathrm{ab}}(V)_{\mathrm{ram}}$ the kernel of the specialization map $\mathrm{sp}\colon \pi_1^{\mathrm{ab}}(V) \to \pi_1^{\mathrm{ab}}(\overline{V})$. In the same way, we define $\pi_1^{\mathrm{ab}}(V)_{\mathrm{ram}}^{\mathrm{geo}}$ by the kernel of $\mathrm{sp}\colon \pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}} \to \pi_1^{\mathrm{ab}}(\overline{V})^{\mathrm{geo}}$ on the geometric fundamental groups. The abelian coverings corresponding to $\pi_1^{\mathrm{ab}}(V)_{\mathrm{ram}}$ are said to be *completely ramified over* $\overline{V}$.

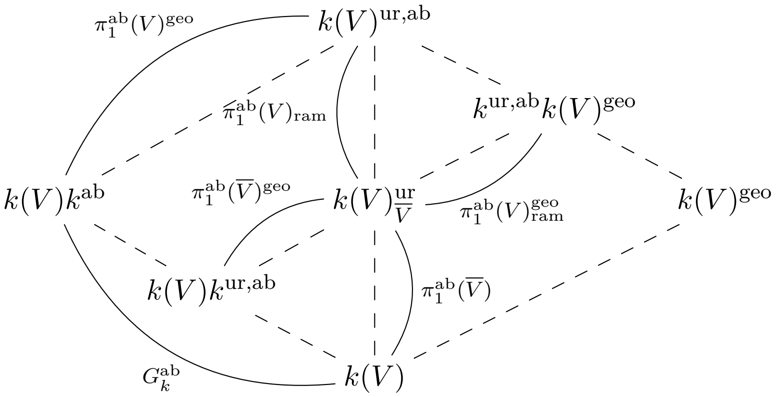
For the later use, we give a precise description of $\pi_1^{\mathrm{ab}}(V)_{\mathrm{ram}}$. First, we recall the construction of the map $\mathrm{sp}\colon \pi_1^{\mathrm{ab}}(V) \to \pi_1^{\mathrm{ab}}(\overline{V})$: For an étale covering $\bar{\varphi}\colon \overline{W} \to \overline{V}$, there exists a unique étale covering $\mathscr{W} \to \mathscr{V}$ such that its closed fiber is $\bar{\varphi}$ ([9, Exposé IX, Théorème 1.10]). By taking the generic fiber $\varphi\colon W \to V$ of $\mathscr{W} \to \mathscr{V}$, we obtain

$$\begin{tikzcd}
W \arrow[r] \arrow[d, "\varphi"'] & \mathscr{W} \arrow[d] & \overline{W} \arrow[l] \arrow[d, "\bar{\varphi}"] \\
V \arrow[r] & \mathscr{V} & \overline{V}. \arrow[l]
\end{tikzcd} \tag{2.7}$$

This induces the map $\mathrm{sp}\colon \pi_1^{\mathrm{ab}}(V) \to \pi_1^{\mathrm{ab}}(\overline{V})$.

Definition 2.8. For an abelian covering $\varphi\colon W \to V$ with Galois group $\mathrm{Aut}(\varphi) = G$, we say that $\varphi\colon W \to V$ is *unramified over* $\overline{V}$, if there exists an abelian covering $\bar{\varphi}\colon \overline{W} \to \overline{V}$ with $\mathrm{Aut}(\bar{\varphi}) \simeq G$ such that φ and $\bar{\varphi}$ fit into the diagram (2.7) as above.

We define $k(V)^{\mathrm{ur}}_{\overline{V}}$ to be the subfield of $k(V)^{\mathrm{ur,ab}}$ generated by all finite extensions of $k(V)$ contained in $k(V)^{\mathrm{ur,ab}}$ that are unramified over $\overline{V}$. Here, a finite field extension $F/k(V)$ is said to be *unramified over* $\overline{V}$ if the normalization of V in F is unramified over $\overline{V}$. We have $\pi_1^{\mathrm{ab}}(\overline{V}) \simeq \mathrm{Gal}(\mathbb{F}_k(\overline{V})^{\mathrm{ur,ab}}/\mathbb{F}_k(\overline{V})) \simeq \mathrm{Gal}(k(V)^{\mathrm{ur}}_{\overline{V}}/k(V))$. In particular, there is a one to one correspondence between the set of abelian coverings of V unramified over $\overline{V}$ and that of abelian coverings of $\overline{V}$. A diagram of fields and their Galois groups is


$\pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}}$
$k(V)^{\mathrm{ur,ab}}$
$\pi_1^{\mathrm{ab}}(V)_{\mathrm{ram}}$
$k^{\mathrm{ur,ab}}k(V)^{\mathrm{geo}}$
$k(V)k^{\mathrm{ab}}$
$\pi_1^{\mathrm{ab}}(\overline{V})^{\mathrm{geo}}$
$k(V)^{\mathrm{ur}}_{\overline{V}}$
$\pi_1^{\mathrm{ab}}(V)^{\mathrm{geo}}_{\mathrm{ram}}$
$k(V)^{\mathrm{geo}}$
$k(V)k^{\mathrm{ur,ab}}$
$\pi_1^{\mathrm{ab}}(\overline{V})$
G_k^{ab}
$k(V)$

(cf. The diagram of fields and Galois groups in [17, Introduction]). An abelian covering $\varphi\colon W \to V$ is completely ramified over $\overline{V}$ if and only if φ does not have a sub covering which is unramified over $\overline{V}$.

Class field theory for curves. Let X be a projective smooth *curve* over k with $X(k) \neq \emptyset$ and with good reduction. There exists a proper smooth model $\mathscr{X}$ over $\mathcal{O}_k$ of X whose closed fiber is denoted by $\overline{X} = X \otimes_{\mathcal{O}_k} \mathbb{F}_k$. Following [1], [31], we recall the class field theory for the curve X. The group $\mathrm{SK}_1(X)$ is defined by the cokernel of the tame symbol map

$$\mathrm{SK}_1(X) = \mathrm{Coker}\Big(\partial\colon K_2^M(k(X)) \longrightarrow \bigoplus_x k(x)^\times\Big),$$

where x runs through the set of closed points in X, $k(x)$ is the residue field at x, and $k(X)$ is the function field of X. The norm maps $N_{k(x)/k}\colon k(x)^\times \to k^\times$ for closed points x induce $N\colon \mathrm{SK}_1(X) \to k^\times$. Its kernel is denoted by $V(X)$. The reciprocity map $\sigma_X\colon \mathrm{SK}_1(X) \to \pi_1^{\mathrm{ab}}(X)$ is compatible with the reciprocity map $\rho_k\colon k^\times \to G_k^{\mathrm{ab}}$ of local class field theory as in the commutative diagram:

(2.8)
$$\begin{tikzcd}
0 \arrow[r] & V(X) \arrow[r] \arrow[d, dashed, "\tau_X"] & \mathrm{SK}_1(X) \arrow[r, "N"] \arrow[d, "\sigma_X"] & k^\times \arrow[d, "\rho_k"] & \\
0 \arrow[r] & \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \arrow[r] & \pi_1^{\mathrm{ab}}(X) \arrow[r] & G_k^{\mathrm{ab}} \arrow[r] & 0,
\end{tikzcd}$$

where the bottom horizontal sequence is induced from the structure map $X \to \mathrm{Spec}(k)$ (cf. (2.5)). The diagram above gives a map $\tau_X \colon V(X) \to \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ to describe the geometric fundamental group $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$. In fact, the above short exact sequences split from the assumption $X(k) \neq \emptyset$. The main theorem of the class field theory for X is the following:

Theorem 2.9 ([1], [31])**.** *The following statements hold for the reciprocity maps σ_X and τ_X.*

(i) *The reciprocity map σ_X has dense image in $\pi_1^{\mathrm{ab}}(X)$, and its kernel is the maximal divisible subgroup,* $\mathrm{SK}_1(X)_{\mathrm{div}}$ *of* $\mathrm{SK}_1(X)$.

(ii) *The map τ_X is surjective, and its kernel is* $\mathrm{Ker}(\tau_X) = V(X)_{\mathrm{div}}$, *which is the maximal divisible subgroup of $V(X)$.*

(iii) *The image* $\mathrm{Im}(\tau_X)$ *of τ_X is finite.*

From the above theorem, the reciprocity map τ_X induces an isomorphism $V(X)/V(X)_{\mathrm{div}} \xrightarrow{\simeq} \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ of finite groups. Since an extension of a finite group by a divisible group splits, $V(X)$ is finite by divisible: $V(X) = V(X)_{\mathrm{fin}} \oplus V(X)_{\mathrm{div}}$. Moreover, the group $V(X)$ can be expressed as a Somekawa K-group, namely

$$V(X) \simeq K(k; J, \mathbb{G}_m) \tag{2.9}$$

associated with the Jacobian variety $J = \mathrm{Jac}(X)$ and $\mathbb{G}_m$ ([36, Theorem 2.1], [28, Remark 2.4.2 (c)]). For X has good reduction, the Jacobian variety J has also good reduction. The reciprocity map $\tau_X \colon V(X) \to \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ coincides with the Galois symbol map associated with J and $\mathbb{G}_m$ ([36, Proposition 1.5]) as in the following commutative (up to sign) diagram: For any $m \in \mathbb{Z}_{\geq 1}$,

(2.10)
$$\begin{tikzcd}
V(X)/m \arrow[r, "\tau_{X,m}"] \arrow[d, "\simeq"', "(2.9)"] & \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}/m \arrow[d, "\simeq"] \\
K(k; J, \mathbb{G}_m)/m \arrow[r, "s_m"] & H^2(k, J[m] \otimes \mu_m)
\end{tikzcd}$$

(cf. [1, Theorem 1.14]). Here, the right vertical isomorphism is induced from $H^2(k, J[m] \otimes \mu_m) \simeq J[m]_{G_k}$. By the class field theory for X (Theorem 2.9), the map $\tau_{X,m}$ induced from τ_X is surjective. As $\mathrm{Ker}(\tau_X)$ is divisible, the map $\tau_{X,m}$ is injective. We conclude that the Galois symbol map s_m is bijective for every $m \geq 1$. (Note that the injectivity of s_m has also been established for an arbitrary field in [40, Appendix].)

There is a surjective homomorphism $\mathrm{SK}_1(X) \to \mathrm{CH}_0(\overline{X})$ (see [16, Section 2]), called the *boundary map*, where $\mathrm{CH}_0(\overline{X})$ is the Chow group of the special fiber $\overline{X} = \mathscr{X} \otimes_{\mathcal{O}_k} \mathbb{F}_k$ of the model $\mathscr{X}$. This map is compatible with the valuation map v_k of k as the following commutative diagram indicates:

$$\begin{tikzcd}
0 \arrow[r] & V(X) \arrow[r] \arrow[d, dashed, "\partial_X"] & \mathrm{SK}_1(X) \arrow[r, "N"] \arrow[d, two heads] & k^{\times} \arrow[r] \arrow[d, "v_k"] & 0 \\
0 \arrow[r] & A_0(\overline{X}) \arrow[r] & \mathrm{CH}_0(\overline{X}) \arrow[r, "\deg"] & \mathbb{Z} \arrow[r] & 0,
\end{tikzcd} \tag{2.11}$$

where deg is the degree map, and $A_0(\overline{X})$ is its kernel. We denote by ∂_X the induced map $V(X) \to A_0(\overline{X})$. Because the horizontal sequences split, the boundary map ∂_X is surjective. A rational point $x \in X(k)$ gives rise to an $\mathbb{F}_k$-rational point of $\overline{X}$ by the valuative criterion for properness. The Abel–Jacobi map gives an isomorphism $A_0(\overline{X}) \xrightarrow{\simeq} \overline{J}(\mathbb{F}_k)$, where $\overline{J} = \mathrm{Jac}(\overline{X})$ is the Jacobian variety of $\overline{X}$.

Lemma 2.10. *The kernel* $\mathrm{Ker}(\partial_X)$ *is finite by divisible (in the sense of Definition 2.1). Namely, we have a decomposition*

$$\mathrm{Ker}(\partial_X) = \mathrm{Ker}(\partial_X)_{\mathrm{fin}} \oplus \mathrm{Ker}(\partial_X)_{\mathrm{div}}$$

for a finite group $\mathrm{Ker}(\partial_X)_{\mathrm{fin}}$ *and a divisible group* $\mathrm{Ker}(\partial_X)_{\mathrm{div}}$.

Proof. Consider the short exact sequence $0 \to \mathrm{Ker}(\partial_X) \to V(X) \xrightarrow{\partial_X} A_0(\overline{X}) \to 0$. As noted above $V(X)$ is finite by divisible and $A_0(\overline{X}) \simeq \overline{J}(\mathbb{F}_k)$ is finite. The assertion follows from Lemma 2.2 (iii). □

The classical class field theory (for the curve $\overline{X}$ over $\mathbb{F}_k$) says that the reciprocity map $\rho_{\overline{X}} : A_0(\overline{X}) \xrightarrow{\simeq} \pi_1^{\mathrm{ab}}(\overline{X})^{\mathrm{geo}} = \pi_1^{\mathrm{ab}}(\overline{X})_{\mathrm{tor}}$ is bijective of finite groups and makes the following diagram commutative:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\partial_X) \arrow[r] \arrow[d, dashed, "\mu_X"] & V(X) \arrow[r, "\partial_X"] \arrow[d, two heads, "\tau_X"] & A_0(\overline{X}) \arrow[r] \arrow[d, "\rho_{\bar{X}}", "\simeq"'] & 0 \\
0 \arrow[r] & \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \arrow[r] & \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \arrow[r, "\mathrm{sp}"] & \pi_1^{\mathrm{ab}}(\overline{X})^{\mathrm{geo}} \arrow[r] & 0.
\end{tikzcd}$$

For the commutativity of the right square in the above diagram, see [16, Proposition 2]. From the diagram, we obtain the surjective homomorphism $\mu_X \colon \mathrm{Ker}(\partial_X) \twoheadrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ with $\mathrm{Ker}(\mu_X) \simeq \mathrm{Ker}(\tau_X) = V(X)_{\mathrm{div}}$. Since the group $A_0(\overline{X})$ is finite, we have an equality $\mathrm{Ker}(\partial_X)_{\mathrm{div}} = V(X)_{\mathrm{div}}$. Moreover, the reciprocity map τ_X induces $V(X)_{\mathrm{fin}} = V(X)/V(X)_{\mathrm{div}} \xrightarrow{\simeq}$

$\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$. It follows that the map μ_X induces an isomorphism of finite groups

$$\mathrm{Ker}(\partial_X)_{\mathrm{fin}} \xrightarrow{\simeq} \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}. \tag{2.12}$$

3. Abelian varieties

Throughout this section, we will be using the following notation:

- A: an abelian variety over k of dimension $g = \dim(A)$ with good *ordinary* reduction.
- $\mathscr{A}$: the Néron model over $\mathcal{O}_k$ of A ([2, Section 1.2]).
- $\overline{A} := \mathscr{A} \otimes_{\mathcal{O}_k} \mathbb{F}_k$: the special fiber of $\mathscr{A}$ which is an ordinary abelian variety over $\mathbb{F}_k$.
- $\widehat{A}$: the formal group law over $\mathcal{O}_k$ of A (cf. [10, Section C.2]).

The formal group law $\widehat{A}$ defines a Mackey functor by the associated group $\widehat{A}(K) := \widehat{A}(\mathfrak{m}_K)$ for a finite extension K/k.

Boundary map. For any $m \geq 1$, the finite flat group scheme $\mathscr{A}[m]$ over $\mathcal{O}_k$ fits into the following connected-étale exact sequence

$$0 \longrightarrow \mathscr{A}[m]^{\circ} \xrightarrow{\iota} \mathscr{A}[m] \xrightarrow{\pi} \mathscr{A}[m]^{\mathrm{et}} \longrightarrow 0 \tag{3.1}$$

(cf. [37, Section 1.4]). By taking the limit $\varprojlim_m$, we obtain the short exact sequence

$$0 \longrightarrow T(\mathscr{A})^{\circ} \xrightarrow{\iota} T(\mathscr{A}) \xrightarrow{\pi} T(\mathscr{A})^{\mathrm{et}} \longrightarrow 0 \tag{3.2}$$

of the full Tate modules, where $T(\mathscr{A})^{\bullet} := \varprojlim_m \mathscr{A}[m]^{\bullet}$ for $\bullet \in \{\circ, \emptyset, \mathrm{et}\}$. On the other hand, the group $\widehat{A}(\overline{k}) := \varinjlim_{k'/k} \widehat{A}(\mathfrak{m}_{k'})$ associated with the formal group law $\widehat{A}$ over $\mathcal{O}_k$ of A gives the short exact sequence

$$0 \longrightarrow \widehat{A}[m] \xrightarrow{\iota} A[m] \xrightarrow{\pi} \overline{A}[m] \longrightarrow 0, \tag{3.3}$$

where $\widehat{A}[m] = \widehat{A}(\overline{k})[m]$ is the m-torsion subgroup of $\widehat{A}(\overline{k})$ ([10, Theorem C.2.6]). The valuative criterion of properness yields $\mathscr{A}[m] \simeq A[m]$ as G_k-modules. By the equivalence of categories between finite étale group schemes over $\mathcal{O}_k$ and finite G_k-modules, we have $\mathscr{A}[m]^{\mathrm{et}} \simeq \overline{A}[m]$ (cf. [37, Section 1.4]). The group $\widehat{A}(\overline{k})$ has no non-trivial prime to p-torsion ([10, Proposition C.2.5]). By comparing the short exact sequences (3.1) and (3.3), we obtain

$$\mathscr{A}[m]^{\circ} \simeq \widehat{A}[m], \quad T(\mathscr{A})^{\mathrm{et}} \simeq \varprojlim_m \overline{A}[m], \quad \text{and} \quad T(\mathscr{A})^{\circ} \simeq \varprojlim_m \widehat{A}[m].$$

By taking the G_k-coinvariance of (3.2), we have

$$(T(\mathscr{A})^{\circ})_{G_k} \xrightarrow{\iota} T(A)_{G_k} \xrightarrow{\pi} (T(\mathscr{A})^{\mathrm{et}})_{G_k} \longrightarrow 0. \tag{3.4}$$

From [36, (3.2.1)] (see also [1, Remark 2.7]), the étale quotient of the above sequence becomes

$$(3.5) \qquad (T(\mathscr{A})^{\mathrm{et}})_{G_k} \simeq \varprojlim_m (\overline{A}[m])_{G_k} \simeq \overline{A}(\mathbb{F}_k).$$

By taking the projective limit, the Galois symbol maps $(s_m)_m$ induce a map $s\colon K(k;A,\mathbb{G}_m) \to \varprojlim_m H^2(k, A[m]\otimes\mu_m)$. The composite map

$$(3.6) \quad \partial_A\colon K(k;A,\mathbb{G}_m) \xrightarrow{s} \varprojlim_m H^2(k,A[m]\otimes\mu_m) \overset{(\diamondsuit)}{\simeq} T(A)_{G_k} \xrightarrow{\pi} \!\!\!\!\to \overline{A}(\mathbb{F}_k),$$

is called the *boundary map* of A, where the middle isomorphism $(\diamondsuit)$ follows from the local Tate duality theorem ([25, Theorem 7.2.6], cf. [1, (2.2)], see also Proposition A.1 in Appendix). Since the limit of the Galois symbol map $s = \varprojlim_m s_m$ in (3.6) is surjective ([36, Theorem 3.3]), so is ∂_A.

Lemma 3.1.

(i) *The groups* $(A\otimes\mathbb{G}_m)(k), K(k;A,\mathbb{G}_m)$ *and* $\mathrm{Ker}(\partial_A)$ *are finite by divisible in the sense of Definition 2.1.*

(ii) *For any* $m\geq 1$ *prime to* p, *we have* $\mathrm{Ker}(\partial_A)/m = 0$.

Proof.

(i). The proof of [28, Theorem 4.5] implies that $(A\otimes\mathbb{G}_m)(k)/m$ is finite and its order is bounded independently of m. This implies the first assertion by Lemma 2.2 (i) (as in Lemma 2.10). Since we have the quotient map $(A\otimes\mathbb{G}_m)(k) \twoheadrightarrow K(k;A,\mathbb{G}_m)$, the second assertion follows from Lemma 2.2 (ii).

Consider the short exact sequence $0 \to \mathrm{Ker}(\partial_A) \to K(k;A,\mathbb{G}_m) \overset{\partial_A}{\to} \overline{A}(\mathbb{F}_k) \to 0$. Since $\overline{A}(\mathbb{F}_k)$ is finite, Lemma 2.2 (iii) implies that $\mathrm{Ker}(\partial_A)$ is finite by divisible.

(ii). From (i), we have $K(k;A,\mathbb{G}_m) = K(k;A,\mathbb{G}_m)_{\mathrm{fin}} \oplus K(k;A,\mathbb{G}_m)_{\mathrm{div}}$, and $\mathrm{Ker}(\partial_A) = \mathrm{Ker}(\partial_A)_{\mathrm{fin}} \oplus \mathrm{Ker}(\partial_A)_{\mathrm{div}}$ (cf. Definition 2.1). As the target of the boundary map $\partial_A\colon K(k;A,\mathbb{G}_m) \to \overline{A}(\mathbb{F}_k)$ is finite, we obtain a short exact sequence $0 \to \mathrm{Ker}(\partial_A)_{\mathrm{fin}} \to K(k;A,\mathbb{G}_m)_{\mathrm{fin}} \overset{\partial_A}{\to} \overline{A}(\mathbb{F}_k) \to 0$. Take any $m\geq 1$ coprime to p. For $K(k;A,\mathbb{G}_m)_{\mathrm{fin}}$ and $\overline{A}(\mathbb{F}_k)$ are finite, the multiplication by m map on these finite groups induces

$$K(k;A,\mathbb{G}_m)_{\mathrm{fin}}[m] \simeq K(k;A,\mathbb{G}_m)_{\mathrm{fin}}/m \overset{(\star)}{\simeq} \overline{A}(\mathbb{F}_k)/m \simeq \overline{A}(\mathbb{F}_k)[m],$$

where the isomorphism $(\star)$ follows from [12, Proposition 2.6] (for the case where A is the Jacobian variety, [1, Proposition 2.29]). The boundary map ∂_A gives an isomorphism $K(k;A,\mathbb{G}_m)\{m\} \overset{\simeq}{\to} \overline{A}(\mathbb{F}_k)\{m\}$, for any m prime to p. This implies that $\mathrm{Ker}(\partial_A)_{\mathrm{fin}}$ is a p-primary torsion group. □

Let $T_p(\mathscr{A})^\bullet = \varprojlim_n(\mathscr{A}[p^n]^\bullet)$ be the p-adic Tate module of $\mathscr{A}[p^n]^\bullet$ for $\bullet \in \{\circ, \emptyset, \mathrm{et}\}$ (cf. (3.1)) and write $T(\mathscr{A})^\bullet = T_p(\mathscr{A})^\bullet \times T'(\mathscr{A})^\bullet$ with $T'(\mathscr{A})^\bullet = \varprojlim_{(m,p)=1}\mathscr{A}[m]^\bullet$. From the following lemma, one can describe $\mathrm{Ker}(\partial_A)_{\mathrm{fin}}$ by using the exact sequence

$$(T_p(\mathscr{A})^\circ)_{G_k} \xrightarrow{\iota} T_p(A)_{G_k} \xrightarrow{\pi} (T_p(\mathscr{A})^{\mathrm{et}})_{G_k} \longrightarrow 0,$$

where $T_p(A) := \varprojlim_n A[p^n] \simeq T_p(\mathscr{A})$ (cf. (3.4)).

Lemma 3.2. *Suppose that, for any $m \geq 1$, the Galois symbol map*

$$s_m : K(k; A, \mathbb{G}_m)/m \longrightarrow H^2(k, A[m] \otimes \mu_m)$$

is injective. We have $\mathrm{Ker}(\partial_A)_{\mathrm{fin}} \simeq \mathrm{Im}((T_p(\mathscr{A})^\circ)_{G_k} \xrightarrow{\iota} T_p(A)_{G_k})$.

Proof. For any $m \in \mathbb{Z}_{\geq 1}$, by [36, Theorem 3.3] the map s_m is surjective. From the assumption, it is bijective. By taking the projective limit, we obtain $\varprojlim_m s_m = s_A \colon K(k; A, \mathbb{G}_m)_{\mathrm{fin}} \xrightarrow{\simeq} T(A)_{G_k}$. From the definition of the boundary map (3.6), we have a commutative diagram

$$\begin{tikzcd}
K(k; A, \mathbb{G}_m)_{\mathrm{fin}} \arrow[r, "s_A", "\simeq"'] \arrow[d, two heads, "\partial_A"] & T(A)_{G_k} \arrow[d, two heads, "\pi"] \\
\overline{A}(\mathbb{F}_k) \arrow[r, "\simeq", "(3.5)"'] & (T(\mathscr{A})^{\mathrm{et}})_{G_k}.
\end{tikzcd}$$

This gives $\mathrm{Ker}(\partial_A)_{\mathrm{fin}} \simeq \mathrm{Ker}\left(T(A)_{G_k} \xrightarrow{\pi} \overline{A}(\mathbb{F}_k)\right)$. Next, Lemma 3.1 (ii) yields an isomorphism $K(k; A, \mathbb{G}_m)/m \simeq \overline{A}(\mathbb{F}_k)/m$ for any $m \in \mathbb{Z}_{\geq 1}$ which is prime to p. Thus, we have $T'(A)_{G_k} \xrightarrow{\simeq} \varprojlim_{(m,p)=1}(\overline{A}(\mathbb{F}_k)/m)_{G_k}$ and the following commutative diagram:

$$\begin{tikzcd}
(T_p(\mathscr{A})^\circ)_{G_k} \arrow[r, "\iota"] \arrow[d, equal] & T_p(A)_{G_k} \arrow[r] \arrow[d, hook] & (T_p(\mathscr{A})^{\mathrm{et}})_{G_k} \arrow[r] \arrow[d, hook] & 0 \\
(T_p(\mathscr{A})^\circ)_{G_k} \arrow[r] & T(A)_{G_k} \arrow[r] & \overline{A}(\mathbb{F}_k) \arrow[r] & 0.
\end{tikzcd}$$

Here, the first vertical map is the identity, the second is the natural inclusion induced by $T_p(A) \hookrightarrow T(A)$ (which splits) and the third one is the composition $(T_p(\mathscr{A})^{\mathrm{et}})_{G_k} \simeq \overline{A}(\mathbb{F}_k)\{p\} \hookrightarrow \overline{A}(\mathbb{F}_k)$ ([1, Remark 2.7]), where $\overline{A}(\mathbb{F}_k)\{p\}$ is the p-primary torsion subgroup of $\overline{A}(\mathbb{F}_k)$. Then, it is clear that

$$\begin{aligned}
\mathrm{Im}((T_p(\mathscr{A})^\circ)_{G_k} \xrightarrow{\iota} T_p(A)_{G_k}) &= \mathrm{Im}((T_p(\mathscr{A})^\circ)_{G_k} \longrightarrow T(A)_{G_k}) \\
&= \mathrm{Ker}(T(A)_{G_k} \xrightarrow{\pi} \overline{A}(\mathbb{F}_k)).
\end{aligned}$$

The lemma follows from these equalities. □

Formal groups associated with abelian varieties. In this paragraph, we give an upper bound for the Mackey product $(\widehat{A} \otimes \mathbb{G}_m)(k)$ associated to $\widehat{A}$ and $\mathbb{G}_m$.

Lemma 3.3. *Let k'/k be a finite tamely ramified extension. Then, the norm map*

$$N_{k'/k} \colon (\widehat{A} \otimes \mathbb{G}_m)(k') \twoheadrightarrow (\widehat{A} \otimes \mathbb{G}_m)(k)$$

is surjective.

Proof. Take any symbol of the form $\{x, a\}_{K/k}$ in $(\widehat{A} \otimes \mathbb{G}_m)(k)$. For Kk'/K is also tamely ramified, there exists $\xi \in \widehat{A}(K)$ such that $N_{Kk'/K}(\xi) = x$ ([3, Proposition 3.9]). The *projection formula*, that is, the relation (PF) defining the Mackey product in Definition 2.5, yields

$$\begin{aligned} \{x, a\}_{K/k} &= \{N_{Kk'/K}(\xi), a\}_{K/k} \\ &\overset{\text{(PF)}}{=} \{\xi, \operatorname{Res}_{Kk'/K}(a)\}_{Kk'/k} \\ &\overset{(2.2)}{=} N_{k'/k}(\{\xi, \operatorname{Res}_{Kk'/K}(a)\}_{Kk'/k'}). \end{aligned}$$

The assertion follows. □

In the same way as in Definition 2.6, for any $n \geq 1$, we define the Galois symbol map

$$s_{p^n} := s_{p^n,k} \colon (\widehat{A} \otimes \mathbb{G}_m)(k)/p^n \longrightarrow H^2(k, \widehat{A}[p^n] \otimes \mu_{p^n}) \tag{3.7}$$

by $s_{p^n}(\{x, a\}_{K/k}) = \operatorname{Cor}_{K/k}(\delta_{\widehat{A}}(x) \cup \delta_{\mathbb{G}_m}(a))$, where $\delta_{\widehat{A}} : \widehat{A}(K)/p^n \hookrightarrow H^1(K, \widehat{A}[p^n])$ is the Kummer map. This map is well-defined by properties of the cup product ([25, Proposition 1.5.3]).

Proposition 3.4. *We assume $\widehat{A}[p] \subset \widehat{A}(k)$, $\mu_p \subset k$, and $\overline{A}[p] \subset \overline{A}(\mathbb{F}_k)$.*

(i) *There is an isomorphism $\widehat{A}/p \simeq \overline{U}^{\oplus g}$ of Mackey functors over k, where $\overline{U}$ is the sub Mackey functor of $\mathbb{G}_m/p$ defined by*

$$\overline{U}(K) := \overline{U}_K := \operatorname{Im}(U_K \longrightarrow K^\times/p) = U_K/p.$$

(ii) *For any $n \geq 1$, the Galois symbol map*

$$s_{p^n} \colon (\widehat{A} \otimes \mathbb{G}_m)(k)/p^n \longrightarrow H^2(k, \widehat{A}[p^n] \otimes \mu_{p^n})$$

defined in (3.7) *is bijective.*

The isomorphism $\widehat{A}/p \simeq \overline{U}^{\oplus g}$ in the assertion (i) is not canonical and depends on the choice of an isomorphism $\widehat{A}[p] \simeq (\mu_p)^{\oplus g}$ of (trivial) Galois modules. The proof of the above proposition essentially follows from [12, Section 4], but the assumptions are weakened slightly.

Proof of Proposition 3.4.

(i). We fix an isomorphism $\widehat{A}[p] \simeq (\mu_p)^{\oplus g}$ of Galois modules. This induces the bijection ($\clubsuit$) below

$$\delta_K\colon \widehat{A}(K)/p \overset{\delta_{\widehat{A}}}{\hookrightarrow} H^1(K, \widehat{A}[p]) \overset{(\clubsuit)}{\simeq} H^1(K, \mu_p)^{\oplus g} \xleftarrow{\simeq} (K^\times/p)^{\oplus g}$$

for any finite extension K/k. Here, the last map is the Kummer map on $\mathbb{G}_m$ (cf. (2.3)) which is bijective from "Hilberts Satz 90". First, we show $\mathrm{Im}(\delta_K) \subset (\overline{U}_K)^{\oplus g}$. Consider the following commutative diagram:

$$\begin{tikzcd}
\widehat{A}(K)/p \arrow[r, "\delta_K"] \arrow[d] & (K^\times/p)^{\oplus g} \arrow[r, "v"] \arrow[d, "\iota"] & (\mathbb{Z}/p)^{\oplus g} \arrow[d, "\mathrm{id}"] \\
\widehat{A}(K^{\mathrm{ur}})/p \arrow[r, "\delta_{K^{\mathrm{ur}}}"] & ((K^{\mathrm{ur}})^\times/p)^{\oplus g} \arrow[r, "v"] & (\mathbb{Z}/p)^{\oplus g},
\end{tikzcd}$$

where K^{ur} is the completion of the maximal unramified extension of K, and v is the valuation map. Since we have $\widehat{A} \otimes_{\mathcal{O}_k} O_{k^{\mathrm{ur}}} \simeq (\widehat{\mathbb{G}}_m)^{\oplus g}$ ([22, Lemma 4.26, Lemma 4.27]), $\widehat{A}(K^{\mathrm{ur}})/p \simeq (\overline{U}_{K^{\mathrm{ur}}})^{\oplus g}$ and the composition $v \circ \delta_{K^{\mathrm{ur}}} = 0$ in the above diagram. Thus, the composition $v \circ \delta_K = 0$ in the top sequence and hence $\mathrm{Im}(\delta_K) \subset (\overline{U}_K)^{\oplus g}$. From the structure theorem of the multiplicative group $K^\times$, we have $U_K/p \simeq (\mathbb{Z}/p)^{\oplus([K:\mathbb{Q}_p]+1)}$ and hence $\#(\overline{U}_K)^{\oplus g} = \{\#(U_K/p)\}^g = p^{g([K:\mathbb{Q}_p]+1)}$. It is enough to show $\#\widehat{A}(K)/p \geq p^{g([K:\mathbb{Q}_p]+1)}$.

By Mattuck's theorem ([21]) and $\#A(K)[p] = p^{2g}$ we have $\#A(K)/p = p^{g([K:\mathbb{Q}_p]+2)}$. Recall that $\overline{A}$ has ordinary reduction so that $\overline{A}[p] \simeq (\mathbb{Z}/p)^{\oplus g}$. The exact sequence

$$\widehat{A}(K)/p \longrightarrow A(K)/p \longrightarrow \overline{A}(\mathbb{F}_K)/p \longrightarrow 0$$

and the equality $\#\overline{A}(\mathbb{F}_K)/p = \#\overline{A}(\mathbb{F}_K)[p]$ imply the inequality $\#\widehat{A}(K)/p \geq p^{g([K:\mathbb{Q}_p]+1)}$. The map $\delta_K\colon \widehat{A}(K)/p \xrightarrow{\simeq} (\overline{U}_K)^{\oplus g}$ is bijective.

(ii). For each $n \in \mathbb{Z}_{\geq 1}$, to simplify the notation, we put

$$\mathscr{M}_n := (\widehat{A} \otimes \mathbb{G}_m)(k)/p^n, \ \mathscr{H}_n := H^2(k, \widehat{A}[p^n] \otimes \mu_{p^n})$$

and $s_n := s_{p^n}\colon \mathscr{M}_n \to \mathscr{H}_n$. We will show by induction that s_n is bijective. First, we show that $s_1\colon \mathscr{M}_1 \to \mathscr{H}_1$ is bijective. As in the proof of (i) above, we fix an isomorphism $\widehat{A}[p] \simeq (\mu_p)^{\oplus g}$ of Galois modules and hence we obtain

$$\mathscr{H}_1 = H^2(k, \widehat{A}[p] \otimes \mu_p) \simeq H^2(k, \mu_p^{\otimes 2})^{\oplus g}. \tag{3.8}$$

By (i), there is an isomorphism $\widehat{A}/p \simeq \overline{U}^{\oplus g}$. For the Mackey product commutes with the direct sum,

$$\mathscr{M}_1 \simeq (\widehat{A}/p \otimes \mathbb{G}_m/p)(k) \simeq (\overline{U} \otimes \mathbb{G}_m/p)(k)^{\oplus g}. \tag{3.9}$$

The natural inclusion $\overline{U} \hookrightarrow \mathbb{G}_m/p$, induces the following commutative diagram:

$$\begin{tikzcd}
\mathscr{M}_1 \arrow[rr, "s_1"] \arrow[d, "\simeq", "(3.9)"'] & & \mathscr{H}_1 \arrow[d, "\simeq", "(3.8)"'] \\
(\overline{U} \otimes \mathbb{G}_m/p)(k)^{\oplus g} \arrow[r] & (\mathbb{G}_m/p \otimes \mathbb{G}_m/p)(k)^{\oplus g} \arrow[r, "(s_p)^{\oplus g}"] & H^2(k, \mu_p^{\otimes 2})^{\oplus g}.
\end{tikzcd}$$

Here, the map s_p in the bottom is the Galois symbol map associated to $\mathbb{G}_m$. In fact, the composition $(\overline{U} \otimes \mathbb{G}_m/p)(k) \to (\mathbb{G}_m/p \otimes \mathbb{G}_m/p)(k) \xrightarrow{s_p} H^2(k, \mu_p^{\otimes 2})$ is bijective ([28, Lemma 4.2.1], see also [12, Lemma 4.5]) and so is $s_1 \colon \mathscr{M}_1 \to \mathscr{H}_1$.

Next, we consider the following commutative diagram with exact rows except possibly at $\mathscr{M}_{n-1}$:

$$\begin{tikzcd}
\widehat{A}[p] \otimes_{\mathbb{Z}} k^{\times} \arrow[r, "\psi"] \arrow[d, "\phi"] \arrow[dr, phantom, "(\Diamond)"] & \mathscr{M}_{n-1} \arrow[r] \arrow[d, "s_{n-1}", "\simeq"'] & \mathscr{M}_n \arrow[r] \arrow[d, "s_n"] & \mathscr{M}_1 \arrow[r] \arrow[d, "s_1", "\simeq"'] & 0 \\
H^1(k, \widehat{A}[p] \otimes \mu_p) \arrow[r] & \mathscr{H}_{n-1} \arrow[r] & \mathscr{H}_n \arrow[r] & \mathscr{H}_1 \arrow[r] & 0
\end{tikzcd}$$

(cf. [28, Lemma 4.2.2]), where the bottom sequence is induced from

$$0 \longrightarrow \widehat{A}[p^{n-1}] \otimes \mu_{p^n} \longrightarrow \widehat{A}[p^n] \otimes \mu_{p^n} \longrightarrow \widehat{A}[p] \otimes \mu_p \longrightarrow 0.$$

Here, the far left vertical map ϕ is given by

$$\widehat{A}[p] \otimes_{\mathbb{Z}} k^{\times} \xrightarrow{\mathrm{id} \otimes \delta} H^0(k, \widehat{A}[p]) \otimes_{\mathbb{Z}} H^1(k, \mu_p) \xrightarrow{\cup} H^1(k, \widehat{A}[p] \otimes \mu_p)$$

and ψ is induced from $\widehat{A}[p] \hookrightarrow \widehat{A}(k) \twoheadrightarrow \widehat{A}(k)/p^{n-1}$: $\psi(w \otimes a) := \{w, a\}_{k/k}$ for $w \otimes a \in \widehat{A}[p] \otimes k^{\times}$. The commutativity of the square $(\Diamond)$ follows from a property of the cup product (cf. [25, Proposition 1.4.3 (i)]). By the fixed isomorphism $\widehat{A}[p] \simeq (\mu_p)^{\oplus g}$ of trivial Galois modules, the map ϕ becomes

$$\widehat{A}[p] \otimes_{\mathbb{Z}} k^{\times} \twoheadrightarrow (\mu_p \otimes_{\mathbb{Z}} k^{\times}/p)^{\oplus g} \simeq H^1(k, \mu_p^{\otimes 2})^{\oplus g} \simeq H^1(k, \widehat{A}[p] \otimes \mu_p).$$

In particular, ϕ is surjective. From the inductive hypothesis, s_{n-1} is bijective and hence s_n is surjective. From the diagram chase and the induction hypothesis, s_n is injective. □

Theorem 3.5. *For any $n \geq 1$, there is a surjective homomorphism*

$$(\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g} \twoheadrightarrow (\widehat{A} \otimes \mathbb{G}_m)(k)/p^n,$$

where $M^{\mathrm{ur}} = \max\{m \geq 0 \mid \mu_{p^m} \subset k^{\mathrm{ur}}\}$.

Proof. Recall that, for any finite unramified extension k'/k, the norm map $(\widehat{A} \otimes \mathbb{G}_m)(k') \to (\widehat{A} \otimes \mathbb{G}_m)(k)$ is surjective (Lemma 3.3). We may assume $M^{\mathrm{ur}} = M := \max\{m \geq 0 \mid \mu_{p^m} \subset k\}$. We have a short exact sequence

$$0 \longrightarrow \widehat{A}[p] \longrightarrow A[p] \longrightarrow \overline{A}[p] \longrightarrow 0$$

by [10, Theorem C.2.6]. Mazur's theorem $\widehat{A}\otimes_{\mathcal{O}_k} O_{k^{\mathrm{ur}}} \simeq (\widehat{\mathbb{G}}_m)^{\oplus g}$ ([22, Lemma 4.26, Lemma 4.27]) indicates that, by replacing k with a finite unramified extension, the above sequence becomes

$$0 \longrightarrow (\mu_p)^{\oplus g} \longrightarrow A[p] \longrightarrow (\mathbb{Z}/p)^{\oplus g} \longrightarrow 0$$

as G_k-modules. In particular, we have $\overline{A}[p] \subset \overline{A}(\mathbb{F}_k)$. In the following, we put $K = k(\mu_p)$.

First, we consider the case $M = 0$ and show $(\widehat{A}\otimes\mathbb{G}_m)(k)/p = 0$. This implies that $(\widehat{A}\otimes\mathbb{G}_m)(k)$ is p-divisible so that $(\widehat{A}\otimes\mathbb{G}_m)(k)/p^n = 0$ for any $n \geq 1$. The assumption $M = 0$ implies $\mu_p \not\subset k$ and $k \subsetneqq K$. Using $\widehat{A}[p] \simeq (\mu_p)^{\oplus g}$, the Galois symbol map defined in (3.7) is of the form:

$$s_p\colon (\widehat{A}\otimes\mathbb{G}_m)(k)/p \longrightarrow H^2(k, \widehat{A}[p]\otimes\mu_p) \simeq H^2(k, \mu_p^{\otimes 2})^{\oplus g}.$$

Since we have $H^2(k, \mu_p^{\otimes 2}) \simeq K_2^M(k)/p = 0$ (cf. [6, Chapter IX, Proposition 4.2]), it is left to show that the Galois symbol map s_p is injective. The extension degree of $K = k(\mu_p)/k$ is prime to p. The composition

$$(\widehat{A}\otimes\mathbb{G}_m)(k)/p \overset{\mathrm{Res}_{K/k}}{\longrightarrow} (\widehat{A}\otimes\mathbb{G}_m)(K)/p \overset{N_{K/k}}{\longrightarrow} (\widehat{A}\otimes\mathbb{G}_m)(k)/p$$

is the multiplication by $[K : k]$ and is bijective. Note that the restriction $\mathrm{Res}_{K/k}$ is injective. Consider the following commutative diagram:

$$\begin{tikzcd}
(\widehat{A}\otimes\mathbb{G}_m)(k)/p \arrow[r, "s_p"] \arrow[d, hook, "\mathrm{Res}_{K/k}"'] & H^2(k, \mu_p^{\otimes 2})^{\oplus g} \arrow[d, "\mathrm{Res}_{K/k}"] \\
(\widehat{A}\otimes\mathbb{G}_m)(K)/p \arrow[r, "s_{p,K}", "\simeq"'] & H^2(K, \mu_p^{\otimes 2})^{\oplus g}.
\end{tikzcd}$$

Here, the Galois symbol map $s_{p,K}$ is bijective from Proposition 3.4 (ii). From the diagram above, the Galois symbol map s_p is injective. We obtain $(\widehat{A}\otimes\mathbb{G}_m)(k)/p^n = 0$.

Next, consider the case $M > 0$. In this case, $K = k$. Fix $\zeta \in \mu_{p^M}$ a primitive p^M-th root of unity. In the following, we show the following claim:

Claim. $(\widehat{A}\otimes\mathbb{G}_m)(k)/p$ is generated by symbols of the form $\{w, \zeta\}_{k/k}$ for some $w \in \widehat{A}(k)$.

Proof. Recall that the Hilbert symbol $(-,-)_p\colon k^\times \otimes k^\times \to \mu_p \simeq \mathbb{Z}/p$ satisfies

$$(y, x)_p = 0 \Leftrightarrow y \in N_{k(\sqrt[p]{x})/k}\left(k(\sqrt[p]{x}\,)^\times\right), \quad \text{for } x, y \in k^\times \tag{3.10}$$

(cf. [38, Proposition 4.3]). From the very definition of M and $M = M^{\mathrm{ur}}$, the extension $L := k(\mu_{p^{M+1}})/k$ is non-trivial, and totally ramified. We have $U_k/N_{L/k}U_L \simeq k^\times/N_{L/k}L^\times$ (cf. the proof of [32, Section V.3, Corollary 7]) and local class field theory says $k^\times/N_{L/k}L^\times \simeq \mathrm{Gal}(L/k) \neq 0$ (cf. [32, Section XIII.3]). Thus, there exists $y \in U_k \smallsetminus N_{L/k}U_L$ such that $(y,\zeta)_p \neq 0$ from (3.10). As $(y,\zeta)_p \neq 0$, the chosen element y induces a non-trivial element in $\overline{U}_k = U_k/p$. We use the same notation y for this induced element in $\overline{U}_k$. For each $1 \leq i \leq g$, put

$$y^{(i)} := (1,\dots,1,\overset{\overset{i}{\vee}}{y},1,\dots,1) \in (\overline{U}_k)^{\oplus g}$$

and we denote by $w^{(i)} \in \widehat{A}(k)/p$ the element corresponding to $y^{(i)}$ through the isomorphism $\widehat{A}(k)/p \simeq (\overline{U}_k)^{\oplus g}$ (Proposition 3.4 (i)). The Galois symbol map is compatible with the Hilbert symbol map ([32, Section XIV.2, Proposition 5]) as the following commutative diagram indicates:

$$\begin{tikzcd}
\widehat{A}(k)/p \otimes_{\mathbb{Z}} k^\times/p \arrow[r, "\iota"] \arrow[d, "\simeq"] & (\widehat{A}\otimes\mathbb{G}_m)(k)/p \arrow[r, "s_p", "\simeq"'] & H^2(k, \widehat{A}[p]\otimes\mu_p) \arrow[d, "\simeq"] \\
\left(\overline{U}_k \otimes_{\mathbb{Z}} k^\times/p\right)^{\oplus g} \arrow[rr, "(-{,}-)_p"] & & (\mathbb{Z}/p)^{\oplus g}.
\end{tikzcd} \tag{3.11}$$

Here, s_p is the Galois symbol map and is bijective (Proposition 3.4 (ii)), and the map ι is given by $\iota(w\otimes x) = \{w,x\}_{k/k}$. The image of $w^{(i)}\otimes\zeta \in \widehat{A}(k)/p\otimes_{\mathbb{Z}} k^\times/p$ in $(\mathbb{Z}/p)^{\oplus g}$ via the lower left corner in (3.11) is

$$\xi^{(i)} := (0,\dots,0,\overset{\overset{i}{\vee}}{(y,\zeta)_p},0,\dots,0) \in (\mathbb{Z}/p)^{\oplus g}.$$

These elements $\xi^{(i)}$ $(1 \leq i \leq g)$ generate $(\mathbb{Z}/p)^{\oplus g}$ and hence the symbols $\{w^{(i)},\zeta\}_{k/k} = \iota(w^{(i)}\otimes\zeta)$ for $1 \leq i \leq g$ generate $(\widehat{A}\otimes\mathbb{G}_m)(k)/p$. □

For any $n \geq 1$, consider the exact sequence

$$(\widehat{A}\otimes\mathbb{G}_m)(k)/p \xrightarrow{p^n} (\widehat{A}\otimes\mathbb{G}_m)(k)/p^{n+1} \longrightarrow (\widehat{A}\otimes\mathbb{G}_m)(k)/p^n \longrightarrow 0,$$

where p^n is the map induced from the multiplication by p^n. From the claim above, the map p^n becomes 0 for all $n \geq M$, so that $(\widehat{A}\otimes\mathbb{G}_m)(k)/p^{n+1} \simeq (\widehat{A}\otimes\mathbb{G}_m)(k)/p^n$. It is left to show $(\mathbb{Z}/p^M)^{\oplus g} \twoheadrightarrow (\widehat{A}\otimes\mathbb{G}_m)(k)/p^M$. From Lemma 3.3, by replacing k with a sufficiently large unramified extension of k, we may assume $\widehat{A}[p^M] \simeq (\mu_{p^M})^{\oplus g}$ as G_k-modules. As the Galois symbol map $(\widehat{A}\otimes\mathbb{G}_m)(k)/p^M \to H^2(k,\widehat{A}[p^M]\otimes\mu_{p^M})$ is bijective (Proposition 3.4 (ii)) and $\mu_{p^M} \subset k$, we have

$$(\widehat{A}\otimes\mathbb{G}_m)(k)/p^M \simeq H^2(k,\widehat{A}[p^M]\otimes\mu_{p^M}) \simeq H^2(k,\mu_{p^M}^{\otimes 2})^{\oplus g} \simeq (\mathbb{Z}/p^M)^{\oplus g}.$$

□

Upper and lower bounds of the kernel of the boundary maps. The Mackey functor defined by the formal group law $\widehat{A}$ associated to A gives the short exact sequence as Mackey functors

$$0 \longrightarrow \widehat{A} \xrightarrow{\iota} A \xrightarrow{\pi} A/\widehat{A} \longrightarrow 0, \tag{3.12}$$

where $A/\widehat{A}$ is defined by the exactness. The Mackey functor $A/\widehat{A}$ is given by $(A/\widehat{A})(K) \simeq \overline{A}(\mathbb{F}_K)$ for each finite extension K/k with residue field $\mathbb{F}_K$ (for the precise description, see [28, (3.3)]). By applying $- \otimes \mathbb{G}_m$ (which is right exact) to the sequence (3.12), we have the following commutative diagram with exact rows

$$\begin{tikzcd}
 & (\widehat{A} \otimes \mathbb{G}_m)(k) \arrow[r, "\iota\otimes\mathrm{id}"] \arrow[d, "\varphi"] & (A \otimes \mathbb{G}_m)(k) \arrow[r] \arrow[d, two heads] & ((A/\widehat{A}) \otimes \mathbb{G}_m)(k) \arrow[r] \arrow[d, dashed, two heads, "\psi"] & 0 \\
0 \arrow[r] & \mathrm{Ker}(\partial_A) \arrow[r] & K(k; A, \mathbb{G}_m) \arrow[r, "\partial_A"] & \overline{A}(\mathbb{F}_k) \arrow[r] & 0,
\end{tikzcd} \tag{3.13}$$

where the middle vertical map is the quotient map, and ∂_A is the boundary map defined in (3.6). Here, the commutativity of the left square in (3.13) follows from the lemma below and this induces the right vertical map ψ which is surjective.

Lemma 3.6. *The boundary map ∂_A annihilates the image of $(\widehat{A} \otimes \mathbb{G}_m)(k)$ in $K(k; A, \mathbb{G}_m)$.*

Proof. For $m = \#\overline{A}(\mathbb{F}_k)$, there is a commutative diagram:

$$\begin{tikzcd}
(\widehat{A} \otimes \mathbb{G}_m)(k) \arrow[r] \arrow[d, "\bmod m"] & K(k; A, \mathbb{G}_m) \arrow[r, "\partial_A"] \arrow[d, "\bmod m"] & \overline{A}(\mathbb{F}_k) \arrow[d, "\bmod m", "\simeq"'] \\
(\widehat{A} \otimes \mathbb{G}_m)(k)/m \arrow[r] & K(k; A, \mathbb{G}_m)/m \arrow[r, "\partial_{A,m}"] & \overline{A}(\mathbb{F}_k)/m.
\end{tikzcd}$$

It is enough to show that the bottom sequence is a complex. The Galois symbol maps induce the following commutative diagram with exact rows:

$$\begin{tikzcd}
(\widehat{A} \otimes \mathbb{G}_m)(k)/m \arrow[r, "\iota\otimes\mathrm{id}"] \arrow[d, "s_m"] & (A \otimes \mathbb{G}_m)(k)/m \arrow[r] \arrow[d, "s_m"] \arrow[dr, "\partial_{A,m}"] & ((A/\widehat{A}) \otimes \mathbb{G}_m)(k) \arrow[r] \arrow[d, dashed] & 0 \\
H^2(k, \widehat{A}[m] \otimes \mu_m) \arrow[r] \arrow[d, "\simeq"] & H^2(k, A[m] \otimes \mu_m) \arrow[r] \arrow[d, "\simeq"] & H^2(k, \overline{A}[m] \otimes \mu_m) \arrow[r] \arrow[d, "\simeq"] & 0 \\
\widehat{A}[m]_{G_k} \arrow[r, "\iota"] & A[m]_{G_k} \arrow[r, "\pi"] & \overline{A}[m]_{G_k} \arrow[r] & 0,
\end{tikzcd}$$

where the second exact sequence is induced from the exact sequence for $A[m]$ noted in (3.3). The definition of the boundary map ∂_A (cf. (3.6)) says that the composition

$$(A\otimes\mathbb{G}_m)(k)/m \xrightarrow{s_m} H^2(k, A[m]\otimes\mu_m) \xrightarrow{\pi} H^2(k, \mathscr{A}[m]^{\mathrm{et}}\otimes\mu_m)$$

is the boundary map $\partial_{A,m}$. Since the bottom sequence in the above diagram is exact, $\partial_{A,m}$ annihilates the image of $(\widehat{A}\otimes\mathbb{G}_m)(k)/m$ and the assertion follows from this. □

Theorem 3.7. *There are surjective homomorphisms*

$$(\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g} \twoheadrightarrow \mathrm{Ker}(\partial_A)_{\mathrm{fin}} \twoheadrightarrow (\mathbb{Z}/p^{N_A})^{\oplus g},$$

where $N_A = \max\{n\geq 0 \mid A[p^n]\subset A(k)\}$ *and* $g=\dim(A)$.

Proof. To give the lower bound, we may assume $N := N_A > 0$. The diagram (3.13) induces

$$\begin{tikzcd}
(\widehat{A}\otimes\mathbb{G}_m)(k)/p^N \arrow[r] \arrow[d] & (A\otimes\mathbb{G}_m)(k)/p^N \arrow[r] \arrow[d] & ((A/\widehat{A})\otimes\mathbb{G}_m)(k)/p^N \arrow[r] \arrow[d] & 0 \\
\mathrm{Ker}(\partial_A)/p^N \arrow[r] & K(k;A,\mathbb{G}_m)/p^N \arrow[r, "\partial_{A,p^N}"] & \overline{A}(\mathbb{F}_k)/p^N \arrow[r] & 0.
\end{tikzcd}$$

In fact, the middle and right vertical maps are bijective ([12, Lemma 4.1, Corollary 4.3 (i)]), the upper sequence is left exact, and $(\widehat{A}\otimes\mathbb{G}_m)(k)/p^N \simeq (\mathbb{Z}/p^N)^{\oplus g}$ ([12, Lemma 4.5 (ii)]). Therefore,

$$\mathrm{Ker}(\partial_A) \twoheadrightarrow \mathrm{Ker}(\partial_A)/p^N \\ \twoheadrightarrow \mathrm{Ker}(\partial_{A,p^N}) \simeq (\widehat{A}\otimes\mathbb{G}_m)(k)/p^N \simeq (\mathbb{Z}/p^N)^{\oplus g}.$$

Next, we consider the decomposition $\overline{A}(\mathbb{F}_k) = \overline{A}(\mathbb{F}_k)\{p\}\oplus\overline{A}(\mathbb{F}_k)\{m\}$ for some m coprime to p. The composition $\partial_A^{\{p\}} : K(k;A,\mathbb{G}_m) \overset{\partial_A}{\to} \overline{A}(\mathbb{F}_k) \twoheadrightarrow \overline{A}(\mathbb{F}_k)\{p\}$ gives the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\partial_A) \arrow[r] \arrow[d, hook, "j"] & K(k;A,\mathbb{G}_m) \arrow[r, "\partial_A"] \arrow[d, equal] & \overline{A}(\mathbb{F}_k) \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & \mathrm{Ker}(\partial_A^{\{p\}}) \arrow[r] & K(k;A,\mathbb{G}_m) \arrow[r, "\partial_A^{\{p\}}"] & \overline{A}(\mathbb{F}_k)\{p\} \arrow[r] & 0.
\end{tikzcd}$$

By applying the snake lemma, the above diagram induces an isomorphism $\overline{A}(\mathbb{F}_k)\{m\} \overset{\simeq}{\to} \mathrm{Coker}(j)$. Since $\mathrm{Tor}_{\mathbb{Z}}(\mathrm{Coker}(j), \mathbb{Z}/p^n) = 0$, we conclude that

$$\mathrm{Ker}(\partial_A)/p^n \xrightarrow{\simeq} \mathrm{Ker}(\partial_A^{\{p\}})/p^n. \tag{3.14}$$

From the diagram (3.13), we have

$$\begin{tikzcd}
 & (\widehat{A}\otimes\mathbb{G}_m)(k) \arrow[r] \arrow[d, "\varphi^{\{p\}}"] & (A\otimes\mathbb{G}_m)(k) \arrow[r] \arrow[d, two heads] & ((A/\widehat{A})\otimes\mathbb{G}_m)(k) \arrow[r] \arrow[d, "\psi^{\{p\}}"] & 0 \\
0 \arrow[r] & \operatorname{Ker}(\partial_A^{\{p\}}) \arrow[r] & K(k;A,\mathbb{G}_m) \arrow[r, "\partial_A^{\{p\}}"] & \overline{A}(\mathbb{F}_k)\{p\} \arrow[r] & 0,
\end{tikzcd} \tag{3.15}$$

where the right vertical map $\psi^{\{p\}}$ is the composition $((A/\widehat{A})\otimes\mathbb{G}_m)(k) \overset{\psi}{\to} \overline{A}(\mathbb{F}_k) \twoheadrightarrow \overline{A}(\mathbb{F}_k)\{p\}$.

Claim. The kernel $\operatorname{Ker}(\psi^{\{p\}})$ is p-divisible.

Proof. Put $\mathscr{M} = ((A/\widehat{A}\,)\otimes\mathbb{G}_m)(k)$. Since $\psi^{\{p\}}$ induces an isomorphism

$$\mathscr{M}/p^n \simeq \overline{A}(\mathbb{F}_k)\{p\}/p^n = \overline{A}(\mathbb{F}_k)/p^n$$

for all $n\geq 1$ ([12, Lemma 4.1]), we have

$$\varprojlim_n \mathscr{M}/p^n \simeq \varprojlim_n \overline{A}(\mathbb{F}_k)/p^n \simeq \overline{A}(\mathbb{F}_k)\{p\}.$$

It follows that

$$\operatorname{Ker}(\psi^{\{p\}}) = \operatorname{Ker}\left(\mathscr{M}\longrightarrow \varprojlim_n \mathscr{M}/p^n\right) = \bigcap_{n\geq 1} p^n\mathscr{M}. \tag{3.16}$$

As $\overline{A}(\mathbb{F}_k)\{p\}$ is a finite p-group, there exists $s\geq 0$ such that p^s annihilates $\overline{A}(\mathbb{F}_k)\{p\}$. To show the claim, take any $x\in\operatorname{Ker}(\psi^{\{p\}})$ and any $n\geq 1$. From (3.16), there exists $y\in\mathscr{M}$ such that $x = p^{n+s}y = p^n(p^s y)$. Here, $p^s y\in\operatorname{Ker}(\psi^{\{p\}})$. Thus, $\operatorname{Ker}(\psi^{\{p\}})$ is p-divisible. □

By the snake lemma, the diagram (3.15) gives a surjective homomorphism $\operatorname{Ker}(\psi^{\{p\}})\twoheadrightarrow\operatorname{Coker}(\varphi^{\{p\}})$. From the above claim, $\operatorname{Coker}(\varphi^{\{p\}})$ is also p-divisible. The map $\varphi^{\{p\}}$ induces a surjective homomorphism

$$\varphi_n : (\widehat{A}\otimes\mathbb{G}_m)(k)/p^n \overset{\varphi^{\{p\}}}{\twoheadrightarrow} \operatorname{Ker}(\partial_A^{\{p\}})/p^n \overset{(3.14)}{\simeq} \operatorname{Ker}(\partial_A)/p^n.$$

From Theorem 3.5, we obtain

$$(\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g} \longrightarrow\!\!\!\!\rightarrow (\widehat{A}\otimes\mathbb{G}_m)(k)/p^n \overset{\varphi_n}{\twoheadrightarrow} \operatorname{Ker}(\partial_A)/p^n$$

for any $n\geq 1$. For the finite part $\operatorname{Ker}(\partial_A)_{\mathrm{fin}}$ is a p-group (Lemma 3.1 (ii)) this implies the existence of surjective homomorphism $(\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g}\twoheadrightarrow \operatorname{Ker}(\partial_A)_{\mathrm{fin}}$ as required. □

Remark 3.8. In the case where $A = E$ is an elliptic curve, define

$$\widehat{N} := \max\{n \mid \widehat{E}[p^n]\subset\widehat{E}(k)\}.$$

In general, we have $N \leq \widehat{N}$. By [22, Lemma 4.26 and Lemma 4.27], the base change $\widehat{E}[p^n]_{k^{\mathrm{ur}}}$ to k^{ur} gives $\widehat{E}_{k^{\mathrm{ur}}}[p^n] \simeq \mu_{p^n}$ and hence $\widehat{N} \leq M^{\mathrm{ur}}$. Using this, we will give a refined upper bound $\mathbb{Z}/p^{\widehat{N}} \twoheadrightarrow \mathrm{Ker}(\partial_E)_{\mathrm{fin}}$ in Proposition 5.2.

Remark 3.9. As noted in the introduction, we apply Theorem 3.7 to the Jacobian variety $J = \mathrm{Jac}(X)$ for a curve X over k which has good reduction to obtain the structure of $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ (Corollary 4.1). However, the structure of $\mathrm{Ker}(\partial_J) \subset K(k; J, \mathbb{G}_m) \simeq V(X)$ can be obtained without assuming X has good reduction. Precisely, let X be a projective smooth curve over k with $X(k) \neq \emptyset$ and assume that the Jacobian variety $J = \mathrm{Jac}(X)$ has good ordinary reduction. From Theorem 3.7 there are surjective homomorphisms

$$(\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g} \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Ker}(\partial_J)_{\mathrm{fin}} \longrightarrow\!\!\!\!\!\rightarrow (\mathbb{Z}/p^{N_J})^{\oplus g}.$$

Note that when X has good reduction (this is the very case studied in [1]), its Jacobian J has good reduction. But, the converse does not hold in general. By the semi-stable reduction theorem, at least X has semi-stable reduction, that is, there exists a model $\mathscr{X}$ over $\mathcal{O}_k$ of X whose closed fiber $\overline{X} = X \otimes_{\mathcal{O}_k} \mathbb{F}_k$ is semistable, i.e., $\overline{X}$ is reduced and has at most ordinary double points as singularities ([4, Theorem 2.4]).

The following proposition due to Yoshiyasu Ozeki insists that if we enlarge the base field k then the difference $N_A \leq M^{\mathrm{ur}}$ becomes arbitrarily large.

Proposition 3.10. *Let A be an abelian variety over k with potentially good reduction. For an extension K/k, we define*

$$N_A(K) := \max\{n \mid A[p^n] \subset A(K)\} = N_{A_K}, \text{ and}$$
$$M(K) := \max\{m \mid \mu_{p^m} \subset K^{\times}\}.$$

Then, for any $x > 0$, there exists a finite extension K/k, such that $M(K) - N_A(K) > x$.

Proof. For each $m \geq 1$, put $k_m := k(\mu_{p^m})$ and $k_\infty := \bigcup_{m \geq 1} k_m$. By definition, for any $m \geq 1$, we always have

$$m \leq M(k_m). \tag{3.17}$$

By Imai's theorem [13], $\#A(k_\infty)_{\mathrm{tor}} < \infty$. In particular, $N_A(k_\infty) < \infty$. For sufficiently large $m > 0$, we have $A(k_\infty)[p^\infty] = A(k_m)[p^\infty]$. Take such m satisfying

$$m > N_A(k_\infty). \tag{3.18}$$

On the other hand, for any $t \geq 1$,

$$A[p^t] \subset A(k_\infty) \Leftrightarrow A[p^t] \subset A(k_\infty)[p^\infty] = A(k_m)[p^\infty] \Leftrightarrow A[p^t] \subset A(k_m).$$

From these equivalences,

$$A[p^{N_A(k_\infty)+1}] \not\subset A(k_m), \quad \text{and} \quad A[p^{N_A(k_\infty)}] \subset A(k_m). \tag{3.19}$$

Thus we obtain

$$N_A(k_m) \overset{(3.19)}{=} N_A(k_\infty) \overset{(3.18)}{<} m \overset{(3.17)}{\leq} M(k_m).$$

As $N_A(k_\infty)$ does not depend on m and we can take arbitrary large m, the assertion follows by putting $K = k_m$. □

4. Curves

In this section, we give a proof of Theorem 1.1 and also construct the maximal covering of a curve X over k which produces the subgroup $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ of $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$. Throughout this section, we use the following notation:

- X: a projective smooth curve over k with $X(k) \neq \emptyset$ and we additionally assume that X has *good reduction.*
- $\overline{X} := \mathscr{X} \otimes_{\mathcal{O}_k} \mathbb{F}_k$: the special fiber of a regular model $\mathscr{X}$ over $\mathcal{O}_k$ of X,
- $J = \mathrm{Jac}(X)$: the Jacobian variety of X which has good reduction from the assumption on X,
- $\mathscr{J}$: the Néron model over $\mathcal{O}_k$ of J, and
- $\overline{J} := \mathrm{Jac}(\overline{X})$: the Jacobian variety of $\overline{X}$ which is also the closed fiber of $\mathscr{J}$.

Finally, we suppose that $\overline{J}$ is an *ordinary* abelian variety. From this assumption, the Jacobian variety J has good ordinary reduction. We fix a rational point $x \in X(k)$. By the valuative criterion for properness, the rational point x gives rise to an $\mathbb{F}_k$-rational point of $\overline{X}$ which is denoted by $\overline{x} \in \overline{X}(\mathbb{F}_k)$.

Proof of the main theorem. The boundary map ∂_J for J defined in (3.6) is compatible with ∂_X defined in (2.11) as in the following commutative diagram:

$$\begin{tikzcd}
V(X) \arrow[r, two heads, "\partial_X"] \arrow[d, "(2.9)"', "\simeq"] & A_0(\overline{X}) \arrow[d, "\simeq"] \\
K(k; J, \mathbb{G}_m) \arrow[r, two heads, "\partial_J"] & \overline{J}(\mathbb{F}_k),
\end{tikzcd}$$

where the right vertical map is the Abel–Jacobi map $A_0(\overline{X}) \overset{\simeq}{\to} \overline{J}(\mathbb{F}_k)$ which is bijective ([36, Lemma 2.2], see also [1, Lemma 2.12]). Recall that both of ∂_X and ∂_J are surjective, we obtain an isomorphism $\mathrm{Ker}(\partial_X) \overset{\simeq}{\to} \mathrm{Ker}(\partial_J)$. This isomorphism and Theorem 3.7 together with the class field theory

$\mu_X\colon \mathrm{Ker}(\partial_X)_{\mathrm{fin}} \xrightarrow{\simeq} \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ (cf. (2.12)) induce the following main result referred in Theorem 1.1:

Corollary 4.1. *We have surjective homomorphisms:*

$$(\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g} \twoheadrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \twoheadrightarrow (\mathbb{Z}/p^{N_J})^{\oplus g}.$$

When the absolute ramification index $e_k = e_{k/\mathbb{Q}_p}$ of k satisfies $e_k < p-1$, we have $\mu_p \not\subset k^{\mathrm{ur}}$, and this implies $M^{\mathrm{ur}} = 0$. From Corollary 4.1 we recover the following assertion in [16, Proposition 7] (cf. [42, Theorem 3.2, Theorem 4.1]. For more general results, see also [27, Proposition 4.25]).

Corollary 4.2. *Assume $e_k < p-1$. Then, we have $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} = 0$.*

Construction of the maximal covering. In the following, we construct a geometric covering $\varphi\colon \widetilde{X} \to X$ such that the composition

$$\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \hookrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \simeq \mathrm{Gal}(k(X)^{\mathrm{geo}}/k(X)) \twoheadrightarrow \mathrm{Aut}(\varphi)$$

is bijective. The construction of such covering is known classically as the pullback of an appropriate isogeny $\widetilde{J} \to J$ along the Albanese map $f^x\colon X \to J = \mathrm{Jac}(X)$ associated with the given rational point $x \in X(k)$ (cf. [33]). Since we could not find appropriate references, we give precise explanations below: Consider also the Albanese map $f^{\overline{x}}\colon \overline{X} \to \overline{J}$ ([23, Section 6]). We have the middle vertical arrow in the commutative diagram below

$$(4.1)\qquad \begin{tikzcd} X \arrow[r] \arrow[d, "f^x"'] & \mathscr{X} \arrow[d, dashed] & \overline{X} \arrow[l] \arrow[d, "f^{\overline{x}}"] \\ J \arrow[r] & \mathscr{J} & \overline{J} \arrow[l] \end{tikzcd}$$

by the Néron mapping property of $\mathscr{J}$.

Lemma 4.3. *The diagram* (4.1) *above induces $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \simeq \pi_1(J)^{\mathrm{geo}}$ and $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \simeq \pi_1(J)^{\mathrm{geo}}_{\mathrm{ram}}$. Note that all finite étale coverings of J are abelian.*

Proof. Because of $H^2(k,\mathbb{Q}) = H^3(k,\mathbb{Z}) = 0$, and the long sequence arising from $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, we have $H^2(k,\mathbb{Q}/\mathbb{Z}) = 0$. The five-term exact sequence induced by the Hochschild–Serre spectral sequence gives short exact sequences

$$\begin{tikzcd} 0 \arrow[r] & H^1(k,\mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "\simeq"] & H^1_{\mathrm{et}}(X,\mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d] & H^1_{\mathrm{et}}(X\otimes_k \overline{k},\mathbb{Q}/\mathbb{Z})^{G_k} \arrow[r] \arrow[d, "\simeq"] & 0 \\ 0 \arrow[r] & H^1(k,\mathbb{Q}/\mathbb{Z}) \arrow[r] & H^1_{\mathrm{et}}(J,\mathbb{Q}/\mathbb{Z}) \arrow[r] & H^1_{\mathrm{et}}(J\otimes_k \overline{k},\mathbb{Q}/\mathbb{Z})^{G_k} \arrow[r] & 0. \end{tikzcd}$$

The sequences are exact on the right because the group $H^2(k,\mathbb{Q}/\mathbb{Z})$ vanishes. Here, the right vertical map is bijective, because f^x induces an isomorphism $\pi_1^{\mathrm{ab}}(X\otimes_k \overline{k}) \simeq \pi_1(J\otimes_k \overline{k}) = \pi_1^{\mathrm{ab}}(J\otimes_k \overline{k})$ ([23, Proposition 9.1]).

We obtain $\pi_1^{\mathrm{ab}}(X) \simeq H^1_{\mathrm{et}}(X, \mathbb{Q}/\mathbb{Z})^\vee \simeq H^1_{\mathrm{et}}(J, \mathbb{Q}/\mathbb{Z})^\vee \simeq \pi_1(J)$. In the same way, we also obtain $\pi_1^{\mathrm{ab}}(\overline{X}) \simeq \pi_1(\overline{J})$. Thus, we obtain $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \simeq \pi_1(J)^{\mathrm{geo}}$ and $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \simeq \pi_1(J)^{\mathrm{geo}}_{\mathrm{ram}}$. □

It follows by Corollary 4.1 that there is an isomorphism

$$\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \simeq \bigoplus_{i=1}^{g} \mathbb{Z}/p^{r_i},$$

for some integers $N_J \leq r_i \leq M^{\mathrm{ur}}$, $i = 1, \ldots, g$. In particular, this implies that $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ has a subgroup isomorphic to $(\mathbb{Z}/p^{N_J})^{\oplus g}$. We wish to find an explicit finite abelian covering $X' \to X$ whose Galois group coincides with the aforementioned subgroup of $\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$. This is of course only interesting when $N_J \geq 1$. Put $N := N_J$ and suppose $N \geq 1$. Consider the splitting

$$J[p^N] \simeq \widehat{J}[p^N] \oplus \overline{J}[p^N] \simeq (\mu_{p^N})^{\oplus g} \oplus (\mathbb{Z}/p^N)^{\oplus g}$$

induced by the connected-étale short exact sequence for J (cf. (3.3)). Put $H_N := \overline{J}[p^N]$ and consider it as a subgroup of $J[p^N]$. This induces an isogeny $\psi : J \to J/H_N =: J_N$ with kernel H_N ([24, Example 4.40]). Let $\check{\psi} : J_N \to J$ be its dual ([24, Proposition 5.12]).

Proposition 4.4. *The isogeny $\check{\psi} : J_N \to J$ is a geometric covering which is completely unramified over $\overline{J}$. Furthermore, we have* $\mathrm{Aut}(\check{\psi}) \simeq (\mathbb{Z}/p^N)^{\oplus g}$.

Proof. Abelian covering. It is known that any isogeny on abelian varieties is finite flat ([24, Proposition 5.2]) and we are working over a characteristic 0 field, hence the isogeny $\check{\psi} : J_N \to J$ is finite étale ([24, Proposition 5.6]). The map $\mathrm{Ker}(\check{\psi}) \to \mathrm{Aut}(\check{\psi})$ which sends $\xi \in \mathrm{Ker}(\check{\psi})$ to the automorphism given by the translation by ξ is bijective, because any non-constant homomorphism is the composition of an isogeny and a translation by some ξ ([24, Proposition 1.14]). Since $\mathrm{Aut}(\check{\psi})$ acts transitively on the fibers $\mathrm{Ker}(\check{\psi})$, the covering $\check{\psi}$ is Galois with Galois group $\mathrm{Aut}(\check{\psi}) \simeq \mathrm{Ker}(\check{\psi}) \simeq (\mathbb{Z}/p^N)^{\oplus g}$.

Geometric covering. Next, we show that $\check{\psi}$ is a geometric covering of J. As we recalled in Section 2, using the zero $0_J \in J(k)$, it suffices to show that the fiber $(J_N)_0$ over 0_J

$$\begin{tikzcd}
J_N \arrow[d, "\check{\psi}"'] & (J_N)_0 = J_N \times_J 0_J \arrow[l] \arrow[d] \\
J & \mathrm{Spec}(k) \arrow[l, "0_J"']
\end{tikzcd}$$

is completely split over $\mathrm{Spec}(k)$. In fact, we have $(J_N)_0 \simeq \mathrm{Ker}(\check{\psi})$ as schemes and the later $\mathrm{Ker}(\check{\psi})$ is precisely the subgroup $\psi(\widehat{J}[p^N])$, which is k-rational by assumption. Therefore, $(J_N)_0$ is the sum of k-rational points, and hence $\check{\psi}\colon J_N \to J$ is a geometric covering of J.

Completely ramified. Finally, we show that the geometric covering $\check{\psi}\colon J_N \to J$ is completely ramified over $\overline{J}$. Suppose that $\check{\psi}$ contains a sub covering $\phi\colon A \to J$ unramified over $\overline{J}$. Since the isogeny $\check{\psi}$ maps 0 in J_N to 0 in J, there exists a rational point $e \in A(k)$ such that $\phi(e) = 0$. From the Lang–Serre theorem ([24, Theorem 10.36]), A is an abelian variety. Let $\mathscr{A}$ be the Néron model of A and $\overline{A}$ its closed fiber. By the functorial property of the Néron models ([2, Section 7.3, Proposition 6]) there exists an isogeny $\Phi\colon \mathscr{A} \to \mathscr{J}$ which makes the following diagram commutative:

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\phi"'] & \mathscr{A} \arrow[d, "\Phi"'] & \overline{A} \arrow[l] \arrow[d, "\bar{\phi}"] \\
J \arrow[r] & \mathscr{J} & \overline{J}. \arrow[l]
\end{tikzcd} \tag{4.2}$$

Claim. The isogenies $\bar{\phi}$ and Φ are étale. In particular, in the correspondence between the set of abelian coverings of J unramified over $\overline{J}$ and that of abelian coverings of $\overline{J}$ referred in Section 2, the isogeny ϕ comes from the above diagram (4.2) with the isogeny $\Phi\colon \mathscr{A} \to \mathscr{J}$ of the Néron models.

Proof. The kernel $\mathrm{Ker}(\Phi)$ of the induced isogeny Φ is a finite group scheme ([24, Proposition 5.2]). Consider the connected-étale sequence

$$0 \longrightarrow \mathrm{Ker}(\Phi)^{\circ} \longrightarrow \mathrm{Ker}(\Phi) \longrightarrow \mathrm{Ker}(\Phi)^{\mathrm{et}} \longrightarrow 0$$

([24, Proposition 4.45]). We can factor Φ as a composition of two isogenies $\mathscr{A} \to \mathscr{A}/\,\mathrm{Ker}(\Phi)^{\circ} \overset{\Phi^{\mathrm{et}}}{\to} \mathscr{J}$. In the same way, $\bar{\phi}$ can be written $\overline{A} \to \overline{A}/\,\mathrm{Ker}(\bar{\phi})^{\circ} \overset{\bar{\phi}^{\mathrm{et}}}{\to} \overline{J}$. Putting $\mathscr{A}^{\mathrm{et}} := \mathscr{A}/\,\mathrm{Ker}(\Phi)^{\circ}$ and $\overline{A}^{\mathrm{et}} := \overline{A}/\,\mathrm{Ker}(\bar{\phi})^{\circ}$, they make the following diagram commutative:

$$\begin{tikzcd}
A \arrow[rr] \arrow[dr, dashed] \arrow[dd, "\phi"'] & & \mathscr{A} \arrow[dr] \arrow[dd] & & \overline{A} \arrow[ll] \arrow[dr] \arrow[dd] & \\
& A^{\mathrm{et}} \arrow[rr, dashed] \arrow[dl, dashed, "\phi^{\mathrm{et}}"] & & \mathscr{A}^{\mathrm{et}} \arrow[dl, "\Phi^{\mathrm{et}}"] & & \overline{A}^{\mathrm{et}} \arrow[ll] \arrow[dl, "\bar{\phi}^{\mathrm{et}}"] \\
J \arrow[rr] & & \mathscr{J} & & \overline{J} \arrow[ll] & ,
\end{tikzcd}$$

where $\phi^{\mathrm{et}}\colon A^{\mathrm{et}} \to J$ is given by taking the generic fiber of Φ^{et}. Here, Φ^{et} and ϕ^{et} are isogenies whose kernels are étale group schemes so that Φ^{et} and ϕ^{et} are étale ([24, Proposition 5.6]). From this, ϕ^{et} is an abelian covering of J which is unramified over $\overline{J}$.

Since ϕ is unramified over $\overline{J}$ (and $A \to A^{\mathrm{et}}$ is not unramified over $\overline{A}^{\mathrm{et}}$), we have $A \simeq A^{\mathrm{et}}$. This implies that $\mathscr{A} \simeq \mathscr{A}^{\mathrm{et}}$ and $\overline{A} \simeq \overline{A}^{\mathrm{et}}$ and the assertions follow. □

Let $\mathscr{J}_N$ be the Néron model of J_N. Extending the diagram (4.2), we have the following commutative diagram:

$$\begin{tikzcd}
J_N \arrow[r] \arrow[d] \arrow[dd, bend right=60, "\check{\psi}"'] & \mathscr{J}_N \arrow[d] \arrow[dd, dashed, bend right] & \bar{J}_N \arrow[l] \arrow[d] \arrow[dd, bend left=60, "\bar{\psi}"] \\
A \arrow[r] \arrow[d, "\phi"] & \mathscr{A} \arrow[d] & \bar{A} \arrow[l] \arrow[d, "\bar{\phi}"'] \\
J \arrow[r] & \mathscr{J} & \bar{J}. \arrow[l]
\end{tikzcd}$$

From the functorial property of Néron models, the above diagram is commutative. Here, $\bar{\phi}$ is étale. From the construction of J_N, $\check{\bar{\psi}}\colon \bar{J}_N \xrightarrow{\simeq} \bar{J}$ is an isomorphism and so is $\bar{\phi}$. This implies that $\phi\colon A \to J$ is an isomorphism. Therefore, $\check{\psi}$ does not contain sub abelian coverings of J which are unramified over $\bar{J}$. □

It follows (see e.g., [23, Section 9]) that the pull-back

$$\begin{tikzcd}
X_N \arrow[r] \arrow[d, "\varphi"'] & J_N \arrow[d, "\check{\psi}"] \\
X \arrow[r, "f^x"] & J
\end{tikzcd}$$

of $\check{\psi}$ along $f^x\colon X \to J$ defines an étale covering of X. From the construction of X_N and the universal property of the Albanese map f^x, we have $\mathrm{Aut}(\check{\psi}) \simeq \mathrm{Aut}(\varphi)$.

Theorem 4.5. *Suppose we have* $\mathrm{Ker}(\partial_X)_{\mathrm{fin}} \simeq (\mathbb{Z}/p^{N_J})^{\oplus g}$ *with* $N := N_J \geq 1$. *The étale covering* $\varphi : X_N \to X$ *is a geometric covering which is completely ramified over* $\overline{X}$. *Furthermore, the composition*

$$\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \hookrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \twoheadrightarrow \mathrm{Aut}(\varphi)$$

is bijective.

Proof. From Proposition 4.4, the right vertical map in the following commutative diagram is surjective

$$\begin{tikzcd}
\mathrm{Aut}(\varphi) \arrow[r, "f^x", "\simeq"'] & \mathrm{Aut}(\check{\psi}) \\
\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \arrow[u] \arrow[r, "f^x", "\simeq"'] & \pi_1(J)^{\mathrm{geo}}. \arrow[u, two heads]
\end{tikzcd}$$

Thus, the left vertical map is surjective, and hence $\varphi\colon X_N \to X$ is a geometric (abelian) covering of X.

Recall that we have $(\mathbb{Z}/p^N)^{\oplus g} \simeq \operatorname{Ker}(\partial_X)_{\mathrm{fin}} \simeq \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}}$ and $\operatorname{Aut}(\varphi) \simeq \operatorname{Aut}(\check{\psi}) \simeq (\mathbb{Z}/p^N)^{\oplus g}$ (Proposition 4.4). Consider the following commutative diagram:

$$\begin{tikzcd}
\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \arrow[r, hook] \arrow[d, "\simeq"] & \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \arrow[r, two heads] \arrow[d, "\simeq"] & \operatorname{Aut}(\varphi) \arrow[d, "\simeq"] \\
\pi_1(J)^{\mathrm{geo}}_{\mathrm{ram}} \arrow[r, hook] & \pi_1(J)^{\mathrm{geo}} \arrow[r, two heads] & \operatorname{Aut}(\check{\psi}).
\end{tikzcd}$$

From Proposition 4.4, the composition of the bottom maps is bijective, so is the top map. This implies that $\varphi\colon X_N \to X$ is completely ramified over $\overline{X}$ and is maximal. □

Remark 4.6. The assumption in Theorem 4.5 holds if we have $N_J = M^{\mathrm{ur}}$ (see Remark 1.2). In Theorem 5.3 below, we also consider elliptic curves which satisfy this assumption.

Products of curves. The above results can be extended to products of curves. For a product $X = X_1 \times \cdots \times X_d$ of smooth and projective curves X_i over k with good reduction and $X_i(k) \neq \emptyset$ for all i, we have a short exact sequence $0 \to V(X) \to SK_1(X) \overset{N}{\to} k^\times \to 0$ and the reciprocity map $\tau_X\colon V(X) \to \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}$ defined similarly as in (2.8) (cf. [31, Section 1]). There is a commutative diagram

$$\begin{tikzcd}
V(X) \arrow[r, "\simeq"] \arrow[d, "\tau_X"] & \displaystyle\bigoplus_{i=1}^{d} V(X_i) \oplus \widetilde{V}(X) \arrow[d, "\oplus\tau_{X_i}"] \\
\pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \arrow[r, "\simeq"] & \displaystyle\bigoplus_{i=1}^{d} \pi_1^{\mathrm{ab}}(X_i)^{\mathrm{geo}},
\end{tikzcd}$$

where $\widetilde{V}(X)$ is a divisible group ([41, Proposition 1.7 and Corollary 2.5, see also the proof of Theorem 1.1]). From the decomposition of $V(X)$, one define the boundary map

$$\partial_X\colon V(X) \xrightarrow{\text{projection}} \bigoplus_{i=1}^{d} V(X_i) \overset{\oplus\partial_{X_i}}{\longrightarrow} \bigoplus_{i=1}^{d} A_0(\overline{X}_i) \simeq \bigoplus_{i=1}^{d} \overline{J}_i(\mathbb{F}_k),$$

where $\overline{J}_i$ is the Jacobian variety of the special fiber $\overline{X}_i$ for each i. Here, the target of the boundary map ∂_X can be considered as the Albanese variety $\operatorname{Alb}(\overline{X})(\mathbb{F}_k) = \bigoplus_i \overline{J}_i(\mathbb{F}_k)$, where $\overline{X} = \overline{X}_1 \times \cdots \times \overline{X}_d$. This induces the commutative diagram with horizontal exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\partial_X) \arrow[r] \arrow[d, dashed, two heads, "\mu_X"] & V(X) \arrow[r] \arrow[d, two heads, "\tau_X"] & \displaystyle\bigoplus_{i=1}^{d} \bar{J}_i(\mathbb{F}_k) \arrow[r] \arrow[d, "\oplus\rho_{\bar{X}_i}", "\simeq"'] & 0 \\
0 \arrow[r] & \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \arrow[r] & \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}} \arrow[r] & \displaystyle\bigoplus_{i=1}^{d} \pi_1^{\mathrm{ab}}(\overline{X}_i)^{\mathrm{geo}} \arrow[r] & 0.
\end{tikzcd}$$

From the top horizontal sequence, we have a decomposition

$$\mathrm{Ker}(\partial_X) \simeq \mathrm{Ker}(\partial_X)_{\mathrm{fin}} \oplus \mathrm{Ker}(\partial_X)_{\mathrm{div}}$$

(Lemma 2.2 (iii)), with $\mathrm{Ker}(\partial_X)_{\mathrm{fin}} \simeq \bigoplus_i \mathrm{Ker}(\partial_{X_i})_{\mathrm{fin}}$ and $\mathrm{Ker}(\partial_X)_{\mathrm{div}} = \widetilde{V}(X)$. Since μ_X induces an isomorphism

$$\mathrm{Ker}(\partial_X)_{\mathrm{fin}} \simeq \bigoplus_{i=1}^{d} \mathrm{Ker}(\partial_{X_i})_{\mathrm{fin}} \xrightarrow{\simeq} \bigoplus_{i=1}^{d} \pi_1^{\mathrm{ab}}(X_i)^{\mathrm{geo}}_{\mathrm{ram}} \simeq \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}},$$

Theorem 3.7 gives the following corollary.

Corollary 4.7. *Let $X = X_1 \times \cdots \times X_d$ be a product of smooth and projective curves over k with good reduction, and $X_i(k) \neq \emptyset$ for all $1 \leq i \leq d$. Assume that the Jacobian variety $\overline{J}_i := \mathrm{Jac}(\overline{X}_i)$ has ordinary reduction for each $1 \leq i \leq d$. Then, there are surjective homomorphisms*

$$\bigoplus_{i=1}^{d} (\mathbb{Z}/p^{M^{\mathrm{ur}}})^{\oplus g_i} \twoheadrightarrow \pi_1^{\mathrm{ab}}(X)^{\mathrm{geo}}_{\mathrm{ram}} \twoheadrightarrow \bigoplus_{i=1}^{d} (\mathbb{Z}/p^{N_{J_i}})^{\oplus g_i},$$

where $g_i = \dim(J_i)$.

5. Elliptic curve

In this section, we consider an elliptic curve $X = E$ over k which has good reduction. Recalling from Lemma 2.10, we have a decomposition $\mathrm{Ker}(\partial_E) \simeq \mathrm{Ker}(\partial_E)_{\mathrm{fin}} \oplus \mathrm{Ker}(\partial_E)_{\mathrm{div}}$. We will obtain a sharp computation of the group $\mathrm{Ker}(\partial_E)_{\mathrm{fin}}$ under some mild assumptions on E. *From now on* we will simply write N for the integer N_E.

Good ordinary reduction. First, we assume that E has good ordinary reduction. Theorem 3.7 gives surjections

$$\mathbb{Z}/p^{M^{\mathrm{ur}}} \twoheadrightarrow \mathrm{Ker}(\partial_E)_{\mathrm{fin}} \twoheadrightarrow \mathbb{Z}/p^{N}.$$

Recall that we have the invariants

$$\widehat{N} = \max\{m \geq 0 \mid \widehat{E}[p^m] \subset \widehat{E}(k)\}, \text{ and } M = \max\{m \geq 0 \mid \mu_{p^m} \subset k\}.$$

In general, we have $N \leq \widehat{N} \leq M^{\mathrm{ur}}$ as noted in Remark 3.8.

Lemma 5.1. *Let $G \subset G_k$ be a closed subgroup, and T a free $\mathbb{Z}_p$-module of rank 1 with non-trivial G-action $\chi : G \to \operatorname{Aut}(T)$. Then, we have isomorphisms*

$$T_G \simeq \varprojlim_n [(T/p^n)_G] \simeq T/p^{M_G},$$

where $M_G = \max\{m \,|\, G$ acts on T/p^m trivially$\}$.

Proof. Put $T_n := T/p^n$ and $m := M_G$. Take a generator (z_n) of $\varprojlim_n T_n = T$ with $z_n \in T_n$. We will show that, for any $n \geq m$, the natural map $T_n \twoheadrightarrow T_m$ induces $(T_n)_G \overset{\simeq}{\to} T_m$. The mod p^n-representation $\chi_n : G \overset{\chi}{\to} \operatorname{Aut}(T) \twoheadrightarrow \operatorname{Aut}(T_n)$ factors through a finite cyclic subgroup $G_n \subset G$. Fix a generator σ_n of G_n. Thus, $(T_n)_G = T_n/I_G(T_n)$, where $I_G(T_n) := \langle (\chi_n(\sigma_n) - 1)x \,|\, x \in T_n \rangle$. Then $\chi_n(\sigma_n)(z_n) = a_n z_n$ for some $a_n \in (\mathbb{Z}/p^n)^{\times}$. Since G acts on T_m trivially, $a_n z_n \bmod p^m = z_n \bmod p^m$ in T_m and hence $a_n \bmod p^m = 1$. Write $a_n - 1 = p^m l_n$. This equality means precisely that the subgroup $I_G(T_n)$ is contained in $p^m T_n$. To prove the reverse inclusion it is enough to show that $(l_n, p) = 1$. Assume for contradiction that $p \mid l_n$. This yields

$$\chi_n(\sigma_n) z_n \bmod p^{m+1} = a_n z_n \bmod p^{m+1} = z_n \bmod p^{m+1} \text{ in } T_{m+1}.$$

But this means that G acts trivially on T_{m+1}, which contradicts the definition of the integer $m = M_G$.

To finish the proof we consider the following commutative diagram with exact rows,

$$\begin{tikzcd}
0 \arrow[r] & I_G(T_n) \arrow[r] \arrow[d] & T_n \arrow[r] \arrow[d, equal] & (T_n)_G \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & p^m T_n \arrow[r] & T_n \arrow[r] & T_m \arrow[r] & 0.
\end{tikzcd}$$

The first two vertical maps are equalities, giving the desired isomorphism $(T_n)_G \simeq T_m$. In the appendix we prove an isomorphism $T_G \simeq \varprojlim_n [(T_n)_G]$ (cf. Proposition A.1). □

Proposition 5.2. *There are surjective homomorphisms*

$$\mathbb{Z}/p^{\widehat{N}} \twoheadrightarrow \operatorname{Ker}(\partial_E)_{\mathrm{fin}} \twoheadrightarrow \mathbb{Z}/p^N.$$

The inequality $N \leq \widehat{N}$ can be strict.

Proof. From Lemma 3.2 we have an isomorphism

$$\operatorname{Ker}(\partial_E)_{\mathrm{fin}} \simeq \operatorname{Im}((T_p(\mathscr{E})^{\circ})_{G_k} \xrightarrow{\iota} T_p(E)_{G_k}).$$

Note that the injectivity of the Galois symbol map follows from (2.10). By the definition of N, G_k acts on $E[p^N]$ trivially and so does on $\widehat{E}[p^N]$. We obtain

$$\operatorname{Im}((T_p(\mathscr{E})^{\circ})_{G_k} \xrightarrow{\iota} T_p(E)_{G_k}) \simeq \operatorname{Im}(\widehat{E}[p^N] \hookrightarrow E[p^N]) \simeq \mathbb{Z}/p^N.$$

From Lemma 5.1, $(T_p(\mathscr{E})^\circ)_{G_k} \simeq \widehat{E}[p^{\widehat{N}}] \simeq \mathbb{Z}/p^{\widehat{N}}$ and this implies the assertion. It is clear that if $\widehat{E}[p^{\widehat{N}}] \not\subset \overline{E}(\mathbb{F}_k)$, the inequality $N \leq \widehat{N}$ becomes strict. □

Let $\mathscr{E}$ be the Néron model of E. For every $n \geq 1$, consider the connected-étale exact sequence of finite flat group schemes over $\mathrm{Spec}(\mathcal{O}_k)$ (cf. (3.2)),

$$0 \longrightarrow \mathscr{E}[p^n]^\circ \longrightarrow \mathscr{E}[p^n] \longrightarrow \mathscr{E}[p^n]^{\mathrm{et}} \longrightarrow 0. \tag{5.1}$$

When E has complex multiplication, (5.1) splits ([34, A.2.4]). Equivalently, the G_k-action on $E[p^n]$ is diagonal for all $n \geq 1$. We will refer to this as the *semisimple case*. In general (5.1) does not split and the G_k-action on $E[p^n]$ is upper triangular. Over k^{ur} the sequence (5.1) becomes

$$0 \longrightarrow \mu_{p^n} \longrightarrow \mathscr{E}[p^n] \longrightarrow \mathbb{Z}/p^n \longrightarrow 0. \tag{5.2}$$

Passing to the limit we obtain a short exact sequence of continuous $G_{k^{\mathrm{ur}}}$-modules

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow T_p(E) \longrightarrow \mathbb{Z}_p \longrightarrow 0. \tag{5.3}$$

When E has complex multiplication, (5.3) splits; that is, $T_p(E)$ is semisimple as $G_{k^{\mathrm{ur}}}$-module. Suppose we are in the non-semisimple case. Assume additionally that $\mu_{p^n} \subset k$ and that $\overline{E}[p^n] \subset \overline{E}(\mathbb{F}_k)$ for some n. Then the sequence (5.2) is given over k. In particular, the group scheme $\mathscr{E}[p^n]$ defines an element of $\mathcal{E}xt^1_{\mathcal{O}_k}(\mathbb{Z}/p^n, \mu_{p^n}) \simeq H^1_{fppf}(\mathcal{O}_k, \mu_{p^n})$. This group is isomorphic to $\mathcal{O}_k^\times/p^n$ and therefore the extension $\mathscr{E}[p^n]$ (or equivalently the Galois module $E[p^n]$) corresponds to a unit $u \in \mathcal{O}_k^\times/p^n$. That is, the sequence (5.2) becomes split after extending to the finite extension $k(\sqrt[p^n]{u})$. The unit u is known as the *Serre–Tate parameter* of E and it is trivial when E has complex multiplication. For more information we refer to [18, Chapter 8, Section 9].

Theorem 5.3. *Let $\rho_n \colon G_k \to \mathrm{Aut}(E[p^n])$ be the mod p^n representation arising from $E[p^n]$ for any $n \geq 1$.*

(i) *If $\rho_{\widehat{N}}$ is semisimple, then* $\mathrm{Ker}(\partial_E)_{\mathrm{fin}} \simeq \mathbb{Z}/p^{\widehat{N}}$.

(ii) *If $\rho_{\widehat{N}}$ is non semisimple, we further assume that $M = M^{\mathrm{ur}}$, $\overline{E}[p^M] \subset \overline{E}(\mathbb{F}_k)$ and the restriction $\rho_{N+1}|_{I_k}$ of the mod p^{N+1} representation ρ_{N+1} to the inertia subgroup $I_k \subset G_k$ is also non semisimple. Then, we have $\widehat{N} = M$, and an isomorphism* $\mathrm{Ker}(\partial_E)_{\mathrm{fin}} \simeq \mathbb{Z}/p^N$. *That is, the lower bound is achieved and the inequality $N \leq M = M^{\mathrm{ur}}$ can be strict.*

Proof. If $N = \widehat{N}$ there is nothing to show, so we assume $N < \widehat{N}$.

(i). As in the proof of Proposition 5.2, $\mathrm{Ker}(\partial_E)_{\mathrm{fin}} \simeq \mathrm{Im}((T_p(\mathscr{E})^\circ)_{G_k} \xrightarrow{\iota} T_p(E)_{G_k})$ and $T_p(\mathscr{E})^\circ \simeq \mathbb{Z}/p^{\widehat{N}}$. From the assumption, the sequences (5.1) are split for all $n \geq 1$ and hence $(T_p(\mathscr{E})^\circ)_{G_k} \xrightarrow{\iota} T_p(E)_{G_k}$ is injective. This implies that $\mathbb{Z}/p^{\widehat{N}} \simeq T_p(\mathscr{E})^\circ \simeq \mathrm{Ker}(\partial_E)_{\mathrm{fin}}$.

(ii). Consider the short exact sequence

$$0 \longrightarrow \widehat{E}[p^M] \longrightarrow E[p^M] \longrightarrow \overline{E}[p^M] \longrightarrow 0 \tag{5.4}$$

as G_k-modules from (3.3). From the assumption $\overline{E}[p^M] \subset \overline{E}(\mathbb{F}_k)$, the Galois invariance of the Weil pairing ([35, Chapter III, Proposition 8.1]) implies that the determinant of the mod p^M representation

$$G_k \xrightarrow{\rho_M} \mathrm{Aut}(E[p^M]) \simeq GL_2(\mathbb{Z}/p^M) \xrightarrow{\det} (\mathbb{Z}/p^M)^\times$$

coincides with the cyclotomic character $\chi_M \colon G_k \to \mu_{p^M}$ by fixing a primitive p^M-th root of unity ζ which is in k. We have $\widehat{E}[p^M] \simeq \mu_{p^M}$ as G_k-modules and hence $M \leq \widehat{N}$. As we assumed $M = M^{\mathrm{ur}}$, we have $M = \widehat{N}$. The above short exact sequence (5.4) becomes

$$0 \longrightarrow \mu_{p^M} \xrightarrow{\iota_M} E[p^M] \xrightarrow{\pi_M} \mathbb{Z}/p^M \longrightarrow 0. \tag{5.5}$$

Let $\zeta = \zeta_{p^M}$ be a fixed primitive p^M-th root of unity in k. Fix a basis (z, y) of $E[p^M]$ where $z = \iota_M(\zeta) \in E[p^M]$ and $\overline{E}[p^M]$ is generated by the reduction of y. This gives $\mathrm{Aut}(E[p^M]) \simeq GL_2(\mathbb{Z}/p^M)$. If the sequence (5.5) splits, then by taking the mod p^{N+1}

$$\begin{tikzcd}
G_k \arrow[r, "\rho_M"] \arrow[dr, "\rho_{N+1}"'] & GL_2(\mathbb{Z}/p^M) \arrow[d, "\bmod p^{N+1}"] \\
& GL_2(\mathbb{Z}/p^{N+1})
\end{tikzcd}$$

the mod p^{N+1} representation ρ_{N+1} becomes semisimple, which contradicts the assumption that the restriction of ρ_{N+1} to the inertia subgroup is irreducible. We conclude that the above short exact sequence (5.5) is non-split.

Applying G_k-coinvariance to (5.5) we obtain an exact sequence of abelian groups,

$$(\mu_{p^M})_{G_k} \xrightarrow{\iota_M} E[p^M]_{G_k} \xrightarrow{\pi_M} (\mathbb{Z}/p^M)_{G_k} \longrightarrow 0.$$

Claim 1. There is an isomorphism $\mathrm{Im}((\mu_{p^M})_{G_k} \xrightarrow{\iota_M} E[p^M]_{G_k}) \simeq \mu_{p^N} \simeq \mathbb{Z}/p^N$.

Proof. The following are true for the sequence (5.5): Its corresponding Serre–Tate parameter $u \in \mathcal{O}_k^\times/p^M$ is nontrivial. The G_k-action on $E[p^M]$ factors through the cyclic quotient $\mathrm{Gal}(k(u^{1/p^M})/k)$. Let $\sigma \in G_k$ be a lift of a generator of the Galois group $\mathrm{Gal}(k(u^{1/p^M})/k)$. For the mod p^M representation $\rho_M \colon G_k \to \mathrm{Aut}(E[p^M]) = GL_2(\mathbb{Z}/p^M)$, we have $\rho_M(\sigma) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$

for some $b \in \mathbb{Z}/p^M$. Namely, $\sigma(z,0) = (z,0)$ and $\sigma(0,y) = (bz, y)$. Consider the map defined by the multiplication by $p^{M-N} \colon E[p^M] \to E[p^N]$ and $(p^{M-N}z, p^{M-N}y)$ is a basis of $E[p^N]$. The following diagram is commutative

$$\begin{tikzcd}
G_k \arrow[r, "\rho_M"] \arrow[dr, "\rho_N"'] & GL_2(\mathbb{Z}/p^M) \arrow[d, "\operatorname{mod} p^N"] \\
& GL_2(\mathbb{Z}/p^N).
\end{tikzcd}$$

Since the action of G_k on $E[p^N]$ is trivial, we have $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod p^N$ and hence $b \equiv 0 \bmod p^N$. If we suppose $b \equiv 0 \bmod p^{N+1}$, then the action of G_k on $E[p^{N+1}]$ becomes trivial so that b is not divisible by p^{N+1}.

Next, we show that $\operatorname{Ker}(\mu_{p^M} \overset{\iota_M}{\to} E[p^M]_{G_k}) = \langle \zeta^b \rangle$. Since $(\mu_{p^M})_{G_k} = \mu_{p^M}$, ζ^b is a non-trivial element of $(\mu_{p^M})_{G_k}$. In fact, it is a primitive p^{M-N}-th root of unity. We have

$$\iota_M(\zeta^b) = (bz, 0) = \sigma(0,y) - (0,y) = 0 \in E[p^M]_{G_k}.$$

This proves $\langle \zeta^b \rangle \subseteq \operatorname{Ker}(\mu_{p^M} \overset{\iota_M}{\to} E[p^M]_{G_k})$. Conversely, take any x in the kernel $\operatorname{Ker}(\mu_{p^M} \overset{\iota_M}{\to} E[p^M]_{G_k})$. Since the G_k-action is cyclic, this means that there exists some $w \in E[p^M]$ such that $\iota_M(x) = \sigma(w) - w$ in $E[p^M]$. Since the G_k-action on μ_{p^M} is trivial, we may assume that $w = l(0,y)$ for some $l \in \mathbb{Z}/p^M$. Then $\iota_M(x) = l(\sigma(0,y) - (0,y)) = lbz = l \cdot \iota_M(\zeta^b)$. This implies $\operatorname{Ker}(\mu_{p^M} \overset{\iota_M}{\to} E[p^M]_{G_k}) = \langle \zeta^b \rangle$. We conclude that there is an exact sequence

$$0 \longrightarrow \mu_{p^M}/\langle \zeta^b \rangle \xrightarrow{\iota_M} E[p^M]_{G_k} \xrightarrow{\pi_M} \mathbb{Z}/p^M \longrightarrow 0.$$

Finally notice that we have an isomorphism $\mu_{p^M}/\langle \zeta^b \rangle \simeq \mu_{p^N}$, since $\langle \zeta^b \rangle \simeq \mu_{p^{M-N}}$, which yields the desired isomorphism $\operatorname{Im}(\iota_M) \simeq \mu_{p^N} \simeq \mathbb{Z}/p^N$. □

Claim 2. The extension $k(E[p^M])/k$ is totally ramified.

Proof. Let G be the image of the Galois representation

$$\rho_M : G_k \longrightarrow \operatorname{Aut}(E[p^M]) = GL_2(\mathbb{Z}/p^M).$$

We have $G \simeq \operatorname{Gal}(k(E[p^M])/k)$. As noted in the proof of Claim 1, G is generated by $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ with $b \equiv 0 \bmod p^N$. We have $\#G \le p^{M-N}$. We denote by I the image of the inertia subgroup $I_k = G_{k^{\mathrm{ur}}}$ by ρ_M which is isomorphic to the inertia subgroup of $\operatorname{Gal}(k(E[p^M])/k)$. Since $I \subset G$, it is isomorphic to an additive subgroup of $\mathbb{Z}/p^M$, and hence I can be written as

$$I = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| \, x \in p^t(\mathbb{Z}/p^M) \right\},$$

for some $N \le t \le M$. We consider what happens mod p^{N+1}. If we assume $N < t$, then $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in I$ for $x \in p^t(\mathbb{Z}/p^M)$ is the identity mod p^{N+1}, and

$x \equiv 0 \bmod p^{N+1}$. The action of I_k on $E[p^{N+1}]$ is trivial. This contradicts the assumption that $\rho_{N+1}|_{I_k}$ is irreducible. Therefore, $t = N$ and hence $\#I = p^{M-N} = \#G$. The extension $k(E[p^M])/k$ is totally ramified. □

Claim 3. We have an isomorphism

$$\mathrm{Im}((T_p(\mathscr{E})^\circ)_{G_k} \xrightarrow{\iota} T_p(E)_{G_k}) \simeq \mathrm{Im}(\mu_{p^M} \longrightarrow E[p^M]_{G_k}).$$

Proof. In the appendix (cf. Proposition A.1) we prove that there are isomorphisms $T_p(E)_{G_k} \simeq \varprojlim_n (E[p^n]_{G_k})$ and $T_p(E)_{I_k} \simeq \varprojlim_n (E[p^n]_{I_k})$. We have commutative diagrams

$$\begin{tikzcd}
(T_p(\mathscr{E})^\circ)_{I_k} \arrow[r, "\iota"] \arrow[d, "\simeq"] & T_p(E)_{I_k} \arrow[d, two heads] \\
(\mu_{p^M})_{I_k} \arrow[r, "\iota_M"] & E[p^M]_{I_k}.
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
(T_p(\mathscr{E})^\circ)_{G_k} \arrow[r, "\iota"] \arrow[d, "\simeq"] & T_p(E)_{G_k} \arrow[d, two heads] \\
(\mu_{p^M})_{G_k} \arrow[r, "\iota_M"] & E[p^M]_{G_k}.
\end{tikzcd}$$

Here, the left vertical map in each diagram is bijective by Lemma 5.1 and the assumption $M = M^{\mathrm{ur}}$. Consider the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Im}((T_p(\mathscr{E})^\circ)_{I_k} \xrightarrow{\iota} T_p(E)_{I_k}) \arrow[r, two heads] \arrow[d, two heads] & \mathrm{Im}((T_p(\mathscr{E})^\circ)_{G_k} \xrightarrow{\iota} T_p(E)_{G_k}) \arrow[d, two heads] \\
\mathrm{Im}((\mu_{p^M})_{I_k} \xrightarrow{\iota_M} E[p^M]_{I_k}) \arrow[r, "\simeq"] & \mathrm{Im}((\mu_{p^M})_{G_k} \xrightarrow{\iota_M} E[p^M]_{G_k}).
\end{tikzcd}$$

Here, the bottom horizontal map is bijective because of Claim 2. Thus, it is enough to prove the injectivity of the left vertical map in the above diagram. It suffices to show that for every $r > M$ we have an isomorphism $\mathrm{Im}((\mu_{p^r})_{I_k} \xrightarrow{\iota_r} E[p^r]_{I_k}) \simeq \mathrm{Im}((\mu_{p^M})_{I_k} \xrightarrow{\iota_M} E[p^M]_{I_k})$. This will follow by Lemma 5.1 and the snake lemma. We have a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & & 0 \arrow[d] & \\
(\mu_{p^{r-M}})_{I_k} \arrow[r, "\iota_{r-M}"] \arrow[d, "\alpha"] & E[p^{r-M}]_{I_k} \arrow[r, "\pi_{r-M}"] \arrow[d] & \mathbb{Z}/p^{r-M} \arrow[r] \arrow[d] & 0 \\
(\mu_{p^r})_{I_k} \arrow[r, "\iota_r"] \arrow[d, "\beta"] & E[p^r]_{I_k} \arrow[r, "\pi_r"] \arrow[d] & \mathbb{Z}/p^r \arrow[r] \arrow[d] & 0 \\
(\mu_{p^M})_{I_k} \arrow[r, "\iota_M"] \arrow[d] & E[p^M]_{I_k} \arrow[r, "\pi_M"] \arrow[d] & \mathbb{Z}/p^M \arrow[r] \arrow[d] & 0 \\
0 & 0 & 0 & .
\end{tikzcd}$$

The snake lemma applied to the rightmost part of the diagram gives an exact sequence

$$\operatorname{Ker}(\pi_{r-M}) \xrightarrow{\alpha} \operatorname{Ker}(\pi_r) \xrightarrow{\beta} \operatorname{Ker}(\pi_M) \xrightarrow{\delta} \operatorname{Coker}(\pi_{r-M}) = 0.$$

Since π_{r-M} is surjective, we get an exact sequence

$$\operatorname{Ker}(\pi_{r-M}) \xrightarrow{\alpha} \operatorname{Ker}(\pi_r) \xrightarrow{\beta} \operatorname{Ker}(\pi_M) \longrightarrow 0.$$

The claim will follow if we show that the map $\operatorname{Ker}(\pi_r) \overset{\beta}{\to} \operatorname{Ker}(\pi_M)$ is an isomorphism, or equivalently that $\operatorname{Ker}(\pi_{r-M}) \overset{\alpha}{\to} \operatorname{Ker}(\pi_r)$ is the zero map. But this follows by Lemma 5.1. Namely, the map $(\mu_{p^r})_{I_k} \overset{\beta}{\to} (\mu_{p^M})_{I_k}$ is an isomorphism. □

From Lemma 3.2, $\operatorname{Ker}(\partial_E)_{\text{fin}} \simeq \operatorname{Im}((T_p(\mathscr{E})^\circ)_{G_k} \overset{\iota}{\to} T_p(E)_{G_k})$. Claim 1 and Claim 3 will complete the proof of the theorem in this case. It is clear that if $\overline{E}[p^{\widehat{N}}] \not\subset \overline{E}(\mathbb{F}_k)$, the inequality $N \leq \widehat{N}$ becomes strict. □

Remark 5.4. One can use part (ii) of Theorem 5.3 to construct examples of elliptic curves for which we have $N < \widehat{N} = M^{\mathrm{ur}}$. In particular, the upper bound of Theorem 1.1 can be strictly achieved. For example, consider E an elliptic curve over $\mathbb{Q}_p$ with complex multiplication. Let $k_0 = \mathbb{Q}_p(\mu_p)$ and for $n \geq 1$ consider the tower of finite extensions $k_n = k_0(\widehat{E}[p^n])$. It follows by [19, Theorem 2.1.6] and [35, IV.6, Theorem 6.1] that for every $n \geq 1$ the extension k_{n+1}/k_n is totally ramified of degree p. Thus, there exists some $n \geq 1$ such that $\overline{E}[p^n] \not\subset \overline{E}(\mathbb{F}_{k_n})$. This means that over k_n we have a strict inequality $N < n = \widehat{N}$. Moreover, notice that $\widehat{N} = M^{\mathrm{ur}}$, since k_{n+1}/k_n is totally ramified.

Construction of the maximal covering. We next consider the case when the elliptic curve E is the base change of an elliptic curve over $\mathbb{Q}$ with potential complex multiplication. Let E_0 be an elliptic curve over $\mathbb{Q}$. For a field extension $F/\mathbb{Q}$, we denote by $\operatorname{End}_F(E_0)$ the ring of endomorphisms on E_0 which are defined over F. Assume first, E_0 has potential complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Namely, $\operatorname{End}_{\overline{\mathbb{Q}}}(E_0) \simeq \mathcal{O}_K$. As all endomorphisms on E_0 are defined over K, we also have $\operatorname{End}_{\overline{\mathbb{Q}}}(E_0) = \operatorname{End}_K(E_0) \simeq \mathcal{O}_K$. It follows by [30, Corollary 5.12] that K has class number one. Suppose that the prime number p splits completely in K and E_0 has good reduction at p. We consider the reduction modulo p,

$$r : \operatorname{End}_K(E_0) \longrightarrow \operatorname{End}_{\overline{\mathbb{F}_p}}(\overline{E}_0).$$

It follows by [5] (see also [20, 13.4, Theorem 12], [26, p. 2]) that there exists a prime element η of $\mathcal{O}_K$ such that $p = \eta\overline{\eta}$ and the endomorphism $\eta : E_0 \to E_0$ of E_0 reduces to the Frobenius automorphism $\varphi : \overline{E}_0 \to \overline{E}_0$.

Since p splits completely in K, the completion of K at (η) is $\mathbb{Q}_p$. Denote by $E = E_0 \otimes_{\mathbb{Q}} \mathbb{Q}_p$ the base change of E_0 to $\mathbb{Q}_p$. We conclude that E has complex multiplication defined over $\mathbb{Q}_p$. That is, $\mathrm{End}_{\mathbb{Q}_p}(E) \simeq \mathcal{O}_K$ and $\eta : E \to E$ reduces to the Frobenius. We claim that for every $n \geq 1$, $\mathrm{Ker}(\eta^n) = \widehat{E}[p^n]$. Since the reduction of η^n is an automorphism, we clearly have $\mathrm{Ker}(\eta^n) \subset \widehat{E}$. Moreover, the equality $\eta\overline{\eta} = p$ implies that $\mathrm{Ker}(\eta^n) \subset E[p^n]$ from where the claim follows.

We conclude that if $\mathrm{Ker}(\eta^n) = \widehat{E}[p^n] \subset \widehat{E}(k)$, then the isogeny $\eta^n : E \to E$ defines a geometric covering of degree p^n and is completely ramified over $\overline{E}$. According to Theorem 5.3 (i), $\eta^{\widehat{N}} : E \to E$ is the maximal covering corresponding to $\pi_1^{\mathrm{ab}}(E)^{\mathrm{geo}}_{\mathrm{ram}}$.

Good supersingular reduction. Next, we consider the elliptic curve E which has good supersingular reduction. The boundary map $\partial_E : V(E) \to \overline{E}(\mathbb{F}_k)$ induces a short exact sequence

$$\mathrm{Ker}(\partial_E)/p^n \longrightarrow V(E)/p^n \longrightarrow \overline{E}(\mathbb{F}_k)/p^n \longrightarrow 0.$$

As the reduction $\overline{E}$ of E satisfies $\overline{E}[p^n] = 0$ for any $n \geq 1$, we have $\overline{E}(\mathbb{F}_k)/p^n = 0$ and $\mathrm{Tor}(\overline{E}(\mathbb{F}_k), \mathbb{Z}/p^n) \simeq \overline{E}(\mathbb{F}_k)[p^n] = 0$ so that we obtain

$$\mathrm{Ker}(\partial_E)/p^n \simeq V(E)/p^n. \tag{5.6}$$

In the following, *we assume* $E[p] \subset E(k)$ and will give bounds of $\mathrm{Ker}(\partial_E)_{\mathrm{fin}}$ (Theorem 5.9). By fixing an isomorphism $E[p] \simeq (\mu_p)^{\oplus 2}$ of (trivial) G_k-modules, the Kummer map gives

$$\widehat{E}(k)/p \hookrightarrow H^1(k, \widehat{E}[p]) \simeq H^1(k, \mu_p)^{\oplus 2} \simeq (k^\times/p)^{\oplus 2}.$$

Its image can be understood by a filtration on $k^\times/p$ using the higher unit group $U_k^i = 1 + \mathfrak{m}_k^i$. Precisely, because $\overline{E}[p] = 0$, we have the following decomposition:

$$E(k)/p \simeq \widehat{E}(k)/p \simeq \overline{U}_k^{p(e_0(k)-t_0(k))} \oplus \overline{U}_k^{pt_0(k)}, \tag{5.7}$$

where $\overline{U}_k^i := \mathrm{Im}(U_k^i \to k^\times/p)$, $e_0(k) = e_k/(p-1)$, and

$$t_0(k) = \max\{v_k(y) \mid 0 \neq y \in \widehat{E}[p]\}$$

(cf. [7, Section 3.4]). By identifying the isomorphism (5.7), we can decompose an element w in $E(k)/p$ as $w = (u', u)$ with $u' \in \overline{U}_k^{p(e_0(k)-t_0(k))}$, $u \in \overline{U}_k^{pt_0(k)}$. The Galois symbol map associated to E and $\mathbb{G}_m$ (Definition 2.6) induces

$$s_p : (E/p \otimes \mathbb{G}_m/p)(k) \longrightarrow H^2(k, E[p] \otimes \mu_p) \simeq H^2(k, \mu_p^{\otimes 2})^{\oplus 2} \simeq (\mathbb{Z}/p)^{\oplus 2}.$$

In fact, this map s_p becomes bijective ([12, Theorem 4.2]), and since it factors through the surjection $(E/p \otimes \mathbb{G}_m/p)(k) \twoheadrightarrow K(k; E, \mathbb{G}_m)/p$, it follows that this surjection is an isomorphism as well. The map above is compatible with the Hilbert symbol map $(-,-)_p : k^\times/p \otimes k^\times/p \to \mu_p \simeq \mathbb{Z}/p$ ([32, Section XIV.2, Proposition 5]) as the following commutative diagram indicates:

$$\begin{tikzcd}
E(k)/p \otimes k^\times/p \arrow[r, "\{-,-\}_{k/k}"] \arrow[d, "\simeq"] & (E/p \otimes \mathbb{G}_m/p)(k) \arrow[d, "\simeq"', "s_p"] \\
(\overline{U}_k^{pt_0(k)} \otimes k^\times/p) \oplus (\overline{U}_k^{p(e_0(k)-t_0(k))} \otimes k^\times/p) \arrow[r, "(-,-)_p^{\oplus 2}"] & (\mathbb{Z}/p)^{\oplus 2}.
\end{tikzcd}$$

Here, the top horizontal map is the symbol map $w \otimes x \mapsto \{w, x\}_{k/k}$ (cf. [12, Proof of Proposition 4.6]). The above commutative diagram gives the following lemma.

Lemma 5.5. *Two elements $\{(u_1', 1), x_1\}_{k/k}$ and $\{(1, u_2), x_2\}_{k/k}$ generate $K(k; E, \mathbb{G}_m)/p$ if they satisfy $(u_1', x_1)_p \neq 0$ and $(u_2, x_2)_p \neq 0$.*

The image of $\overline{U}_k^i \otimes \overline{U}_k^j$ by the Hilbert symbol is known as follows:

Lemma 5.6 ([11, Lemma 3.4])**.** *If $p \nmid i$ or $p \nmid j$, then*

$$\#(\overline{U}_k^i, \overline{U}_k^j)_p = \begin{cases} p, & \text{if } i + j \le pe_0(k), \\ 0, & \text{otherwise.} \end{cases}$$

For $m \ge 1$, put $k_m := k(\mu_{p^m})$. Moreover, consider the invariant

$$R = \min\{r \ge 0 \mid e_k \le (p-1)p^r\}.$$

Using the above observations, we determine generators of $K(k_m; E, \mathbb{G}_m)/p$ for some m.

Lemma 5.7. *We assume $E[p] \subset E(k)$ and $M = M^{\mathrm{ur}}$. Then, there exists $M \le m \le M + R$ such that the K-group $K(k_m; E, \mathbb{G}_m)/p$ is generated by elements of the form $\{a, \zeta_{p^m}\}_{k_m/k_m}$, where ζ_{p^m} is a primitive p^m-th root of unity.*

Proof. Recalling from [7, Lemma 3.4], we have $\overline{U}_k^i = 1$ for $i > pe_0(k)$ and $\overline{U}_k^i = \overline{U}_k^{i+1}$ for i with $p \mid i$. For some $i \le pe_0(k)$ which is prime to p or $i = pe_0(k)$, we have $\zeta = \zeta_{p^M} \in \overline{U}_k^i \smallsetminus \overline{U}_k^{i+1}$. From the assumption $M = M^{\mathrm{ur}}$, $k_{M+1} = k(\zeta_{p^{M+1}})/k$ is a totally ramified extension of degree p. In the case $i = pe_0(k)$, the extension k_{M+1}/k is unramified ([19, Lemma 2.1.5]) so we conclude that $i < pe_0(k)$. If we have

$$i \le \min\{pt_0(k), p(e_0(k) - t_0(k))\}, \tag{5.8}$$

then $i + pt_0(k), i + p(e_0(k) - t_0(k)) \le pe_0(k)$. There exist $u' \in \overline{U}_k^{pt_0(k)}$ and $u \in \overline{U}_k^{p(e_0(k)-t_0(k))}$ such that $(u', \zeta)_p \neq 0$ and $(u, \zeta)_p \neq 0$ (Lemma 5.6).

Thus, the elements $\{(u',1),\zeta\}_{k/k}$ and $\{(1,u),\zeta\}_{k/k}$ generate $K(k;E,\mathbb{G}_m)/p$ by Lemma 5.5. The assertion holds for $m=M$ and for $k=k_M$.

Suppose that the above inequality (5.8) does not hold. It follows by Lemma 5.8 below that we have $\zeta_{p^{M+1}} \in \overline{U}^{i}_{k_{M+1}} \smallsetminus \overline{U}^{i+1}_{k_{M+1}}$, while $e_0(k_{M+1}) = pe_0(k)$, and $t_0(k_{M+1}) = pt_0(k)$. Since $i < pe_0(k)$ and we defined R to be the smallest nonnegative integer such that $e_0(k) \le p^R$. We have

$$i < pe_0(k) \le p^{R+1} \le p^R \min\{pt_0(k), p(e_0(k) - t_0(k)\}.$$

It follows that there exists $r \le R$ such that over the extension $k_m = k(\mu_{p^m})/k$, with $m = M+r$, we have

$$i \le \min\{pt_0(k_m), p(e_0(k_m) - t_0(k_m))\} = p^r \min\{pt_0(k), p(e_0(k) - t_0(k))\}.$$

Applying Lemma 5.5 and Lemma 5.6 as above to k_m, there are symbols of the form $\{a,\zeta_{p^m}\}_{k_m/k_m}$ which generate $K(k_m;E,\mathbb{G}_m)/p$ as required. □

Lemma 5.8 (cf. [8, Lemma 3.23] for the case $M \ge 2$)**.** *We assume $\mu_p \subset k$. Let $x \in \overline{U}^{i}_{k} \smallsetminus \overline{U}^{i+1}_{k}$, where $0 < i < pe_0(k)$ and i is coprime to p. Let $K = k(\sqrt[p]{x})$ and write $\xi = \sqrt[p]{x}$. Then, $\xi \in \overline{U}^{i}_{K} \smallsetminus \overline{U}^{i+1}_{K}$.*

Proof. In this proof, we denote by $\bar{x}$ the residue class in $\overline{U}^i_k = U^i_k/U^i_k \cap (k^\times)^p$ represented by the unit $x \in U^i_k$. First, we note that the extension K/k is a totally ramified extension of degree p ([19, Lemma 2.1.5]). Thus, $v_K(x-1) = pv_k(x-1) = pi$. Suppose that $\xi = \sqrt[p]{x}$ is in $U^j_K \smallsetminus U^{j+1}_K$ for some j and write $\xi = 1 + u\pi_K^j$ for a unit $u \in \mathcal{O}_K^\times$, where π_K is a fixed uniformizer of K. From [6, (5.7)], we calculate the valuation of $\xi^p - 1 = x - 1$ as follows:

- If $j > e_0(K) = pe_0(k)$, then $\xi^p \equiv 1 + u'\pi_K^{j+e_K} \bmod \pi_K^{j+e_K+1}$ for some unit $u' \in \mathcal{O}_K^\times$. Thus,

$$pi = v_K(x-1) = v_K(\xi^p - 1) = j + e_K > pe_0(k) + pe_k = p^2 e_0(k).$$

  This gives $i > pe_0(k)$ and contradicts the assumption on i.
- If $j = e_0(K)$, then $\xi^p \equiv 1 + (u^p + u')\pi_K^{pe_0(K)} \bmod \pi_K^{pe_0(K)+1}$ for some unit $u' \in \mathcal{O}_K^\times$ and hence

$$pi = v_K(x-1) = v_K(\xi^p - 1) \ge pe_0(K) = p^2 e_0(k).$$

  Therefore, $i \ge pe_0(k)$, which is again a contradiction.
- If $j < e_0(K)$, then $\xi^p \equiv 1 + u^p\pi_K^{pj} \bmod \pi_K^{pj+1}$. We have

$$pi = v_K(x-1) = v_K(\xi^p - 1) = pj.$$

  This implies $i = j$.

As $\xi \in U^i_K \smallsetminus U^{i+1}_K$, the residue class $\bar{\xi}$ is in $\overline{U}^i_K \smallsetminus \overline{U}^{i+1}_K$. □

Theorem 5.9. *Let E be an elliptic curve over k which has good supersingular reduction. We assume that $E[p] \subset E(k)$. Then, we have surjective homomorphisms*

$$(\mathbb{Z}/p^{M^{\mathrm{ur}}+R})^{\oplus 2} \twoheadrightarrow \mathrm{Ker}(\partial_E)_{\mathrm{fin}} \twoheadrightarrow (\mathbb{Z}/p^N)^{\oplus 2},$$

where $R = \min\{r \mid e_k \le (p-1)p^r\}$.

Proof. As we noted in (5.6), there are isomorphisms

$$\mathrm{Ker}(\partial_E)/p^n \simeq V(E)/p^n \simeq K(k; E, \mathbb{G}_m)/p^n$$

for any $n \ge 1$. Recalling from (2.9), we have $V(E) \simeq K(k; E, \mathbb{G}_m)$. The lower bound is given by

$$\mathrm{Ker}(\partial_E) \twoheadrightarrow \mathrm{Ker}(\partial_E)/p^N \simeq K(k; E, \mathbb{G}_m)/p^N \simeq (\mathbb{Z}/p^N)^{\oplus 2}, \tag{5.9}$$

where the last isomorphism follows from [11, Remark 4.3].

Since the norm map $K(k'; E, \mathbb{G}_m) \to K(k; E, \mathbb{G}_m)$ is surjective for any finite extension k'/k ([41, Proposition 3.1]), we may assume $M = M^{\mathrm{ur}}$. In particular, the Kummer extension $k(\mu_{p^{M+1}})/k$ is a totally ramified p-extension. Take $m \le M + R$ as in Lemma 5.7 and put $k_m = k(\mu_{p^m})$. For each $n \ge m$, we consider the following diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & K(k_m; E, \mathbb{G}_m)/p \arrow[r, "p^n"] \arrow[d, two heads] & K(k_m; E, \mathbb{G}_m)/p^{n+1} \arrow[r] \arrow[d, two heads] & K(k_m; E, \mathbb{G}_m)/p^n \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & K(k; E, \mathbb{G}_m)/p \arrow[r, "p^n"] & K(k; E, \mathbb{G}_m)/p^{n+1} \arrow[r] & K(k; E, \mathbb{G}_m)/p^n \arrow[r] & 0,
\end{tikzcd}$$

where the vertical maps are given by norms which are surjective. The far left vertical map $K(k_m; E, \mathbb{G}_m)/p \to K(k; E, \mathbb{G}_m)/p$ is bijective because of

$$K(k_m; E, \mathbb{G}_m)/p \simeq K(k; E, \mathbb{G}_m)/p \simeq (\mathbb{Z}/p)^{\oplus 2}$$

using the assumption $E[p] \subset E(k)$ as in (5.9). By Lemma 5.7, the map $p^n \colon K(k_m; E, \mathbb{G}_m)/p \to K(k_m; E, \mathbb{G}_m)/p^{n+1}$ defined by the multiplication by p^n is the 0-map and so is $p^n \colon K(k; E, \mathbb{G}_m)/p \to K(k; E, \mathbb{G}_m)/p^{n+1}$. From the above diagram, we have $K(k; E, \mathbb{G}_m)/p^{n+1} \simeq K(k; E, \mathbb{G}_m)/p^n$ for any $n \ge m$. Putting $K = k(E[p^{M+R}])$, there are surjective homomorphisms

$$K(K; E, \mathbb{G}_m)/p^{M+R} \twoheadrightarrow K(K; E, \mathbb{G}_m)/p^m \twoheadrightarrow K(k; E, \mathbb{G}_m)/p^m.$$

Here, the last map is induced from the norm map which is surjective. From this, we have

$$(\mathbb{Z}/p^{M+R})^{\oplus 2} \simeq K(K; E, \mathbb{G}_m)/p^{M+R} \twoheadrightarrow K(k; E, \mathbb{G}_m)/p^n \simeq \mathrm{Ker}(\partial_E)/p^n$$

for any $n \ge 1$. This implies the existence of a surjective homomorphism $(\mathbb{Z}/p^{M+R})^{\oplus 2} \twoheadrightarrow \mathrm{Ker}(\partial_E)_{\mathrm{fin}}$ as required. □

Appendix A. Profinite Group Homology

In this appendix, we show the following proposition which is used in [1, (2.21)] and [36, Section 3]:

Proposition A.1. *Let l be a prime, A a semi-abelian variety over a p-adic field k, and G a closed normal subgroup of G_k. Then, we have*

$$T_l(A)_G \simeq \varprojlim_n [(A[l^n])_G].$$

Put $T := T_l(A)$ and $A_n := A[l^n]$. Using this notation, $T = \varprojlim_n A_n$ can be regarded as a profinite $\mathbb{Z}_l[\![G]\!]$-module. Recall that, for a profinite $\mathbb{Z}_l[\![G]\!]$-module M, the m-th *homology group* $H_m(G,M)$ of G with coefficients in M is given by the m-th left derived functor of $-\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}\mathbb{Z}_l$ (cf. [29, Section 6.3]). The homology group $H_m(G,M)$ can be computed by using the homogeneous bar resolution $L_\bullet \twoheadrightarrow \mathbb{Z}_l$ as follows:

$$H_m(G,M) = H_m(M\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_\bullet)$$

(cf. [29, Theorem 6.3.1]). Each term L_m in $L_\bullet$ is a free profinite $\mathbb{Z}_l[\![G]\!]$-module, so that we have $\varprojlim(A_n\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_\bullet) = T\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_\bullet$ and

$$H_m(G,T) = H_m(T\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_\bullet),\ H_m(G,A_n) = H_m(A_n\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_\bullet).$$

As $A_n\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_m = A_n \otimes_{\mathbb{Z}/l^n[\![G]\!]} L_m/l^n$ is finite, the tower of chain complexes $\cdots \to A_n\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_\bullet \to \cdots \to A_1\widehat{\otimes}_{\mathbb{Z}_l[\![G]\!]}L_\bullet$ satisfies the Mittag-Leffler condition. By [39, Theorem 3.5.8], we have an exact sequence for each m:

$$0 \longrightarrow \varprojlim_n{}^1 H_{m+1}(G,A_n) \longrightarrow H_m(G,T) \longrightarrow \varprojlim_n H_m(G,A_n) \longrightarrow 0.$$

In particular, we have

$$0 \longrightarrow \varprojlim_n{}^1 H_1(G,A_n) \longrightarrow T_G \longrightarrow \varprojlim_n (A_n)_G \longrightarrow 0.$$

Here, $H_1(G,A_n)^\vee \simeq H^1(G,A_n^\vee)$, where $\vee$ denotes the Pontrjagin dual. Since $A_n^\vee$ is finite, the action of G on $A_n^\vee$ factors through a finite quotient G/K_n for some open normal subgroup $K_n \subset G$. By the inflation-restriction sequence ([29, Corollary 7.2.5]), we have a short exact sequence

$$0 \longrightarrow H^1(G/K_n, A_n^\vee) \xrightarrow{\mathrm{inf}} H^1(G,A_n^\vee) \xrightarrow{\mathrm{Res}} H^1(K_n,A_n^\vee).$$

As $H^1(K_n,A_n^\vee) = \mathrm{Hom}_{\mathrm{cont}}(K_n,A_n^\vee)$ and $H^1(G/K_n,A_n^\vee)$ are finite abelian groups, so is $H^1(G,A_n^\vee)$ and hence $H_1(G,A_n)$ is finite. From this, the tower $\cdots \to H_1(G,A_{n+1}) \to H_1(G,A_n) \to \cdots \to H_1(G,A_1)$ satisfies the Mittag-Leffler condition (cf. [39, Exercise 3.5.1]). We have $\varprojlim_n{}^1 H_1(G,A_n) = 0$ by [39, Proposition 3.5.7]. This gives Proposition A.1.

References

[1] S. Bloch, "Algebraic K-theory and classfield theory for arithmetic surfaces", *Ann. Math.* **114** (1981), no. 2, p. 229-265.

[2] S. Bosch, W. Lütkebohmert & M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 21, Springer, 1990.

[3] J. Coates & R. Greenberg, "Kummer theory for abelian varieties over local fields", *Invent. Math.* **124** (1996), no. 1-3, p. 129-174.

[4] P. Deligne & D. Mumford, "The irreducibility of the space of curves of given genus", *Publ. Math., Inst. Hautes Étud. Sci.* (1969), no. 36, p. 75-109.

[5] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper", *Abh. Math. Semin. Hansische Univ.* **14** (1941), p. 197-272.

[6] I. B. Fesenko & S. V. Vostokov, *Local fields and their extensions*, Translations of Mathematical Monographs, vol. 121, American Mathematical Society, 2002, xi+345 pages.

[7] E. Gazaki & T. Hiranouchi, "Divisibility results for zero-cycles", *Eur. J. Math.* **7** (2021), no. 4, p. 1458-1501.

[8] E. Gazaki & I. Leal, "Zero cycles on a product of elliptic curves over a p-adic Field", *Int. Math. Res. Not.* **2022** (2022), no. 14, p. 10586-10625.

[9] A. Grothendieck, *Revêtements étales et groupe fondamental. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1)*, Lecture Notes in Mathematics, vol. 224, Springer, 1971, dirigé par Alexandre Grothendieck, augmenté de deux exposés de M. Raynaud, xviii+325 pages.

[10] M. Hindry & J. H. Silverman, *Diophantine geometry: An introduction*, Graduate Texts in Mathematics, vol. 201, Springer, 2000, xiii+558 pages.

[11] T. Hiranouchi, "Milnor K-groups attached to elliptic curves over a p-adic field", *Funct. Approximatio, Comment. Math.* **54** (2016), no. 1, p. 39-55.

[12] ———, "Galois symbol maps for abelian varieties over a p-adic field", *Acta Arith.* **197** (2021), no. 2, p. 137-157.

[13] H. Imai, "On the rational points of some Jacobian varieties over large algebraic number fields", *Kodai Math. J.* **3** (1980), no. 1, p. 56-58.

[14] B. Kahn, "The decomposable part of motivic cohomology and bijectivity of the norm residue homomorphism", in *Algebraic K-theory, commutative algebra, and algebraic geometry (Santa Margherita Ligure, 1989)*, Contemporary Mathematics, vol. 126, American Mathematical Society, 1989, p. 79-87.

[15] ———, "Nullité de certains groupes attachés aux variétés semi-abéliennes sur un corps fini; application", *C. R. Acad. Sci. Paris* **314** (1992), no. 13, p. 1039-1042.

[16] K. Kato & S. Saito, "Unramified class field theory of arithmetical surfaces", *Ann. Math.* **118** (1983), no. 2, p. 241-275.

[17] N. M. Katz & S. Lang, "Finiteness theorems in geometric classfield theory", *Enseign. Math.* **27** (1981), no. 3-4, p. 285-319, with an appendix by Kenneth A. Ribet.

[18] N. M. Katz & B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, 1985, xiv+514 pages.

[19] M. Kawachi, "Isogenies of degree p of elliptic curves over local fields and Kummer theory", *Tokyo J. Math.* **25** (2002), no. 2, p. 247-259.

[20] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics, vol. 112, Springer, 1987, with an appendix by J. Tate.

[21] A. Mattuck, "Abelian varieties over p-adic ground fields", *Ann. Math.* **62** (1955), p. 92-119.

[22] B. Mazur, "Rational points of abelian varieties with values in towers of number fields", *Invent. Math.* **18** (1972), p. 183-266.

[23] J. S. Milne, "Jacobian varieties", in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, 1986, p. 167-212.

[24] B. Moonen, B. Edixhoven & G. van der Geer, "Abelian varieties", `https://www.math.ru.nl/~bmoonen/research.html#bookabvar`.

[25] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2008, xv+825 pages.

[26] A. R. RAJWADE, “Arithmetic on curves with complex multiplication by the ring of Eisenstein series”, *Proc. Camb. Philos. Soc.* **65** (1969), p. 59-73.

[27] W. RASKIND, “Abelian class field theory of arithmetic schemes”, in *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*, Proceedings of Symposia in Pure Mathematics, vol. 58, American Mathematical Society, 1992, p. 85-187.

[28] W. RASKIND & M. SPIESS, “Milnor K-groups and zero-cycles on products of curves over p-adic fields”, *Compos. Math.* **121** (2000), no. 1, p. 1-33.

[29] L. RIBES & P. ZALESSKII, *Profinite groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 40, Springer, 2010.

[30] K. RUBIN, “Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer”, in *Arithmetic theory of elliptic curves (Cetraro 1997)*, Lecture Notes in Mathematics, vol. 1716, Springer, 1997, p. 167-234.

[31] S. SAITO, “Class field theory for curves over local fields”, *J. Number Theory* **21** (1985), no. 1, p. 44-80.

[32] J.-P. SERRE, *Corps locaux*, Publications de l’Institut de Mathématique de l’Université de Nancago, vol. 8, Hermann, 1968, 248 pages.

[33] ———, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer, 1988, translated from the French, ix+207 pages.

[34] ———, *Abelian l-adic representations and elliptic curves*, Advanced Book Classics, Addison-Wesley Publishing Group, 1989.

[35] J. H. SILVERMAN, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009, xx+513 pages.

[36] M. SOMEKAWA, “On Milnor K-groups attached to semi-abelian varieties”, *K-Theory* **4** (1990), no. 2, p. 105-119.

[37] J. T. TATE, “p-divisible groups”, in *Proc. Conf. Local Fields (Driebergen, 1966)*, Springer, 1967, p. 158-183.

[38] ———, “Relations between K_2 and Galois cohomology”, *Invent. Math.* **36** (1976), p. 257-274.

[39] C. A. WEIBEL, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, 1994, xiv+450 pages.

[40] T. YAMAZAKI, “On Chow and Brauer groups of a product of Mumford curves”, *Math. Ann.* **333** (2005), no. 3, p. 549-567.

[41] ———, “Class field theory for a product of curves over a local field”, *Math. Z.* **261** (2009), no. 1, p. 109-121.

[42] T. YOSHIDA, “Abelian étale coverings of curves over local fields and its application to modular curves”, master thesis, 2002.

[43] ———, “Finiteness theorems in the class field theory of varieties over local fields”, *J. Number Theory* **101** (2003), no. 1, p. 138-150.

Evangelia GAZAKI
Department of Mathematics, University of Virginia
221 Kerchof Hall, 141 Cabell Dr., Charlottesville, VA, 22904, USA
E-mail: eg4va@virginia.edu

Toshiro HIRANOUCHI
Department of Basic Sciences, Graduate School of Engineering, Kyushu Institute of Technology
1-1 Sensui-cho, Tobata-ku, Kitakyushu-shi, Fukuoka 804-8550, Japan
E-mail: hira@mns.kyutech.ac.jp