Algebra & Number Theory

Volume 5
2011
No. 2

msp

Algebra & Number Theory

www.jant.org

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2011 is US $150/year for the electronic version, and $210/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

ALGEBRA AND NUMBER THEORY 5:2(2011)

msp

On the Hom-form of Grothendieck's birational anabelian conjecture in positive characteristic

Mohamed Saïdi and Akio Tamagawa

We prove that a certain class of open homomorphisms between Galois groups of function fields of curves over finite fields arises from embeddings between the function fields.

Introduction

Let K be an infinite field that is finitely generated over its prime field. Let $\overline{K}$ be an algebraic closure of K. We denote by K^{sep} the separable closure, and by K^{perf} the perfection, of K in $\overline{K}$. Let $G_K \stackrel{\mathrm{def}}{=} \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group of K. (Observe that $G_K = G_{K^{\mathrm{perf}}}$.) The ultimate aim of Grothendieck's birational anabelian conjectures is to reconstruct the field structure of K from the topological group structure of G_K. More precisely, these conjectures can be formulated as follows.

Saïdi was holding an EPSRC advanced research fellowship GR/R75861/02 during the preparation of this paper, and would very much like to thank EPSRC for its support.

MSC2010: primary 14G15; secondary 14H25, 14H30, 11G20.

Keywords: Grothendieck's birational anabelian conjecture, homomorphisms between Galois groups.

Birational anabelian conjectures. There exists a group-theoretic recipe for recovering finitely generated infinite fields (or their perfections) from their absolute Galois groups G_K. In particular, if for such fields K and L one has $G_K \xrightarrow{\sim} G_L$, then $L^{\mathrm{perf}} \xrightarrow{\sim} K^{\mathrm{perf}}$. Moreover, given two such fields K and L, one has the following.

Isom-form. Every isomorphism $\sigma : G_K \xrightarrow{\sim} G_L$ is defined by a field isomorphism $\overline{\gamma} : \overline{L} \xrightarrow{\sim} \overline{K}$. This isomorphism is unique if the characteristic is 0, and unique up to Frobenius twists if the characteristic is positive. In particular, $\overline{\gamma}$ induces an isomorphism $L^{\mathrm{perf}} \xrightarrow{\sim} K^{\mathrm{perf}}$.

Hom-form. Every open homomorphism $\sigma : G_K \to G_L$ is defined by a field embedding $\overline{\gamma} : \overline{L} \hookrightarrow \overline{K}$. This embedding is unique if the characteristic is 0, and unique up to Frobenius twists if the characteristic is positive. In particular, $\overline{\gamma}$ induces a field embedding $L^{\mathrm{perf}} \hookrightarrow K^{\mathrm{perf}}$.

Thus, the Hom-form is stronger than the Isom-form. The first results concerning these conjectures were obtained by Neukirch and Uchida in the case of global fields.

Theorem (Neukirch, Uchida). *Let K and L be global fields. Then the natural map*

$$\mathrm{Isom}(L, K) \to \mathrm{Isom}(G_K, G_L)/\mathrm{Inn}(G_L)$$

is a bijection.

More precisely, this is due to Neukirch [1969a; 1969b] and Uchida [1976] for number fields, and due to Uchida [1977] for function fields of curves over finite fields. Later, Pop generalized their results to the case of finitely generated fields of higher transcendence degree ([Pop 1994; 2002]; see also [Szamuely 2004] for a survey on Pop's results).

In characteristic 0, Mochizuki proved the following relative version of the Hom-form of the birational conjectures.

Theorem [Mochizuki 1999]. *Let K and L be two finitely generated, regular extensions of a field k. Assume that k is a sub-p-adic field (that is, k can be embedded in a finitely generated extension of $\mathbb{Q}_p$) for some prime number p. Then the natural map*

$$\mathrm{Hom}_k(L, K) \to \mathrm{Hom}^{\mathrm{open}}_{G_k}(G_K, G_L)/\mathrm{Inn}(\mathrm{Ker}(G_L \to G_k))$$

is a bijection. Here, Hom_k denotes the set of k-embeddings, and $\mathrm{Hom}^{\mathrm{open}}_{G_k}$ denotes the set of open G_k-homomorphisms.

However, almost nothing is known about the absolute version (that is, not relative with respect to a fixed base field k) of the Hom-form, except for Uchida's result [1981] for $K = \mathbb{Q}$ and $[L : \mathbb{Q}] < \infty$.

A major obstacle in proving the Hom-form of the birational anabelian conjectures is that one of the main common ingredients in the proofs of Neukirch, Uchida,

and Pop, which is the so-called local theory (or Galois characterization of the decomposition subgroups), and which is used in order to establish a one-to-one correspondence between divisorial valuations, is not available in the case of open homomorphisms between Galois groups. More precisely, the main result of local theory available so far, Proposition 1.5, gives very little information on the image of the decomposition subgroups in this case, though one can still prove some partial results (Proposition 2.2, Lemmas 2.6 and 2.9). It seems quite difficult, for the moment, to establish a satisfactory local theory that is suitable to the Hom-form of the above conjecture. Also, the methods used in the proof of Mochizuki's theorem above are quite different, and do not rely on local theory. Instead, Mochizuki proves his result as an application of his fundamental anabelian result that relative open homomorphisms between arithmetic fundamental groups of curves over sub-p-adic fields arise from morphisms between corresponding curves, the proof of which relies on p-adic Hodge theory. It is not clear how to adapt Mochizuki's method to the case of positive characteristics.

In this paper we investigate the Hom-form of the birational anabelian conjectures for function fields of curves over finite fields. For $i = 1, 2$, let k_i be a finite field. Let X_i be a proper, smooth, geometrically connected algebraic curve over k_i. Let K_i be the function field of X_i and fix an algebraic closure $\overline{K}_i$ of K_i. Let K_i^{sep} and K_i^{perf} be the separable closure and the perfection of K_i in $\overline{K}_i$, and $\bar{k}_i$ the algebraic closure of k_i in $\overline{K}_i$. Write $G_i \stackrel{\mathrm{def}}{=} G_{K_i} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(K_i^{\mathrm{sep}}/K_i)$ for the absolute Galois group of K_i, and $G_{k_i} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\bar{k}_i/k_i)$ for the absolute Galois group of k_i. We have the natural exact sequence of profinite groups

$$1 \to \overline{G}_i \to G_i \stackrel{\mathrm{pr}_i}{\to} G_{k_i} \to 1,$$

where $\overline{G}_i$ is the absolute Galois group $\mathrm{Gal}(K_i^{\mathrm{sep}}/K_i\bar{k}_i)$ of $K_i\bar{k}_i$, and pr_i is the canonical projection.

Further, let p_i be the characteristic of k_i, and let $\overline{G}_i^{p_i'}$ be the maximal prime-to-p_i quotient of $\overline{G}_i$. The push-forward of this sequence with respect to the natural surjection $\overline{G}_i \to \overline{G}_i^{p_i'}$ gives rise to the natural exact sequence

$$1 \to \overline{G}_i^{p_i'} \to G_i^{(p_i')} \stackrel{\mathrm{pr}_i}{\to} G_{k_i} \to 1.$$

Set $\mathfrak{G}_i \stackrel{\mathrm{def}}{=} G_i$, $i = 1, 2$ (which we call the *profinite* case) or $\mathfrak{G}_i \stackrel{\mathrm{def}}{=} G_i^{(p_i')}$, $i = 1, 2$ (the *prime-to-characteristic* case). We investigate two classes of continuous, open homomorphisms — rigid and proper homomorphisms — between $\mathfrak{G}_1$ and $\mathfrak{G}_2$.

First, we investigate a class of continuous, open homomorphisms $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$, which we call rigid. More precisely, we say that σ is strictly rigid if the image of each decomposition subgroup of $\mathfrak{G}_1$ coincides with a decomposition subgroup of $\mathfrak{G}_2$, and we say that σ is rigid if there exist open subgroups $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$, such

that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$ and that $\mathfrak{H}_1 \overset{\sigma}{\to} \mathfrak{H}_2$ is strictly rigid. Thus, isomorphisms between $\mathfrak{G}_1$ and $\mathfrak{G}_2$ are (strictly) rigid by the main result of local theory for the Isom-form. Let $\mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{rig}}$ be the set of rigid homomorphisms between $\mathfrak{G}_1$ and $\mathfrak{G}_2$.

We say that a homomorphism $\gamma : K_2 \to K_1$ of fields (which defines an extension K_1/K_2 of fields) is admissible if the extension K_1/K_2 appears in the extensions of K_2 corresponding to the open subgroups of $\mathfrak{G}_2$. An equivalent condition in the profinite case is that the extension K_1/K_2 is finite separable; and in the prime-to-characteristic case, that the extension K_1/K_2 is finite separable and the Galois closure of the extension $K_1\bar{k}_1/K_2\bar{k}_2$ is of degree prime to $p \overset{\mathrm{def}}{=} p_1 = p_2$. We define $\mathrm{Hom}(K_2, K_1)^{\mathrm{adm}} \subset \mathrm{Hom}(K_2, K_1)$ to be the set of admissible homomorphisms $K_2 \to K_1$.

Now, our first main result is the following (see Theorem 3.4).

Theorem A. *The natural map* $\mathrm{Hom}(K_2, K_1) \to \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)/\mathrm{Inn}(\mathfrak{G}_2)$ *induces a bijection*

$$\mathrm{Hom}(K_2, K_1)^{\mathrm{adm}} \overset{\sim}{\to} \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{rig}}/\mathrm{Inn}(\mathfrak{G}_2).$$

Our method of proving Theorem A is as follows. First, we prove, using a certain weight argument based on the Weil conjecture for curves, that a strictly rigid homomorphism $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ induces a bijection $\Sigma_{X_1} \overset{\sim}{\to} \Sigma_{X_2}$ between the set of closed points of X_1 and X_2 (see Lemma 3.8). With this we can reduce the Hom-form in this case to the Isom-form, which has been established in [Uchida 1977] (profinite case) and [Saïdi and Tamagawa 2009] (prime-to-characteristic case).

Next we consider a class of continuous, open homomorphisms $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$, which we call proper. These are homomorphisms with the property that the image of each decomposition subgroup of $\mathfrak{G}_1$ coincides with an open subgroup of a decomposition subgroup of $\mathfrak{G}_2$, such that each decomposition subgroup of $\mathfrak{G}_2$ contains images of only finitely many conjugacy classes of decomposition subgroups of $\mathfrak{G}_1$. We also consider a certain rigidity condition, which we call *inertia-rigidity*, on the various identifications between the modules of the roots of unity (Definition 4.5). Unfortunately, we are not able to prove that this condition automatically holds for proper homomorphisms. Let $\mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{pr,inrig}}$ be the set of proper and inertia-rigid homomorphisms between $\mathfrak{G}_1$ and $\mathfrak{G}_2$. Our second main result is the following (see Theorem 4.8).

Theorem B. *The natural map* $\mathrm{Hom}(K_2, K_1) \to \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)/\mathrm{Inn}(\mathfrak{G}_2)$ *induces a bijection*

$$\mathrm{Hom}(K_2, K_1)^{\mathrm{sep}} \overset{\sim}{\to} \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{pr,inrig}}/\mathrm{Inn}(\mathfrak{G}_2).$$

Here, we define $\mathrm{Hom}(K_2, K_1)^{\mathrm{sep}} \subset \mathrm{Hom}(K_2, K_1)$ *to be the set of separable homomorphisms* $K_2 \to K_1$.

To prove Theorem B, we first show, using a weight argument, that a homomorphism $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ as above induces a surjective map $\Sigma_{X_1} \to \Sigma_{X_2}$ between the sets

of closed points of X_1 and X_2, which has finite fibers (Lemma 2.9). Second, using Kummer theory, we reconstruct functorially an embedding $K_2^\times \hookrightarrow (K_1^{\mathrm{perf}})^\times$ between multiplicative groups (Lemma 4.13). Finally, we show that this embedding $K_2^\times \hookrightarrow (K_1^{\mathrm{perf}})^\times$ is additive.

Recovering the additive structure is one of the main steps in the proof. This problem was treated by Uchida in the case of a bijective identification $K_2^\times \xrightarrow{\sim} K_1^\times$ between multiplicative groups, which is order-preserving and value-preserving. In fact, one needs only to restore the additivity between constants. For this one has to show identities of the form $\gamma(f_2 + 1) = \gamma(f_2) + 1$ for some specific nonconstant function $f_2 \in K_2$. Uchida succeeded in his case by choosing f_2 to be a function with a minimal pole divisor (he called such a function a minimal element.) His argument fails in the case of an embedding between multiplicative groups that is not surjective, because the image of a minimal element is not necessarily minimal in this case. Roughly speaking, we extend his arguments by using, instead, a function that has a unique pole. This one-pole argument turns out to be very efficient, and leads to the recovery of the additive structure under quite general assumptions (Proposition 5.3).

Although rigid homomorphisms are a special case of proper homomorphisms, we choose to treat them separately for several reasons. First, the important condition of inertia-rigidity is automatically satisfied in the case of rigid homomorphisms (Remark 4.9(i)). Second, in the case of (strictly) rigid homomorphisms we can reduce directly to the Isom-form, the proof of which can be based on class field theory. This is not possible for proper homomorphisms, in general. In fact, in the case of proper homomorphisms, class field theory reconstructs only the norm map between the multiplicative groups of function fields.

This paper is organized as follows. In Section 1, we review well-known facts concerning Galois theory of function fields of curves over finite fields, including the main results of local theory. In Section 2, we investigate some basic properties of homomorphisms between absolute Galois groups of function fields of curves over finite fields, as well as homomorphisms between decomposition subgroups. In Section 3, we investigate rigid homomorphisms between (geometrically prime-to-characteristic quotients of) absolute Galois groups, and prove Theorem A. In Section 4, we investigate proper homomorphisms between (geometrically prime-to-characteristic quotients of) absolute Galois groups, and prove Theorem B. In Section 5, we investigate the problem of recovering the additive structure of function fields. Using the above one-pole argument, we prove Proposition 5.3, which is used in the proof of Theorem B in Section 4.

We hope very much that this paper is a first step towards proving the Hom-form of Grothendieck's anabelian conjecture concerning arithmetic fundamental groups

of hyperbolic curves over finite fields, whose Isom-form was proven by Tamagawa [1997] for affine curves and Mochizuki [2007] for proper curves.

1. Generalities on Galois groups of function fields of curves

1A. ***Notations on profinite groups and fields.*** Let $\mathscr{C}$ be a full class of finite groups ($\mathscr{C}$ is closed under taking subgroups, quotients, finite products, and extensions). For a profinite group H, denote by $H^{\mathscr{C}}$ the maximal pro-$\mathscr{C}$ quotient of H, and set $H^{(\mathscr{C})} \stackrel{\text{def}}{=} H/\operatorname{Ker}(\overline{H} \twoheadrightarrow \overline{H}^{\mathscr{C}})$, where $\overline{H}$ is a closed normal subgroup of H. Note that $H^{(\mathscr{C})}$ coincides with $H^{\mathscr{C}}$ if and only if the quotient $A \stackrel{\text{def}}{=} H/\overline{H}$ is a pro-$\mathscr{C}$ group. By definition, we have the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{H} & \longrightarrow & H & \longrightarrow & A & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & \overline{H}^{\mathscr{C}} & \longrightarrow & H^{(\mathscr{C})} & \longrightarrow & A & \longrightarrow & 1, \end{array}$$

where the rows are exact and the columns are surjective.

If l is a prime number, we write H^l and $H^{(l)}$ instead of $H^{\mathscr{C}}$ and $H^{(\mathscr{C})}$ when $\mathscr{C}$ is the class of finite l-groups, and we write $H^{l'}$ and $H^{(l')}$ when $\mathscr{C}$ is the class of finite l'-groups (finite groups of order prime to l).

For a profinite group H, we write H^{ab} for the maximal abelian quotient of H; $\mathrm{Sub}(H)$ for the set of closed subgroups of H; $\mathrm{Aut}(H)$ for the group of (continuous) automorphisms of H; and $\mathrm{Inn}(H)$ for the group of inner automorphisms of H.

For a profinite group H and a prime number l, denote by $\mathrm{cd}(H)$ and $\mathrm{cd}_l(H)$ the cohomological and l-cohomological dimensions of H. It is well-known that if $\mathrm{cd}(H) < \infty$, then H is torsion-free.

Let κ be a field and κ^{sep} a separable closure of κ. Denote the absolute Galois group $\mathrm{Gal}(\kappa^{\mathrm{sep}}/\kappa)$ by G_κ. We write

$$M_{\kappa^{\mathrm{sep}}} \stackrel{\text{def}}{=} \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, (\kappa^{\mathrm{sep}})^\times).$$

Thus, $M_{\kappa^{\mathrm{sep}}}$ is a free $\hat{\mathbb{Z}}^\dagger$-module of rank one, where $\hat{\mathbb{Z}}^\dagger$ is defined as $\hat{\mathbb{Z}}$ if $\mathrm{char}\,\kappa = 0$ and as $\hat{\mathbb{Z}}^{p'}$ if $\mathrm{char}\,\kappa = p > 0$. Further, $M_{\kappa^{\mathrm{sep}}}$ has a natural structure of G_κ-module, which is isomorphic to the Tate twist $\hat{\mathbb{Z}}^\dagger(1)$; that is, G_κ acts on $M_{\kappa^{\mathrm{sep}}}$ via the cyclotomic character $\chi_\kappa : G_\kappa \to (\hat{\mathbb{Z}}^\dagger)^\times$.

1B. ***Galois groups of local fields of positive characteristic.*** Let p be a prime number. Let L be a local field of characteristic p, that is, a complete discrete valuation field of equal characteristic p, with finite residue field ℓ. We denote the ring of integers of L by $\mathbb{O}_L$. Also, fix a separable closure L^{sep} of L. We shall denote the residue field of L^{sep} by $\bar{\ell}$, since it is an algebraic closure of ℓ. Note that ℓ and $\bar{\ell}$ can also be regarded naturally as subfields of L and L^{sep}, respectively. Write

$D \overset{\text{def}}{=} \mathrm{Gal}(L^{\mathrm{sep}}/L)$ for the corresponding absolute Galois group of L, and define the inertia group of L by

$$I \overset{\text{def}}{=} \{\gamma \in D \mid \gamma \text{ acts trivially on } \bar{\ell}\}.$$

We have a canonical exact sequence

$$1 \to I \to D \to G_\ell \overset{\text{def}}{=} \mathrm{Gal}(\bar{\ell}/\ell) \to 1,$$

and, for a full class $\mathscr{C}$ of finite groups, we get a canonical exact sequence

$$1 \to I^{\mathscr{C}} \to D^{(\mathscr{C})} \to G_\ell \to 1.$$

The inertia subgroup I possesses a unique p-Sylow subgroup I^{w}. The quotient $I^{\mathrm{t}} \overset{\text{def}}{=} I/I^{\mathrm{w}}$ is isomorphic to $\hat{\mathbb{Z}}^{p'}$, and is naturally identified with the Galois group $\mathrm{Gal}(L^{\mathrm{t}}/L^{\mathrm{ur}})$, where L^{t} and L^{ur} are the maximal tamely ramified and maximal unramified extensions of L contained in L^{sep}. We have a natural exact sequence

$$1 \to I^{\mathrm{t}} \to D^{\mathrm{t}} \to G_\ell \to 1,$$

where $D^{\mathrm{t}} \overset{\text{def}}{=} \mathrm{Gal}(L^{\mathrm{t}}/L)$. (Observe that $I^{\mathrm{t}} = I^{p'}$ and $D^{\mathrm{t}} = D^{(p')}$.) In particular, I^{t} has a natural structure of G_ℓ-module. Further, there exists a natural identification $I^{\mathrm{t}} \overset{\sim}{\to} M_{\bar{\ell}}$ of G_ℓ-modules. These follow from well-known facts in ramification theory. See [Serre 1968, chapitre IV] for more details.

Let l be a prime number. Denote by D_l an l-Sylow subgroup of D. Then the intersection $I_l \overset{\text{def}}{=} I \cap D_l$ is an l-Sylow subgroup of I. Thus, $I_p = I^{\mathrm{w}}$ and, for $l \neq p$, I_l is isomorphic to $\mathbb{Z}_l$. The image $G_{\ell,l}$ of D_l in G_ℓ is the unique l-Sylow subgroup of $G_\ell \simeq \hat{\mathbb{Z}}$, and hence $G_{\ell,l} \simeq \mathbb{Z}_l$. We have a canonical exact sequence

$$1 \to I_l \to D_l \to G_{\ell,l} \to 1.$$

In particular, I_l has a natural structure of $G_{\ell,l}$-module, and, if $l \neq p$, there exists a natural identification $I_l \overset{\sim}{\to} M_{\bar{\ell},l}$ of $G_{\ell,l}$-modules, where $M_{\bar{\ell},l}$ stands for the l-Sylow subgroup of the profinite abelian group $M_{\bar{\ell}}$.

It is well-known that $\mathrm{cd}_l(D) = \mathrm{cd}(D_l) = 2$ for any prime number $l \neq p$, and that $\mathrm{cd}_p(D) = \mathrm{cd}(D_p) = 1$. Thus, $\mathrm{cd}(D) = 2 < \infty$. In particular, D is torsion-free.

Proposition 1.1. *Let $\mathfrak{D}$ be a quotient of D, let $\mathfrak{I}$ be the image of I in $\mathfrak{D}$, and let $\mathfrak{G}_\ell \overset{def}{=} \mathfrak{D}/\mathfrak{I}$. For each prime number l, let $\mathfrak{D}_l$, $\mathfrak{I}_l$ and $\mathfrak{G}_{\ell,l}$ be the images of D_l, I_l and $G_{\ell,l}$ in $\mathfrak{D}$, $\mathfrak{I}$ and $\mathfrak{G}_\ell$, respectively, which are each l-Sylow subgroups of $\mathfrak{D}$, $\mathfrak{I}$ and $\mathfrak{G}_\ell$, respectively. Let l be a prime number $\neq p$.*

(i) *One of the following cases occurs.*

Case 0: $\mathrm{cd}_l(\mathfrak{D}) = 0$, $\mathfrak{D}_l = \{1\}$, $\mathfrak{I}_l = \{1\}$, *and* $\mathfrak{G}_{\ell,l} = \{1\}$.
Case 1: $\mathrm{cd}_l(\mathfrak{D}) = 1$, $\mathfrak{D}_l \simeq G_\ell$, $\mathfrak{I}_l = \{1\}$, *and* $\mathfrak{G}_{\ell,l} \simeq G_\ell$.
Case 2: $\mathrm{cd}_l(\mathfrak{D}) = 2$, $\mathfrak{D}_l \simeq D_l$, $\mathfrak{I}_l \simeq I_l$, *and* $\mathfrak{G}_{\ell,l} \simeq G_\ell$.

Case ∞: $\mathrm{cd}_l(\mathfrak{D}) = \infty$, *and* $\mathfrak{I}_l$ *is a finite group.*

(ii) *Assume that Case* 2 *occurs. Let* $\mathfrak{D}'$ *be an open subgroup of* $\mathfrak{D}$, L' *the* (*finite*, *separable*) *extension of* L *corresponding to* $\mathfrak{D}' \subset \mathfrak{D}$, *and* D' *the inverse image of* $\mathfrak{D}'$ *in* D. (*Thus*, $D' = G_{L'}$.) *Then*, *for each finite* l*-primary* $\mathfrak{D}'$*-module* M *and each* $k \geq 0$, *one has* $H^k(\mathfrak{D}', M) \xrightarrow{\sim} H^k(D', M)$.

Proof. (i) Since $\mathfrak{I}_l$ is a quotient of $I_l \simeq \mathbb{Z}_l$, one of the following occurs: (a) $\mathfrak{I}_l = \{1\}$, (b) $\mathfrak{I}_l \simeq \mathbb{Z}/l^m\mathbb{Z}$ for an integer $m > 0$, and (c) $\mathfrak{I}_l \simeq \mathbb{Z}_l$. If (a), $\mathfrak{D}_l$ is a quotient of $D_l/I_l = G_\ell \simeq \mathbb{Z}_l$. Thus, it is easy to see that one of Cases 0, 1, or ∞ occurs. If (b), Case ∞ occurs. If (c), we have $\mathfrak{G}_{\ell,l} \simeq G_{\ell,l}$. This follows from the fact that I_l is isomorphic to $M_{\bar{\ell},l}$ on which $G_{\ell,l}$ acts via the l-adic cyclotomic character, and that the l-adic cyclotomic charter $\chi_l : G_{\ell,l} \to \mathbb{Z}_l^\times$ is injective. Thus, it is easy to see that Case 2 occurs.

(ii) Replacing L by L', we may assume that $L' = L$. (Observe that Case 2 occurs also for the quotient $G_{L'} = D' \twoheadrightarrow \mathfrak{D}'$.)

Denote by N the kernel of the surjection $D \twoheadrightarrow \mathfrak{D}$. By the assumption that Case 2 occurs, D_l is injectively mapped into $\mathfrak{D}$, and hence $D_l \cap N$, which is an l-Sylow subgroup of N, is trivial. Since N is of order prime to l, we have $H^k(D, M) = H^k(\mathfrak{D}, H^0(N, M)) = H^k(\mathfrak{D}, M)$, as desired. □

1C. ***Galois groups of function fields of curves.*** Let k be a finite field of characteristic $p > 0$. Let X be a proper, smooth, geometrically connected curve over k. Let $K = K_X$ be the function field of X and fix an algebraic closure $\overline{K}$ of K. Write K^{sep} and $\bar{k} = k^{\mathrm{sep}}$ for the separable closures of K and k in $\overline{K}$. Write $G = G_K \overset{\mathrm{def}}{=} \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $G_k \overset{\mathrm{def}}{=} \mathrm{Gal}(\bar{k}/k)$ for the absolute Galois groups of K and k, respectively. We have the exact sequence of profinite groups

$$1 \to \overline{G} \to G \xrightarrow{\mathrm{pr}} G_k \to 1, \tag{1.1}$$

where $\overline{G}$ is the absolute Galois group $G_{K\bar{k}} = \mathrm{Gal}(K^{\mathrm{sep}}/K\bar{k})$ of $K\bar{k}$, and pr is the canonical projection. Here, it is well-known that the right term G_k is a profinite free group of rank 1 that is (topologically) generated by the Frobenius element, while the left term $\overline{G}$ is a profinite free group of countably infinite rank [Pop 1995; Harbater 1995]. However, the structure of the extension (1.1) itself is not understood well. From (1.1) above, we also obtain the exact sequence

$$1 \to \overline{G}^{\mathscr{C}} \to G^{(\mathscr{C})} \xrightarrow{\mathrm{pr}} G_k \to 1$$

for each full class $\mathscr{C}$ of finite groups.

In the rest of this section, let N be a closed normal subgroup of G and set $\mathfrak{G} \overset{\mathrm{def}}{=} G/N$. Let $\tilde{K}$ denote the Galois extension of K corresponding to N, that is, $\tilde{K} \overset{\mathrm{def}}{=} (K^{\mathrm{sep}})^N$. Let $\overline{\mathfrak{G}}$ be the image of $\overline{G}$ in $\mathfrak{G}$, and set $\mathfrak{G}_k \overset{\mathrm{def}}{=} \mathfrak{G}/\overline{\mathfrak{G}}$, which is a quotient of G_k.

For a scheme T, denote by Σ_T the set of closed points of T. Write $\tilde{\tilde{X}}$ for the integral closure of X in K^{sep}. The absolute Galois group G acts naturally on the set $\Sigma_{\tilde{\tilde{X}}}$, and the quotient $\Sigma_{\tilde{\tilde{X}}}/G$ is naturally identified with Σ_X. For a point $\tilde{\tilde{x}} \in \Sigma_{\tilde{\tilde{X}}}$, with residue field $k(\tilde{\tilde{x}})$ (which is naturally identified with $\bar{k}$), we define its decomposition group $D_{\tilde{\tilde{x}}}$ and inertia group $I_{\tilde{\tilde{x}}}$ by

$$D_{\tilde{\tilde{x}}} \stackrel{\mathrm{def}}{=} \{\gamma \in G \mid \gamma(\tilde{\tilde{x}}) = \tilde{\tilde{x}}\}$$

and

$$I_{\tilde{\tilde{x}}} \stackrel{\mathrm{def}}{=} \{\gamma \in D_{\tilde{\tilde{x}}} \mid \gamma \text{ acts trivially on } k(\tilde{\tilde{x}})\},$$

respectively. We have a canonical exact sequence

$$1 \to I_{\tilde{\tilde{x}}} \to D_{\tilde{\tilde{x}}} \to G_{k(x)} \to 1,$$

where x stands for the image of $\tilde{\tilde{x}}$ in Σ_X.

More generally, write $\tilde{X}$ for the integral closure of X in $\tilde{K}$. The Galois group $\mathfrak{G}$ acts naturally on the set $\Sigma_{\tilde{X}}$, and the quotient $\Sigma_{\tilde{X}}/\mathfrak{G}$ is naturally identified with Σ_X. For a point $\tilde{x} \in \Sigma_{\tilde{X}}$, with residue field $k(\tilde{x})$ (which is naturally identified with a subfield of $\bar{k}$), we define its decomposition group $\mathfrak{D}_{\tilde{x}}$ and inertia group $\mathfrak{I}_{\tilde{x}}$ by

$$\mathfrak{D}_{\tilde{x}} \stackrel{\mathrm{def}}{=} \{\gamma \in \mathfrak{G} \mid \gamma(\tilde{x}) = \tilde{x}\}$$

and

$$\mathfrak{I}_{\tilde{x}} \stackrel{\mathrm{def}}{=} \{\gamma \in \mathfrak{D}_{\tilde{x}} \mid \gamma \text{ acts trivially on } k(\tilde{x})\},$$

respectively. (For any $g \in \mathfrak{G}$, one has $\mathfrak{D}_{g\tilde{x}} = g\mathfrak{D}_{\tilde{x}}g^{-1}$ and $\mathfrak{I}_{g\tilde{x}} = g\mathfrak{I}_{\tilde{x}}g^{-1}$.) Set $\mathfrak{G}_{k(x)} \stackrel{\mathrm{def}}{=} \mathfrak{D}_{\tilde{x}}/\mathfrak{I}_{\tilde{x}}$. Thus, if we take a point $\tilde{\tilde{x}} \in \Sigma_{\tilde{\tilde{X}}}$ above $\tilde{x} \in \Sigma_{\tilde{X}}$, then $\mathfrak{D}_{\tilde{x}}$, $\mathfrak{I}_{\tilde{x}}$, and $\mathfrak{G}_{k(x)}$ are quotients of $D_{\tilde{\tilde{x}}}$, $I_{\tilde{\tilde{x}}}$ and $G_{k(x)}$, respectively, where x stands for the image of $\tilde{\tilde{x}}$ in Σ_X. We have a canonical exact sequence

$$1 \to \mathfrak{I}_{\tilde{x}} \to \mathfrak{D}_{\tilde{x}} \to \mathfrak{G}_{k(x)} \to 1.$$

For each closed subgroup $\mathfrak{H} \subset \mathfrak{G}$, denote by $\tilde{x}_{\mathfrak{H}}$ the image of $\tilde{x}$ in $X_{\mathfrak{H}}$. Define

$$\tilde{K}_{\tilde{x}} \stackrel{\mathrm{def}}{=} \bigcup_{\mathfrak{H} \subset \mathfrak{G}} (K_{\mathfrak{H}})_{\tilde{x}_{\mathfrak{H}}},$$

where $\mathfrak{H}$ runs over all open subgroups of $\mathfrak{G}$, and $(K_{\mathfrak{H}})_{\tilde{x}_{\mathfrak{H}}}$ means the $\tilde{x}_{\mathfrak{H}}$-adic completion of $K_{\mathfrak{H}} \stackrel{\mathrm{def}}{=} (\tilde{K})^{\mathfrak{H}}$. Then the Galois group $\mathrm{Gal}(\tilde{K}_{\tilde{x}}/K_x)$ is naturally identified with $\mathfrak{D}_{\tilde{x}}$, where $x \stackrel{\mathrm{def}}{=} \tilde{x}_{\mathfrak{G}} \in \Sigma_X$.

In the rest of this subsection, we fix a prime number $l \neq p$, and make two assumptions: (1) $N^l = N$, or, equivalently, $\tilde{K}$ admits no l-cyclic extension; and (2) $\tilde{K}$ contains a primitive l-th root of unity.

Remark 1.2. Let $\mathscr{C}$ be a full class of finite groups.

(i) If $\mathbb{F}_l \in \mathscr{C}$, then the quotient $G^{(\mathscr{C})}$ of G satisfies these two assumptions.

(ii) If $\mathbb{F}_l \in \mathscr{C}$ and $\mathrm{Gal}(K(\zeta_l)/K) \in \mathscr{C}$, then the quotient $G^{\mathscr{C}}$ of G satisfies these two assumptions.

Lemma 1.3. *Let $\tilde{x} \in \Sigma_{\tilde{X}}$ and take $\tilde{\tilde{x}} \in \Sigma_{\tilde{\tilde{X}}}$ above $\tilde{x}$. Let $D_{\tilde{\tilde{x}},l}$ be an l-Sylow subgroup of $D_{\tilde{\tilde{x}}}$ and $\mathfrak{D}_{\tilde{x},l}$ the image of $D_{\tilde{\tilde{x}},l}$ under the natural surjection $D_{\tilde{\tilde{x}}} \twoheadrightarrow \mathfrak{D}_{\tilde{x}}$, which is an l-Sylow subgroup of $\mathfrak{D}_{\tilde{x}}$. Then the natural surjection $D_{\tilde{\tilde{x}},l} \twoheadrightarrow \mathfrak{D}_{\tilde{x},l}$ is an isomorphism.*

Proof. Take $t \in K$ such that t is a uniformizer at $x \overset{\text{def}}{=} \tilde{x}_{\mathfrak{G}} \in \Sigma_X$. Then by the two assumptions (and by Kummer theory), any l^n-th root t^{1/l^n} of t is contained in $\tilde{K}$. From this, it follows that $I_{\tilde{\tilde{x}},l} \overset{\text{def}}{=} D_{\tilde{\tilde{x}},l} \cap I_{\tilde{\tilde{x}}}$ is injectively mapped into $\mathfrak{D}_{\tilde{x}}$. Now, applying Proposition 1.1(i) to the quotient $G_{K_x} = D_{\tilde{\tilde{x}}} \twoheadrightarrow \mathfrak{D}_{\tilde{x}}$, we conclude that only Case 2 from that proposition can occur, as desired. □

Lemma 1.4. *Let $\mathfrak{G}'$ be an open subgroup of $\mathfrak{G}$, K' the (finite, separable) extension of K corresponding to $\mathfrak{G}' \subset \mathfrak{G}$, and G' the inverse image of $\mathfrak{G}'$ in G. (Thus, $G' = G_{K'}$.) Then, for each finite l-primary $\mathfrak{G}'$-module M and each $k \geq 0$, one has $H^k(\mathfrak{G}', M) \xrightarrow{\sim} H^k(G', M)$.*

Proof. Replacing K by K', we may assume that $K' = K$. (Observe that the two assumptions also hold for the quotient $G' \overset{\text{def}}{=} G_{K'} \twoheadrightarrow \mathfrak{G}' = G'/N$.) By Lemma 1.3, one has $\mathrm{cd}_l(N) \leq 1$. (See [Serre 1994, chapitre II, proposition 9], which only treats the number field case but whose proof works as it is in our function field case.) Next, by the assumption that $N^l = N$, one has $H^1(N, M) = \mathrm{Hom}(N, M) = 0$. Thus, we have $H^k(G, M) = H^k(\mathfrak{G}, H^0(N, M)) = H^k(\mathfrak{G}, M)$, as desired. □

Proposition 1.5 (Galois characterization of decomposition subgroups).

(i) *Let $\tilde{x} \neq \tilde{x}'$ be two elements of $\Sigma_{\tilde{X}}$. Then $\mathfrak{D}_{\tilde{x}} \cap \mathfrak{D}_{\tilde{x}'}$ is of order prime to l, and hence, in particular, is open neither in $\mathfrak{D}_{\tilde{x}}$ nor in $\mathfrak{D}_{\tilde{x}'}$.*

(ii) *Let $\mathrm{Dec}_l(\mathfrak{G}) \subset \mathrm{Sub}(\mathfrak{G})$ be the set of closed subgroups $\mathfrak{D}$ of $\mathfrak{G}$ satisfying the following property: There exists an open subgroup $\mathfrak{D}_0$ of $\mathfrak{D}$ such that for any open subgroup $\mathfrak{D}' \subset \mathfrak{D}_0$, $\dim_{\mathbb{F}_l} H^2(\mathfrak{D}', \mathbb{F}_l) = 1$. Define $\mathrm{Dec}_l^{\max}(\mathfrak{G}) \subset \mathrm{Dec}_l(\mathfrak{G})$ to be the set of maximal elements of $\mathrm{Dec}_l(\mathfrak{G})$. Then the map $\Sigma_{\tilde{X}} \to \mathrm{Sub}(\mathfrak{G})$, $\tilde{x} \mapsto \mathfrak{D}_{\tilde{x}}$ induces a bijection $\Sigma_{\tilde{X}} \xrightarrow{\sim} \mathrm{Dec}_l^{\max}(\mathfrak{G})$, and, in particular, is injective.*

Proof. (i) As in [Uchida 1977], this follows from the approximation theorem [Neukirch 1969b, Lemma 8]. More precisely, let $\mathfrak{D}_l$ be an l-Sylow subgroup of $\mathfrak{D}_{\tilde{x}} \cap \mathfrak{D}_{\tilde{x}'}$, and suppose that $\mathfrak{D}_l \neq 1$. Since $\mathfrak{D}_l \subset \mathfrak{D}_{\tilde{x},l}$ is torsion-free, $\mathfrak{D}_l$ is an infinite group. Thus, one may replace $\mathfrak{G}$ by any open subgroup, and assume that $\zeta_l \in K$, that the images x and x' in Σ_X of $\tilde{x}$ and $\tilde{x}'$ are distinct, and that the image of $\mathfrak{D}_l$ in $\mathfrak{G}^{\mathrm{ab}}/(\mathfrak{G}^{\mathrm{ab}})^l$ is nontrivial. In particular, this implies that the natural map

$$\mathfrak{D}_{\tilde{x}}^{\mathrm{ab}}/(\mathfrak{D}_{\tilde{x}}^{\mathrm{ab}})^l \times \mathfrak{D}_{\tilde{x}'}^{\mathrm{ab}}/(\mathfrak{D}_{\tilde{x}'}^{\mathrm{ab}})^l \to \mathfrak{G}^{\mathrm{ab}}/(\mathfrak{G}^{\mathrm{ab}})^l$$

is not injective. By Kummer theory, this last condition is equivalent to saying that the natural map

$$K^\times/(K^\times)^l \to K_x^\times/(K_x^\times)^l \times K_{x'}^\times/(K_{x'}^\times)^l$$

is not surjective. This contradicts the approximation theorem. (Note that $(K_x^\times)^l$ and $(K_{x'}^\times)^l$ are open in $K_x^\times$ and $K_{x'}^\times$, respectively.)

(ii) By Proposition 1.1(i) and Lemmas 1.3 and 1.4, the proof of Uchida [1977] (which is essentially due to Neukirch, [1969a; 1969b]) works as it is. See [Uchida 1977, Lemmas 1–3] for more details. □

Remark 1.6. For other characterizations of decomposition groups — applicable to much more general situations — see, for example, Theorem 1.16 of [Pop 1994], Theorem 2 of [Koenigsmann 2003], or the results in [Engler and Koenigsmann 1998; Engler and Nogueira 1994].

1D. ***Fundamental groups of curves.*** Write

$$I \stackrel{\text{def}}{=} \langle I_{\tilde{\tilde{x}}} \rangle_{\tilde{\tilde{x}} \in \Sigma_{\tilde{\tilde{X}}}}$$

for the closed subgroup of G generated by the inertia subgroups $I_{\tilde{\tilde{x}}}$ for all $\tilde{\tilde{x}} \in \Sigma_{\tilde{\tilde{X}}}$, and call it the inertia subgroup of G. Then I is normal in G. The quotient G/I is canonically identified with the fundamental group $\pi_1(X)$ of X with base point $\mathrm{Spec}(\overline{K}) \to X$ [Grothendieck and Raynaud 1971]. We have a natural exact sequence

$$1 \to \pi_1(\overline{X}) \to \pi_1(X) \stackrel{\text{pr}}{\to} G_k \to 1,$$

where $\pi_1(\overline{X})$ is the fundamental group of $\overline{X} \stackrel{\text{def}}{=} X \times_k \bar{k}$ with base point $\mathrm{Spec}(\overline{K}) \to \overline{X}$ and pr is the canonical projection. We have the exact sequence

$$1 \to \pi_1(X)^{\text{ab,tor}} \to \pi_1(X)^{\text{ab}} \stackrel{\text{pr}}{\to} G_k \to 1,$$

where $\pi_1(X)^{\text{ab,tor}}$ is the torsion subgroup of $\pi_1(X)^{\text{ab}}$, and pr is the canonical projection. Moreover, $\pi_1(X)^{\text{ab,tor}}$ is a finite abelian group that is canonically isomorphic to the group $J_X(k)$ of k-rational points of the Jacobian variety J_X of X.

More generally, write $\mathfrak{I} \stackrel{\text{def}}{=} \langle \mathfrak{I}_{\tilde{x}} \rangle_{\tilde{x} \in \Sigma_{\tilde{X}}}$ for the closed subgroup of $\mathfrak{G}$ generated by the inertia subgroups $\mathfrak{I}_{\tilde{x}}$ for all $\tilde{x} \in \Sigma_{\tilde{X}}$, and call it the inertia subgroup of $\mathfrak{G}$. Then $\mathfrak{I}$ is normal in $\mathfrak{G}$. Set $\Pi_X \stackrel{\text{def}}{=} \mathfrak{G}/\mathfrak{I}$, which is a quotient of $\pi_1(X)$. Define $\Pi_{\overline{X}}$ to be the image of $\pi_1(\overline{X})$ in Π_X. Then we have a natural exact sequence

$$1 \to \Pi_{\overline{X}} \to \Pi_X \stackrel{\text{pr}}{\to} \mathfrak{G}_k \to 1.$$

When $\mathfrak{G} = G^{(\mathscr{C})}$ for a full class $\mathscr{C}$ of finite groups, we have $\Pi_X = \pi_1(X)^{(\mathscr{C})}$. In this case, we have the exact sequence:

$$1 \to \Pi_X^{\text{ab,tor}} \to \Pi_X^{\text{ab}} \stackrel{\text{pr}}{\to} G_k \to 1,$$

where $\Pi_X^{\mathrm{ab,tor}}$ is the torsion subgroup of Π_X^{ab}. Moreover, $\Pi_X^{\mathrm{ab,tor}}$ is a finite abelian group that is canonically isomorphic to the maximal (pro-)$\mathscr{C}$-quotient $J_X(k)^{\mathscr{C}}$ of the finite group $J_X(k)$.

2. Basic properties of homomorphisms between Galois groups

In this section we investigate some basic properties of homomorphisms between Galois groups of function fields of curves over finite fields. First, we shall investigate a class of homomorphisms between decomposition subgroups, which arise naturally from the class of homomorphisms between (quotients of) Galois groups that we consider in Sections 3 and 4.

2A. ***Homomorphisms between Galois groups of local fields of positive characteristics.*** For $i \in \{1, 2\}$, let $p_i > 0$ be a prime number. Let L_i be a complete discrete valuation field of equal characteristic p_i, with finite residue field ℓ_i. Let $\mathbb{O}_{L_i}$ be the ring of integers of L_i. Also, fix a separable closure L_i^{sep} of L_i. We shall denote the residue field of L_i^{sep} by $\bar{\ell}_i$, since it is an algebraic closure of ℓ_i. Note that ℓ_i and $\bar{\ell}_i$ can also be regarded naturally as subfields of L_i and L_i^{sep}, respectively. Write $D_i \overset{\mathrm{def}}{=} \mathrm{Gal}(L_i^{\mathrm{sep}}/L_i)$ for the corresponding absolute Galois group of L_i, and call $I_i \subset D_i$ the inertia subgroup. For each prime number l, let $D_{i,l}$ be an l-Sylow subgroup of D_i.

By local class field theory [Serre 1967], we have a natural isomorphism

$$(L_i^{\times})^{\wedge} \xrightarrow{\sim} D_i^{\mathrm{ab}},$$

where $(L_i^{\times})^{\wedge} \overset{\mathrm{def}}{=} \varprojlim_n L_i^{\times}/(L_i^{\times})^n$. In particular, D_i^{ab} fits into an exact sequence

$$0 \to \mathbb{O}_{L_i}^{\times} \to D_i^{\mathrm{ab}} \to \hat{\mathbb{Z}} \to 0$$

(arising from a similar exact sequence for $(L_i^{\times})^{\wedge}$), where $\mathbb{O}_{L_i}^{\times}$ is the group of multiplicative units in $\mathbb{O}_{L_i}$. Moreover, we obtain natural inclusions

$$\ell_i^{\times} \times U_i^1 = \mathbb{O}_{L_i}^{\times} \subset L_i^{\times} \hookrightarrow D_i^{\mathrm{ab}},$$

where U_i^1 is the group of principal units in $\mathbb{O}_{L_i}^{\times}$, and

$$L_i^{\times}/\mathbb{O}_{L_i}^{\times} \xrightarrow{\sim} \mathbb{Z} \hookrightarrow D_i^{\mathrm{ab}}/\mathrm{Im}(\mathbb{O}_{L_i}^{\times})$$

(where $\xrightarrow{\sim}$ is the isomorphism induced by the valuation), by considering the Frobenius element.

Let $\mathfrak{D}_i$ be a quotient of D_i, $\mathfrak{I}_i$ the image of I_i in $\mathfrak{D}_i$, and $\mathfrak{G}_{\ell_i} \overset{\mathrm{def}}{=} \mathfrak{D}_i/\mathfrak{I}_i$. For each prime number l, let $\mathfrak{D}_{i,l}$ be the image of $D_{i,l}$ in $\mathfrak{D}_i$, which is an l-Sylow subgroup of $\mathfrak{D}_i$. Write

$$\mathfrak{Im}(\ell_i^{\times}),\ \mathfrak{Im}(U_i^1) \subset \mathfrak{Im}(\mathbb{O}_{L_i}^{\times}) \subset \mathfrak{Im}(L_i^{\times}) \subset \mathfrak{D}_i^{\mathrm{ab}}$$

for the images of $\ell_i^\times$, U_i^1, $\mathbb{O}_{L_i}^\times$ and $L_i^\times$ in $\mathfrak{D}_i^{\mathrm{ab}}$, respectively. In the rest of this subsection, we assume that either $\mathfrak{D}_i = D_i$, $i = 1, 2$ or $\mathfrak{D}_i = D_i^{\mathrm{t}} = D_i^{(p_i')}$, $i = 1, 2$, and refer to the former and the latter cases as the profinite and the tame cases, respectively. Thus, we have $\mathfrak{D}_i^{\mathrm{ab}} = (L_i^\times)^\wedge$, $\mathfrak{Im}(L_i^\times) = L_i^\times$, $\mathfrak{Im}(\mathbb{O}_{L_i}^\times) = \mathbb{O}_{L_i}^\times$, $\mathfrak{Im}(\ell_i^\times) = \ell_i^\times$ and $\mathfrak{Im}(U_i^1) = U_i^1$ in the profinite case, and $\mathfrak{D}_i^{\mathrm{ab}} = (L_i^\times)^\wedge/U_i^1$, $\mathfrak{Im}(L_i^\times) = L_i^\times/U_i^1$, $\mathfrak{Im}(\mathbb{O}_{L_i}^\times) = \mathbb{O}_{L_i}^\times/U_i^1 = \mathfrak{Im}(\ell_i^\times) = \ell_i^\times$ and $\mathfrak{Im}(U_i^1) = \{1\}$ in the tame case.

Let

$$\tau : \mathfrak{D}_1 \twoheadrightarrow \mathfrak{D}_2$$

be a surjective homomorphism between profinite groups. Write $\tau^{\mathrm{ab}} : \mathfrak{D}_1^{\mathrm{ab}} \twoheadrightarrow \mathfrak{D}_2^{\mathrm{ab}}$ for the induced surjective homomorphism between the maximal abelian quotients. For each prime number l, $\tau(\mathfrak{D}_{1,l})$ is an l-Sylow subgroup of $\mathfrak{D}_2$, and we shall assume that $\tau(\mathfrak{D}_{1,l}) = \mathfrak{D}_{2,l}$.

Proposition 2.1 (invariants of arbitrary surjective homomorphisms between decomposition groups). (i) *The equality $p_1 = p_2$ holds. Set $p \overset{def}{=} p_1 = p_2$.*

(ii) *Let $l \neq p$ be a prime number. We have $\mathfrak{D}_{1,l} \cap \mathrm{Ker}\,\tau = \{1\}$. In particular, $\mathrm{Ker}\,\tau$ is pro-p. In the tame case, τ is an isomorphism.*

(iii) *The homomorphism τ induces a natural bijection $\ell_1^\times \xrightarrow{\sim} \ell_2^\times$ between the multiplicative groups of residue fields. In particular, ℓ_1 and ℓ_2 have the same cardinality.*

(iv) *τ induces naturally an isomorphism $M_{\bar{\ell}_1} \xrightarrow{\sim} M_{\bar{\ell}_2}$, which is Galois-equivariant with respect to τ. In particular, τ commutes with the cyclotomic characters $\chi_i : \mathfrak{D}_i \to (\hat{\mathbb{Z}}^{p'})^\times$ of $\mathfrak{D}_i$, that is, the following diagram is commutative:*

$$\begin{array}{ccc} (\hat{\mathbb{Z}}^{p'})^\times & = & (\hat{\mathbb{Z}}^{p'})^\times \\ {\scriptstyle\chi_1}\uparrow & & \uparrow{\scriptstyle\chi_2} \\ \mathfrak{D}_1 & \xrightarrow{\tau} & \mathfrak{D}_2. \end{array}$$

(v) *We have $\tau(\mathfrak{I}_1) = \mathfrak{I}_2$.*

(vi) *The homomorphism $\tau^{\mathrm{ab}} : \mathfrak{D}_1^{\mathrm{ab}} \to \mathfrak{D}_2^{\mathrm{ab}}$ preserves $\mathfrak{Im}(L_i^\times)$, $\mathfrak{Im}(\mathbb{O}_{L_i}^\times)$, $\mathfrak{Im}(\ell_i^\times)$ and $\mathfrak{Im}(U_i^1)$. Further, the isomorphism $\mathfrak{D}_1^{\mathrm{ab}}/\mathfrak{Im}(\mathbb{O}_{L_1}^\times) \to \mathfrak{D}_2^{\mathrm{ab}}/\mathfrak{Im}(\mathbb{O}_{L_2}^\times)$ induced by τ preserves the respective Frobenius elements.*

Proof. Property (i) follows by considering the q-Sylow subgroups of $\mathfrak{D}_i$ for various prime numbers q. Indeed, for $i \in \{1, 2\}$, $\mathfrak{D}_{i,p_i}$ is not (topologically) finitely generated (resp. is cyclic) in the profinite (resp. tame) case, while $\mathfrak{D}_{i,l}$ for a prime number $l \neq p_i$ is (topologically) finitely generated and noncyclic. Accordingly, the surjection $\mathfrak{D}_{1,p_2} \twoheadrightarrow \mathfrak{D}_{2,p_2}$ (resp. $\mathfrak{D}_{1,p_1} \twoheadrightarrow \mathfrak{D}_{2,p_1}$) cannot exist in the profinite (resp. tame) case, unless $p_1 = p_2$. Thus, we must have $p_1 = p_2$.

The first assertion of (ii) follows from Proposition 1.1(i), applied to the quotient $D_1 \twoheadrightarrow \mathfrak{D}_1 \overset{\tau}{\twoheadrightarrow} \mathfrak{D}_2$. The second assertion follows from the first. The third assertion follows from the second, together with the fact (which can be checked easily) that D_1^{t} admits no nontrivial normal pro-p subgroup.

Next, we prove (iii). By local class field theory, the torsion subgroup $\mathfrak{D}_i^{\mathrm{ab,tor}}$ of $\mathfrak{D}_i^{\mathrm{ab}}$ is naturally identified with ${\ell_i}^{\times}$ (both in the profinite and the tame cases), and hence, in particular, is finite of order prime to p. By (ii), the kernel of the surjective homomorphism $\tau^{\mathrm{ab}} : \mathfrak{D}_1^{\mathrm{ab}} \to \mathfrak{D}_2^{\mathrm{ab}}$ is pro-p. Thus, τ^{ab} induces a natural isomorphism $\mathfrak{D}_1^{\mathrm{ab,tor}} \overset{\sim}{\to} \mathfrak{D}_2^{\mathrm{ab,tor}}$, which is naturally identified with $\ell_1^{\times} \overset{\sim}{\to} \ell_2^{\times}$, as desired.

By applying the above argument to open subgroups of $\mathfrak{D}_i$ (which correspond to each other via τ), with $i = 1, 2$, and passing to the projective limit with respect to the norm maps, we obtain a natural isomorphism $M_{\bar{\ell}_1} \overset{\sim}{\to} M_{\bar{\ell}_2}$ between the modules of roots of unity. Here, we use the fact that if L_i' is a finite extension of L_i corresponding to an open subgroup $\mathfrak{D}_i'$ of $\mathfrak{D}_i$, then the following diagram commutes:

$$\begin{array}{ccc} ({L_i'}^{\times})^{\wedge} & \twoheadrightarrow & \mathfrak{D}_i'^{\mathrm{ab}} \\ {\scriptstyle \mathrm{Norm}}\downarrow & & \downarrow \\ ({L_i}^{\times})^{\wedge} & \twoheadrightarrow & \mathfrak{D}_i^{\mathrm{ab}}, \end{array}$$

where the horizontal maps are the natural surjective homomorphisms from local class field theory, and the map $\mathfrak{D}_i'^{\mathrm{ab}} \to \mathfrak{D}_i^{\mathrm{ab}}$ is induced by the natural inclusion $\mathfrak{D}_i' \subset \mathfrak{D}_i$. Further, this identification is (by construction) Galois-compatible with respect to the homomorphism τ. This completes the proof of (iv).

Property (v) follows from property (iv), since $\mathfrak{I}_i$ coincides with the kernel of χ_i for $i = 1, 2$.

Next, we prove (vi). First, τ^{ab} preserves the image $\mathfrak{Im}(\mathbb{O}_{L_i}^{\times})$ by (v), since this image coincides with the image of the inertia subgroup $\mathfrak{I}_i$. Since $\mathfrak{Im}(\ell_i^{\times})$ (resp. $\mathfrak{Im}(U_i^1)$) is the maximal prime-to-p (resp. pro-p) subgroup of $\mathfrak{Im}(\mathbb{O}_{L_i}^{\times})$, property (vi) for $\mathfrak{Im}(\ell_i^{\times})$ (resp. $\mathfrak{Im}(U_i^1)$) follows. Further, by (iii) and (iv), the homomorphism $\mathfrak{D}_1^{\mathrm{ab}}/\mathfrak{Im}(\mathbb{O}_{L_1}^{\times}) \to \mathfrak{D}_2^{\mathrm{ab}}/\mathfrak{Im}(\mathbb{O}_{L_2}^{\times})$ induced by τ preserves the respective Frobenius elements, since such an element is characterized as the unique element whose image under χ_i is $\sharp(\ell_i)$. Finally, since $\mathfrak{Im}(L_i^{\times})$ is the inverse image in $\mathfrak{D}_i^{\mathrm{ab}}$ of the subgroup generated by the Frobenius element in $\mathfrak{D}_i^{\mathrm{ab}}/\mathfrak{Im}(\mathbb{O}_{L_i}^{\times})$ for $i = 1, 2$, they are preserved by τ^{ab}. □

2B. ***Homomorphisms between Galois groups of function fields of curves over finite fields.*** Next, we shall investigate some basic properties of homomorphisms between Galois groups of function fields of curves over finite fields. We follow the notations in Section 1, especially subsections 1A and 1B. Moreover:

Notation. (i) For $i \in \{1, 2\}$, let k_i be a finite field of characteristic $p_i > 0$. Let X_i be a smooth, proper, geometrically connected curve of genus $g_i \geq 0$ over k_i. Let $K_i = K_{X_i}$ be the function field of X_i and fix an algebraic closure $\overline{K}_i$ of K_i. Let K_i^{sep} be the separable closure of K_i in $\overline{K}_i$, and $\bar{k}_i$ the algebraic closure of k_i in $\overline{K}_i$. Following the notations in Section 1, we will write $G_i \overset{\mathrm{def}}{=} G_{K_i} = \mathrm{Gal}(K_i^{\mathrm{sep}}/K_i)$ for the absolute Galois group of K_i, and $\overline{G}_i \overset{\mathrm{def}}{=} G_{K_i\bar{k}_i} = \mathrm{Gal}(K_i^{\mathrm{sep}}/K_i\bar{k}_i)$ for the absolute Galois group of $K_i\bar{k}_i$.

(ii) Let N_i be a normal closed subgroup of G_i and set $\mathfrak{G}_i \overset{\mathrm{def}}{=} G_i/N_i$. Let $\tilde{K}_i$ denote the Galois extension of K_i corresponding to N_i, that is, $\tilde{K}_i \overset{\mathrm{def}}{=} (K_i^{\mathrm{sep}})^{N_i}$. Let $\overline{G}_i$ be the image of $\overline{G}_i$ in $\mathfrak{G}_i$, and set $\mathfrak{G}_{k_i} \overset{\mathrm{def}}{=} \mathfrak{G}_i/\overline{\mathfrak{G}}_i$, which is a quotient of $G_{k_i} = \mathrm{Gal}(\bar{k}_i/k_i)$. For $i = 1, 2$, let us denote by φ_{k_i} the image in $\mathfrak{G}_{k_i}$ of the $\sharp(k_i)$-th power Frobenius element of G_{k_i}.

(iii) Write $\tilde{X}_i$ for the integral closure of X_i in $\tilde{K}_i$. The Galois group $\mathfrak{G}_i$ acts naturally on the set $\Sigma_{\tilde{X}_i}$, and the quotient $\Sigma_{\tilde{X}_i}/\mathfrak{G}_i$ is naturally identified with Σ_{X_i}. Denote the natural quotient map $\Sigma_{\tilde{X}_i} \to \Sigma_{X_i}$ by q_i. For a point $\tilde{x}_i \in \Sigma_{\tilde{X}_i}$, with residue field $k_i(\tilde{x}_i)$ (which is naturally identified with a subfield of $\bar{k}_i$), we define its decomposition group $\mathfrak{D}_{\tilde{x}_i}$ and inertia group $\mathfrak{I}_{\tilde{x}_i}$ by

$$\mathfrak{D}_{\tilde{x}_i} \overset{\mathrm{def}}{=} \{\gamma \in \mathfrak{G}_i \mid \gamma(\tilde{x}_i) = \tilde{x}_i\}$$

and

$$\mathfrak{I}_{\tilde{x}_i} \overset{\mathrm{def}}{=} \{\gamma \in \mathfrak{D}_{\tilde{x}_i} \mid \gamma \text{ acts trivially on } k_i(\tilde{x}_i)\},$$

respectively. Set $\mathfrak{G}_{k_i(x_i)} \overset{\mathrm{def}}{=} \mathfrak{D}_{\tilde{x}_i}/\mathfrak{I}_{\tilde{x}_i}$, where x_i stands for the image of $\tilde{x}_i$ in Σ_{X_i}.

Write $\mathfrak{I}_i \overset{\mathrm{def}}{=} \langle I_{\tilde{x}_i}\rangle_{\tilde{x}_i \in \Sigma_{\tilde{X}_i}}$ for the closed subgroup of $\mathfrak{G}_i$ generated by the inertia subgroups $\mathfrak{I}_{\tilde{x}_i}$ for all $\tilde{x}_i \in \Sigma_{\tilde{X}_i}$, and call it the inertia subgroup of $\mathfrak{G}_i$. Then $\mathfrak{I}_i$ is normal in $\mathfrak{G}_i$.

(iv) Let $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ be a continuous homomorphism between profinite groups.

Proposition 2.2 (image of a decomposition subgroup). *Let $l \neq p_1, p_2$ be a prime number, and assume that* (1) $N_2^l = N_2$, *or, equivalently, $\tilde{K}_2$ admits no l-cyclic extension*; *and* (2) *$\tilde{K}_2$ contains a primitive l-th root of unity. For each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$, fix an l-Sylow subgroup $\mathfrak{D}_{\tilde{x}_1,l}$ of $\mathfrak{D}_{\tilde{x}_1}$ and set $\mathfrak{I}_{\tilde{x}_1,l} \overset{def}{=} \mathfrak{I}_{\tilde{x}_1} \cap \mathfrak{D}_{\tilde{x}_1,l}$, which is an l-Sylow subgroup of $\mathfrak{I}_{\tilde{x}_1}$. Let $\Sigma_{\tilde{X}_1,\sigma,l}$ be the set of $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$ such that $\mathrm{cd}_l(\sigma(\mathfrak{D}_{\tilde{x}_1})) = 2$. Then*:

(i) *There exists a unique map $\tilde{\phi} = \tilde{\phi}_{\sigma,l} : \Sigma_{\tilde{X}_1,\sigma,l} \to \Sigma_{\tilde{X}_2}$ such that $\sigma(\mathfrak{D}_{\tilde{x}_1}) \subset \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$ for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1,\sigma,l}$.*

(ii) *For each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1,\sigma,l}$, there exists an l-Sylow subgroup $\mathfrak{D}_{\tilde{\phi}(\tilde{x}_1),l}$ of $\mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$ such that $\sigma(\mathfrak{D}_{\tilde{x}_1,l}) \subset \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1),l}$. Moreover, we have $\sigma(\mathfrak{I}_{\tilde{x}_1,l}) \subset \mathfrak{I}_{\tilde{\phi}(\tilde{x}_1),l}$, where we set*

$$\mathfrak{I}_{\tilde{\phi}(\tilde{x}_1),l} \overset{def}{=} \mathfrak{I}_{\tilde{\phi}(\tilde{x}_1)} \cap \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1),l},$$

which is an l-Sylow subgroup of $\mathfrak{I}_{\tilde{\phi}(\tilde{x}_1)}$.

(iii) *The subset $\Sigma_{\tilde{X}_1,\sigma,l} \subset \Sigma_{\tilde{X}_1}$ is $\mathfrak{G}_1$-stable, or, equivalently,*

$$\Sigma_{\tilde{X}_1,\sigma,l} = q_1^{-1}(\Sigma_{X_1,\sigma,l}),$$

where $\Sigma_{X_1,\sigma,l} \overset{def}{=} q_1(\Sigma_{\tilde{X}_1,\sigma,l})$. The map $\tilde{\phi}$ is Galois-compatible with respect to σ: we have

$$\tilde{\phi}(g_1\tilde{x}_1) = \sigma(g_1)\tilde{\phi}(\tilde{x}_1)$$

for any $\tilde{x}_1 \in \Sigma_{\tilde{X}_1,\sigma,l}$ and any $g_1 \in \mathfrak{G}_1$. In particular, $\tilde{\phi}$ induces naturally a map $\phi = \phi_{\sigma,l} : \Sigma_{X_1,\sigma,l} \to \Sigma_{X_2}$.

(iv) *For any $\tilde{x}_1 \in \Sigma_{\tilde{X}_1} \smallsetminus \Sigma_{\tilde{X}_1,\sigma,l}$, we have $\sigma(\mathfrak{I}_{\tilde{x}_1,l}) = \{1\}$.*

(v) *For two primes $l = l_1, l_2$ satisfying the assumptions, $\tilde{\phi}_{\sigma,l_1}$ and $\tilde{\phi}_{\sigma,l_2}$ coincide with each other on the intersection $\Sigma_{\tilde{X}_1,\sigma,l_1} \cap \Sigma_{\tilde{X}_1,\sigma,l_2}$.*

Proof.

(i) Take $\tilde{x}_1 \in \Sigma_{\tilde{X}_1,\sigma,l}$. Applying Proposition 1.1(i)(ii) to $\mathfrak{D} = \sigma(\mathfrak{D}_{\tilde{x}_1})$, we have $\sigma(\mathfrak{D}_{\tilde{x}_1}) \in \mathrm{Dec}_l(\mathfrak{G}_2)$ in the notation of the result in part (ii) of Proposition 1.5. Thus, by this same result, there exists $\tilde{x}_2 \in \Sigma_{\tilde{X}_2}$ such that $\sigma(\mathfrak{D}_{\tilde{x}_1}) \subset \mathfrak{D}_{\tilde{x}_2}$. By Proposition 1.5(i), such $\tilde{x}_2$ is unique. So, set

$$\tilde{\phi}(\tilde{x}_1) = \tilde{x}_2,$$

which has the desired properties.

(ii) The existence of $\mathfrak{D}_{\tilde{\phi}(\tilde{x}_1),l}$ follows from the fact that $\sigma(\mathfrak{D}_{\tilde{x}_1,l}) \subset \sigma(\mathfrak{D}_{\tilde{x}_1}) \subset \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$ and that $\sigma(\mathfrak{D}_{\tilde{x}_1,l})$ is pro-l. Finally, consider the composite map of

$$\mathfrak{D}_{\tilde{x}_1} \overset{\sigma}{\to} \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)} \twoheadrightarrow \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}/\mathfrak{I}_{\tilde{\phi}(\tilde{x}_1)} = \mathfrak{G}_{k_2(q_2(\tilde{\phi}(\tilde{x}_1)))}.$$

Then, since $\mathrm{cd}_l(\mathfrak{G}_{k_2(q_2(\tilde{\phi}(\tilde{x}_1)))}) = 1$, the image of $\mathfrak{I}_{\tilde{x}_1,l}$ in $\mathfrak{G}_{k_2(q_2(\tilde{\phi}(\tilde{x}_1)))}$ must be trivial by Proposition 1.1(i), as desired.

(iii) Immediate from the definitions.

(iv) We have $\mathrm{cd}_l(\sigma(\mathfrak{D}_{\tilde{x}_1})) \leq \mathrm{cd}_l(\mathfrak{G}_2) \leq 2 < \infty$, where the second inequality follows from Lemma 1.4. Now, the assertion follows from Proposition 1.1(i).

(v) This follows from the fact that the defining property $\sigma(\mathfrak{D}_{\tilde{x}_1}) \subset \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$ of $\tilde{\phi}$ is independent of l. □

We shall consider the following conditions:

Condition 1. Either $\mathfrak{G}_i = G_i$, $i = 1, 2$ or $\mathfrak{G}_i = G_i^{(p_i')}$, $i = 1, 2$. We refer to the former and the latter cases as the profinite and the prime-to-characteristic cases, respectively. (Observe that conditions (1) and (2) in Proposition 2.2 are then satisfied for any prime number $l \neq p_1, p_2$.) In particular, we have $\mathfrak{G}_{k_i} = G_{k_i}$ in both cases.

Condition 2. The map $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ commutes with the projections $\mathrm{pr}_1, \mathrm{pr}_2$, that is, it inserts into the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{\mathfrak{G}}_1 & \longrightarrow & \mathfrak{G}_1 & \xrightarrow{\mathrm{pr}_1} & G_{k_1} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \bar{\sigma}} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma_0} & & \\ 1 & \longrightarrow & \overline{\mathfrak{G}}_2 & \longrightarrow & \mathfrak{G}_2 & \xrightarrow{\mathrm{pr}_2} & G_{k_2} & \longrightarrow & 1, \end{array}$$

where the rows are exact.

Condition 3. The map $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is an open homomorphism.

In the rest of this section, we assume that Condition 1 holds.

Lemma 2.3. *In the prime-to-characteristic case, Condition 2 automatically holds. In the profinite case, if $\sigma(\mathfrak{I}_1) \subseteq \mathfrak{I}_2$, then Condition 2 holds.*

Proof. In the prime-to-characteristic case, the quotient $\mathrm{pr}_i : \mathfrak{G}_i \twoheadrightarrow G_{k_i}$ coincides with $\mathfrak{G}_i^{\mathrm{ab}}$ modulo the closure of the torsion subgroup. Thus, σ commutes with the projections $\mathrm{pr}_1, \mathrm{pr}_2$.

In the profinite case, assume that $\sigma(\mathfrak{I}_1) \subseteq \mathfrak{I}_2$. Then σ induces naturally, by passing to the quotients $\mathfrak{G}_i/\mathfrak{I}_i$, a homomorphism $\pi_1(X_1) \to \pi_1(X_2)$ between fundamental groups. The quotient $\mathrm{pr}_i : \mathfrak{G}_i \twoheadrightarrow \pi_1(X_i) \twoheadrightarrow G_{k_i}$ coincides with $\pi_1(X_i)^{\mathrm{ab}}$ modulo the torsion subgroup. Thus, σ commutes with the projections $\mathrm{pr}_1, \mathrm{pr}_2$. □

In the rest of this section, we assume, moreover, that Condition 3 holds. Then note that, if Condition 2 also holds and if $\sigma_0 : G_{k_1} \to G_{k_2}$ and $\bar{\sigma} : \overline{\mathfrak{G}}_1 \to \overline{\mathfrak{G}}_2$ are homomorphisms induced by σ, then automatically σ_0 is open and injective and $\bar{\sigma}$ is open.

Lemma 2.4 (invariance of the characteristics). *The equality $p_1 = p_2$ holds.*

Proof. By replacing $\mathfrak{G}_2$ by the open subgroup $\sigma(\mathfrak{G}_1) \subset \mathfrak{G}_2$, we may and shall assume that σ is surjective.

In the profinite case, the assertion follows by considering the (pro-)q-parts of $\mathfrak{G}_i^{\mathrm{ab}}$ for various prime numbers q. More precisely, for $i \in \{1, 2\}$, consider the filtration $\mathfrak{G}_i^{\mathrm{ab}} = F_i^0 \supset F_i^1 \supset F_i^2$, where F_i^1 is the image of $\overline{\mathfrak{G}}_i = \mathrm{Ker}(\mathfrak{G}_i \to G_{k_i})$ and F_i^2 is the image of $\mathrm{Ker}(\mathfrak{G}_i \to \pi_1(X_i))$. Then, by global class field theory, $F_i^0/F_i^1 = G_{k_i}$ ($\simeq \hat{\mathbb{Z}}$), $F_i^1/F_i^2 = J_{X_i}(k_i)$ (finite), and

$$F_i^2 = \Big(\prod_{x_i \in \Sigma_{X_i}} \hat{\mathbb{O}}_{X_i, x_i}^{\times} \Big) \Big/ k_i^{\times},$$

where $\hat{\mathbb{O}}_{X_i, x_i}^{\times}$ is the multiplicative group of the completed local ring of X_i at x_i. Further, we have a natural decomposition $\hat{\mathbb{O}}_{X_i, x_i}^{\times} = k(x_i)^{\times} \times U_{x_i}^1$, where $k(x_i)^{\times}$ is the multiplicative group of the residue field of X_i at x_i (and hence finite) and $U_{x_i}^1$ is

the group of principal units in $\hat{\mathbb{O}}^{\times}_{X_i,x_i}$ (and hence isomorphic to a direct product of countably infinite copies of $\mathbb{Z}_{p_i}$). Therefore, the p_i-part of $\mathfrak{G}_i^{\mathrm{ab}}$ modulo the closure of the torsion subgroup is not finitely generated, while the l-part of $\mathfrak{G}_i^{\mathrm{ab}}$ modulo the closure of the torsion subgroup, for a prime number $l \neq p_i$, is finitely generated (and even cyclic). (Note, however, that the l-torsion subgroup of $\mathfrak{G}_i^{\mathrm{ab}}$ is infinite.) Thus, $\mathfrak{G}_2$ being a quotient of $\mathfrak{G}_1$ (via σ) we must have $p_1 = p_2$.

In the prime-to-characteristic case, the assertion follows by considering the q-Sylow subgroups $\mathfrak{G}_{i,q}$ of $\mathfrak{G}_i$ for various prime numbers q. As σ is assumed to be surjective, we may and shall take $\mathfrak{G}_{2,q} = \sigma(\mathfrak{G}_{1,q})$. Indeed, for $i \in \{1, 2\}$, $\mathfrak{G}_{i,p_i}$ is cyclic, while $\mathfrak{G}_{i,l}$ for a prime number $l \neq p_i$ is noncyclic. Accordingly, the surjection $\mathfrak{G}_{1,p_1} \twoheadrightarrow \mathfrak{G}_{2,p_1}$ cannot exist, unless $p_1 = p_2$. Thus $p_1 = p_2$. □

So, from now on, set $p \overset{\text{def}}{=} p_1 = p_2$.

Remark 2.5. The same argument used in the proof of (the prime-to-characteristic case of) Lemma 2.3 shows that an open homomorphism $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ between profinite groups automatically commutes with the natural projections $\mathrm{pr}_i' : \mathfrak{G}_i \to G_{k_i}^{p'}$, induced by pr_i, for $i = 1, 2$. Thus, we have the commutative diagram

$$\begin{array}{ccc} \mathfrak{G}_1 & \xrightarrow{\mathrm{pr}_1'} & G_{k_1}^{p'} \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma_0'} \\ \mathfrak{G}_2 & \xrightarrow{\mathrm{pr}_2'} & G_{k_2}^{p'}, \end{array}$$

where the right column is automatically open and injective. The authors do not know, at least at the time of writing, whether or not Condition 2 follows from Conditions 1 and 3 in general (that is, even in the profinite case).

In the rest of this subsection we assume that Condition 2 holds.

Lemma 2.6. *The map σ induces a natural open homomorphism $\sigma' : G_1^{(p')} \to G_2^{(p')}$, which commutes with the canonical projections*

$$G_i^{(p')} \to G_{k_i}; \quad i = 1, 2.$$

For $i = 1, 2$, let $\mathfrak{I}_i'$ be the image of $\mathfrak{I}_i \subset \mathfrak{G}_i$ in $G_i^{(p')}$. Then $\sigma'(\mathfrak{I}_1') \subset \mathfrak{I}_2'$. Thus, σ induces a natural open homomorphism $\tau' : \pi_1(X_1)^{(p')} \to \pi_1(X_2)^{(p')}$, which commutes with the canonical projections $\pi_1(X_i)^{(p')} \to G_{k_i}$; $i = 1, 2$. In particular, we have $g_1 \geq g_2$.

Proof. The first assertion is clear. The second follows from Proposition 2.2(ii)(iv). The third assertion follows from the second. Now, $\tau' : \pi_1(X_1)^{(p')} \to \pi_1(X_2)^{(p')}$ induces an open homomorphism $\pi_1(\overline{X}_1)^{p'} \to \pi_1(\overline{X}_2)^{p'}$, and hence an open homomorphism $\pi_1(\overline{X}_1)^{p',\mathrm{ab}} \to \pi_1(\overline{X}_2)^{p',\mathrm{ab}}$. Since $\pi_1(\overline{X}_i)^{p',\mathrm{ab}}$ is a free $\hat{\mathbb{Z}}^{p'}$-module of rank $2g_i$ for $i = 1, 2$, this implies the last assertion. □

Lemma 2.7. *For a prime number $l \neq p$, the map $\phi = \phi_{\sigma,l} : \Sigma_{X_1,\sigma,l} \to \Sigma_{X_2}$ is almost surjective, that is, $\Sigma_{X_2} \setminus \phi(\Sigma_{X_1,\sigma,l})$ is finite. In particular, $\Sigma_{X_1,\sigma,l}$ is infinite* (*and hence, a fortiori, nonempty*).

Proof. Assume that the set $S \overset{\text{def}}{=} \Sigma_{X_2} \setminus \phi(\Sigma_{X_1,\sigma,l})$ is infinite. Set $U_2 \overset{\text{def}}{=} X_2 \setminus S$.

As in (the third assertion of) Lemma 2.6, then σ induces an open homomorphism $\tau_1^{(l)} : \pi_1(X_1)^{(l)} \to \pi_1(U_2)^{(l)}$, which is a lifting of the homomorphism $\tau^{(l)} : \pi_1(X_1)^{(l)} \to \pi_1(X_2)^{(l)}$ induced by $\tau' : \pi_1(X_1)^{(p')} \to \pi_1(X_2)^{(p')}$. We have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(\overline{X}_1)^l & \twoheadrightarrow & \pi_1(X_1)^{(l)} & \overset{\mathrm{pr}_1}{\twoheadrightarrow} & G_{k_1} & \longrightarrow & 1 \\ & & \bar{\tau}_1^l \downarrow & & \tau_1^{(l)} \downarrow & & \sigma_0 \downarrow & & \\ 1 & \longrightarrow & \pi_1(\overline{U}_2)^l & \twoheadrightarrow & \pi_1(U_2)^{(l)} & \overset{\mathrm{pr}_2}{\twoheadrightarrow} & G_{k_2} & \longrightarrow & 1, \end{array}$$

where $\overline{U}_2 \overset{\text{def}}{=} U_2 \times_{k_2} \bar{k}_2$. Since $\tau_1^{(l)} : \pi_1(X_1)^{(l)} \to \pi_1(U_2)^{(l)}$ is open and $\sigma_0 : G_{k_1} \to G_{k_2}$ is (open and) injective, we see that $\bar{\tau}_1^l : \pi_1(\overline{X}_1)^l \to \pi_1(\overline{U}_2)^l$ is open. This is a contradiction, since $\pi_1(\overline{X}_1)^l$ is (topologically) finitely generated, while $\pi_1(\overline{U}_2)^l$ (and hence $\bar{\tau}_1^l(\pi_1(\overline{X}_1)^l)$ also) is not (topologically) finitely generated, since S is infinite. □

Lemma 2.8. *Let $\sigma_0 : G_{k_1} \to G_{k_2}$ be the* (*open, injective*) *homomorphism induced by σ. Set $d_0 \overset{def}{=} [G_{k_2} : \sigma_0(G_{k_1})]$.*

(i) *The following diagram is commutative*:

$$\begin{array}{ccc} (\hat{\mathbb{Z}}^{p'})^\times & = & (\hat{\mathbb{Z}}^{p'})^\times \\ {\scriptstyle \chi_{k_1}}\uparrow & & \uparrow{\scriptstyle \chi_{k_2}} \\ G_{k_1} & \xrightarrow{\sigma_0} & G_{k_2} \\ {\scriptstyle \mathrm{pr}_1}\uparrow & & \uparrow{\scriptstyle \mathrm{pr}_2} \\ \mathfrak{G}_1 & \xrightarrow{\sigma} & \mathfrak{G}_2, \end{array}$$

where χ_{k_i} is the cyclotomic character of G_{k_i} for $i = 1, 2$.

(ii) *We have $\sharp(k_1) = \sharp(k_2)^{d_0}$ and $\sigma_0(\varphi_{k_1}) = \varphi_{k_2}^{d_0}$.*

Proof. (i) Since the bottom square is commutative by the definition of σ_0, we only have to prove that the top square is commutative. As G_{k_2} is (topologically) generated by φ_{k_2}, we may write $\sigma_0(\varphi_{k_1}) = \varphi_{k_2}^{\alpha}$, where $\alpha \in \hat{\mathbb{Z}}$. Now, the desired commutativity $\chi_{k_2} \circ \sigma_0 = \chi_{k_1}$ is equivalent to saying that $\chi_{k_2}(\sigma_0(\varphi_{k_1})) = \chi_{k_1}(\varphi_{k_1})$ (as G_{k_1} is (topologically) generated by φ_{k_1}). Since $\chi_{k_1}(\varphi_{k_1}) = \sharp(k_1) = p^{[k_1:\mathbb{F}_p]}$ and

$$\chi_{k_2}(\sigma_0(\varphi_{k_1})) = \chi_{k_2}(\varphi_{k_2}^{\alpha}) = \chi_{k_2}(\varphi_{k_2})^{\alpha} = \sharp(k_2)^{\alpha} = p^{\alpha[k_2:\mathbb{F}_p]},$$

the desired commutativity is thus equivalent to the equality $\alpha[k_2:\mathbb{F}_p]=[k_1:\mathbb{F}_p]$ in $\hat{\mathbb{Z}}$. (The homomorphism $\hat{\mathbb{Z}}\to(\hat{\mathbb{Z}}^{p'})^\times$, $\beta\mapsto p^\beta$ is injective by [Chevalley 1951, théorème 1].) In particular, it suffices to prove the desired commutativity on an open subgroup $H\subset G_{k_1}$. Indeed, set $m\overset{\text{def}}{=}[G_{k_1}:H]$. Then, since $\varphi_{k_1}^m$ is the Frobenius element for H, the commutativity on H is equivalent to the equality $m\alpha[k_2:\mathbb{F}_p]=m[k_1:\mathbb{F}_p]$ in $\hat{\mathbb{Z}}$, which implies $\alpha[k_2:\mathbb{F}_p]=[k_1:\mathbb{F}_p]$, as desired. Thus, by replacing $\mathfrak{G}_1$ and $\mathfrak{G}_2$ by suitable open subgroups, we may and shall assume that $g_2>0$.

Next, for each prime number $l\neq p$ and $i\in\{1,2\}$, let $\chi_{k_i,l}:G_{k_i}\to\mathbb{Z}_l^\times$ denote the l-adic cyclotomic character. Thus, corresponding to the decomposition $(\hat{\mathbb{Z}}^{p'})^\times=\prod_{l\neq p}\mathbb{Z}_l^\times$, we have $\chi_{k_i}=(\chi_{k_i,l})_{l\neq p}$. We have to prove that $\chi_{k_2}\circ\sigma_0=\chi_{k_1}$, which is equivalent to saying that $\chi_{k_2,l}\circ\sigma_0=\chi_{k_1,l}$ for all $l\neq p$.

We shall first prove that the last equality holds up to torsion. More precisely, denote by $\bar{\chi}_{k_i,l}$ the composite of

$$G_{k_i}\overset{\chi_{k_i,l}}{\to}\mathbb{Z}_l^\times\twoheadrightarrow\mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{\mathrm{tor}}.$$

By Lemma 2.7, we can take $\tilde{x}_1\in\Sigma_{\tilde{X}_1,\sigma,l}\neq\varnothing$. Set $\tilde{x}_2\overset{\text{def}}{=}\tilde{\phi}(\tilde{x}_1)$. Let x_i denote the image of $\tilde{x}_i$ in Σ_{X_i} for $i=1,2$. By Proposition 2.2(ii), we have $\sigma:\mathfrak{D}_{\tilde{x}_1,l}\to\mathfrak{D}_{\tilde{x}_2,l}$ and $\sigma:\mathfrak{I}_{\tilde{x}_1,l}\to\mathfrak{I}_{\tilde{x}_2,l}$, which are injective by Proposition 1.1(i). This implies that $\chi_{k_2,l}\circ\sigma_0=\chi_{k_1,l}$ holds on the image of $\mathfrak{D}_{\tilde{x}_1,l}$ in G_{k_1}, which is an open subgroup of the l-Sylow subgroup $G_{k_1,l}$ of G_{k_1}. As $\mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{\mathrm{tor}}\simeq\mathbb{Z}_l$ is torsion-free and pro-l, this implies that $\bar{\chi}_{k_2,l}\circ\sigma_0=\bar{\chi}_{k_1,l}$.

In particular, we have $\bar{\chi}_{k_2,l}(\sigma_0(\varphi_{k_1}))=\bar{\chi}_{k_1,l}(\varphi_{k_1})$. This implies the equality $\sharp(k_2)^\alpha=\sharp(k_1)$ in $\mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{\mathrm{tor}}\simeq\mathbb{Z}_l$. Since $p\in\mathbb{Z}_l^\times$ is not torsion, this last equality shows that $\alpha_l[k_2:\mathbb{F}_p]=[k_1:\mathbb{F}_p]$ in $\mathbb{Z}_l$. Here, corresponding to the decomposition $\hat{\mathbb{Z}}=\prod_{l:\text{ prime}}\mathbb{Z}_l$, we write $\alpha=(\alpha_l)_{l:\text{ prime}}$. Or, equivalently, we have

$$\alpha[k_2:\mathbb{F}_p]=[k_1:\mathbb{F}_p]+\iota_p(\epsilon)$$

in $\hat{\mathbb{Z}}$, where $\iota_p:\mathbb{Z}_p\hookrightarrow\hat{\mathbb{Z}}$ is the natural injection and $\epsilon\overset{\text{def}}{=}\alpha_p[k_2:\mathbb{F}_p]-[k_1:\mathbb{F}_p]\in\mathbb{Z}_p$.

On the other hand, by Lemma 2.6, we get an open homomorphism $\pi_1(\overline{X}_1)^{p'}\to\pi_1(\overline{X}_2)^{p'}$, and hence a surjection $\pi_1(\overline{X}_1)^{p',\mathrm{ab}}\otimes_{\mathbb{Z}}\mathbb{Q}\twoheadrightarrow\pi_1(\overline{X}_2)^{p',\mathrm{ab}}\otimes_{\mathbb{Z}}\mathbb{Q}$, which is Galois-compatible with respect to

$$\sigma_0:G_{k_1}\to G_{k_2}.$$

For each $i=1,2$, let $P_i(T)$ be the characteristic polynomial of $\varphi_{k_i}^{[k_{i'}:\mathbb{F}_p]}$ on the free $\hat{\mathbb{Z}}^{p'}$-module $\pi_1(\overline{X}_i)^{p',\mathrm{ab}}$ (of rank $2g_i$), where i' is defined by $\{i,i'\}=\{1,2\}$. Then it is known that $P_i(T)\in\mathbb{Z}[T]$.

Write ρ_i for the natural representation $G_{k_i}\to\mathrm{Aut}_{\hat{\mathbb{Z}}^{p'}}(\pi_1(\overline{X}_i)^{p',\mathrm{ab}})$. Let $R_{\mathbb{Q}}$ be the (commutative) $\mathbb{Q}$-subalgebra of $\mathrm{End}_{\hat{\mathbb{Z}}^{p'}\otimes_{\mathbb{Z}}\mathbb{Q}}(\pi_1(\overline{X}_2)^{p',\mathrm{ab}}\otimes_{\mathbb{Z}}\mathbb{Q})$ generated by

$\rho_2(G_{k_2})$. We have

$$P_2(\rho_2(\varphi_{k_2}^{[k_1:\mathbb{F}_p]})) = 0$$

in $R_{\mathbb{Q}}$. By the Galois-compatibility, we also have

$$P_1(\rho_2(\sigma_0(\varphi_{k_1}^{[k_2:\mathbb{F}_p]}))) = 0$$

in $R_{\mathbb{Q}}$. These identities imply that both of $\rho_2(\varphi_{k_2}^{[k_1:\mathbb{F}_p]})$, $\rho_2(\sigma_0(\varphi_{k_2}^{[k_2:\mathbb{F}_p]})) \in R_{\mathbb{Q}}$ are algebraic over $\mathbb{Q}$, and hence so is the ratio

$$\rho_2(\sigma_0(\varphi_{k_1}^{[k_2:\mathbb{F}_p]})(\varphi_{k_2}^{[k_1:\mathbb{F}_p]})^{-1}) = \rho_2(\varphi_{k_2}^{\alpha[k_2:\mathbb{F}_p]-[k_1:\mathbb{F}_p]}) = \rho_2(\varphi_{k_2}^{\iota_p(\epsilon)}) \stackrel{\text{def}}{=} \eta$$

in $R_{\mathbb{Q}}$. So, take a monic polynomial $Q(T) \in \mathbb{Q}[T]$ satisfying $Q(\eta) = 0$ in $R_{\mathbb{Q}}$. Set $b \stackrel{\text{def}}{=} \deg(Q)$.

Let $l \neq p$ be a prime number, and let $R_{l,\mathbb{Q}}$ be the image of $R_{\mathbb{Q}}$ in

$$\mathrm{End}_{\mathbb{Q}_l}(\pi_1(\overline{X}_2)^{l,\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Q}).$$

Then observe that the image η_l of η in $R_{l,\mathbb{Q}} \subset \mathrm{End}_{\mathbb{Q}_l}(\pi_1(\overline{X}_2)^{l,\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Q})$ is a pro-p element of $\mathrm{End}_{\mathbb{Z}_l}(\pi_1(\overline{X}_2)^{l,\mathrm{ab}})^{\times}$, and hence a torsion element of p-power order. So, let p^{a_l} be the order of η_l. As $Q(\eta_l) = 0$ in the commutative $\mathbb{Q}$-algebra $R_{l,\mathbb{Q}}$, we conclude: $((p-1)/p)p^{a_l} \leq \varphi(p^{a_l}) \leq b$, where φ stands for Euler's function. (Use $\mathbb{Q} \hookrightarrow R_{l,\mathbb{Q}}$, which follows from $g_2 > 0$.) Thus, a_l is bounded: there exists $a \geq 0$ such that $a_l \leq a$ for all $l \neq p$. Namely, $(\eta_l)^{p^a} = 1$ for all $l \neq p$.

Set $\zeta_l \stackrel{\text{def}}{=} \det(\eta_l)$, where the determinant is taken as an element of

$$\mathrm{End}_{\mathbb{Q}_l}(\pi_1(\overline{X}_2)^{l,\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Q}).$$

Since det is a multiplicative homomorphism, we have $(\zeta_l)^{p^a} = 1$ for all $l \neq p$. Set $\zeta \stackrel{\text{def}}{=} (\zeta_l)_{l \neq p}$ in $(\hat{\mathbb{Z}}^{p'})^{\times} = \prod_{l \neq p} \mathbb{Z}_l^{\times}$. Now, by construction, we have

$$\zeta = \chi_{k_2}^{g_2}(\varphi_{k_2}^{\iota_p(\epsilon)}) = \sharp(k_2)^{g_2 \iota_p(\epsilon)},$$

and hence $\sharp(k_2)^{p^a g_2 \iota_p(\epsilon)} = 1$ in $(\hat{\mathbb{Z}}^{p'})^{\times}$. Since the homomorphism $\hat{\mathbb{Z}} \to (\hat{\mathbb{Z}}^{p'})^{\times}$, $\beta \mapsto p^{\beta}$ is injective, this last equality forces $[k_2 : \mathbb{F}_p]p^a g_2 \iota_p(\epsilon) = 0$ in $\hat{\mathbb{Z}}$. As $[k_2 : \mathbb{F}_p]p^a g_2 > 0$, this implies $\iota_p(\epsilon) = 0$. Namely, we have $\alpha[k_2 : \mathbb{F}_p] = [k_1 : \mathbb{F}_p]$ in $\hat{\mathbb{Z}}$, as desired.

(ii) As in the proof of (i), set $\sigma_0(\varphi_{k_1}) = \varphi_{k_2}^{\alpha}$. Since $G_{k_2} \simeq \hat{\mathbb{Z}}$ and $[G_{k_2} : \sigma_0(G_{k_1})] = d_0$, we must have $\alpha = d_0 u$, where $u \in \hat{\mathbb{Z}}^{\times}$. Now, since $\alpha[k_2 : \mathbb{F}_p] = [k_1 : \mathbb{F}_p]$ by (i), we get $d_0 u[k_2 : \mathbb{F}_p] = [k_1 : \mathbb{F}_p]$, and thus $u = [k_1 : \mathbb{F}_p]/(d_0[k_2 : \mathbb{F}_p]) \in \mathbb{Q}_{>0}$ $(\subset \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q})$. Since $\hat{\mathbb{Z}}^{\times} \cap \mathbb{Q}_{>0} = \{1\}$, we conclude $u = 1$. Thus, $d_0[k_2 : \mathbb{F}_p] = [k_1 : \mathbb{F}_p]$ and $\sigma_0(\varphi_{k_1}) = \varphi_{k_2}^{d_0}$, as desired. □

Lemma 2.9. *For each prime number $l \neq p$, the map $\tilde{\phi}_{\sigma,l} : \Sigma_{\tilde{X}_1,\sigma,l} \to \Sigma_{\tilde{X}_2}$ is surjective. In particular, the map $\phi_{\sigma,l} : \Sigma_{X_1,\sigma,l} \to \Sigma_{X_2}$ is surjective.*

Proof. As in the proof of Lemma 2.7, set

$$S \stackrel{\text{def}}{=} \Sigma_{X_2} \smallsetminus \phi(\Sigma_{X_1,\sigma,l}) \quad \text{and} \quad U_2 \stackrel{\text{def}}{=} X_2 \smallsetminus S.$$

By Lemma 2.7, S is a finite set. Let $r < \infty$ be the cardinality of $S(\bar{k}_2)$. Then σ induces an open homomorphism $\tau_1^{(l)} : \pi_1(X_1)^{(l)} \to \pi_1(U_2)^{(l)}$, which is a lifting of the homomorphism $\tau^{(l)} : \pi_1(X_1)^{(l)} \to \pi_1(X_2)^{(l)}$ induced by $\tau' : \pi_1(X_1)^{(p')} \to \pi_1(X_2)^{(p')}$ in Lemma 2.6. We have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(\overline{X}_1)^l & \twoheadrightarrow & \pi_1(X_1)^{(l)} & \stackrel{\text{pr}_1}{\twoheadrightarrow} & G_{k_1} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \bar{\tau}_1^l} & & \downarrow{\scriptstyle \tau_1^{(l)}} & & \downarrow{\scriptstyle \sigma_0} & & \\ 1 & \longrightarrow & \pi_1(\overline{U}_2)^l & \twoheadrightarrow & \pi_1(U_2)^{(l)} & \stackrel{\text{pr}_2}{\twoheadrightarrow} & G_{k_2} & \longrightarrow & 1, \end{array}$$

where $\overline{U}_2 \stackrel{\text{def}}{=} U_2 \times_{k_2} \bar{k}_2$. Since $\tau_1^{(l)} : \pi_1(X_1)^{(l)} \to \pi_1(U_2)^{(l)}$ is open and $\sigma_0 : G_{k_1} \to G_{k_2}$ is (open and) injective, we see that $\bar{\tau}_1^l : \pi_1(\overline{X}_1)^l \to \pi_1(\overline{U}_2)^l$ is open. The open homomorphism $\bar{\tau}_1^l : \pi_1(\overline{X}_1)^l \to \pi_1(\overline{U}_2)^l$ induces an open homomorphism $\bar{\tau}_1^{l,\text{ab}} : \pi_1(\overline{X}_1)^{l,\text{ab}} \to \pi_1(\overline{U}_2)^{l,\text{ab}}$. This last homomorphism is, by construction, Galois-compatible with respect to $\sigma_0 : G_{k_1} \to G_{k_2}$. In other words, if we regard $\pi_1(\overline{U}_2)^{l,\text{ab}}$ as a G_{k_1}-module via σ_0, then $\bar{\tau}_1^{l,\text{ab}}$ is a homomorphism as G_{k_1}-modules.

The absolute values of eigenvalues of $\varphi_{k_1} \in G_{k_1}$ in $\pi_1(\overline{X}_1)^{l,\text{ab}}$ are all $\sharp(k_1)^{1/2}$, with multiplicity $2g_1$. On the other hand, by Lemma 2.8(ii), the absolute values of eigenvalues of φ_{k_1} in $\pi_1(\overline{U}_2)^{l,\text{ab}}$ are the same as those of $\varphi_{k_2}^{d_0}$, which are $\sharp(k_2)^{d_0/2}$ with multiplicity $2g_2$ and $\sharp(k_2)^{d_0}$ with multiplicity $\max(r-1, 0)$. By Lemma 2.8(i), they coincide with $\sharp(k_1)^{1/2}$ and $\sharp(k_1)$, respectively. Thus, we conclude $r \leq 1$. However, if $r \neq 0$, by replacing $\mathfrak{G}_1, \mathfrak{G}_2$ with suitable open subgroups, we may assume that $r > 1$, a contradiction. So, we have established $r = 0$.

To prove the surjectivity of $\tilde{\phi}_{\sigma,l}$, we may freely replace $\mathfrak{G}_1, \mathfrak{G}_2$ by open subgroups $\mathfrak{H}_1, \mathfrak{H}_2$, respectively, such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$. (Indeed, the map

$$\tilde{\phi}_{\sigma,l} : \Sigma_{\tilde{X}_1,\sigma,l} \to \Sigma_{\tilde{X}_2}$$

remains unchanged.) In particular, we may assume that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is surjective. Then the surjectivity of $\tilde{\phi}_{\sigma,l} : \Sigma_{\tilde{X}_1,\sigma,l} \to \Sigma_{\tilde{X}_2}$ is equivalent to the surjectivity of $\phi_{\sigma,l} : \Sigma_{X_1,\sigma,l} \to \Sigma_{X_2}$, which is then equivalent to $r = 0$. □

3. Rigid homomorphisms between Galois groups

In this section we investigate a class of homomorphisms between (geometrically prime-to-characteristic quotients of) absolute Galois groups of function fields of curves over finite fields, which we call rigid. We follow the notations in Sections 1 and 2. In particular, we follow the Notation at the beginning of subsection 2B. We assume that Condition 3 holds.

Definition 3.1 (rigid homomorphisms). (i) We say that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid if there exists a map

$$\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2},$$

such that

$$\sigma(\mathfrak{D}_{\tilde{x}_1}) = \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$$

for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$.

(ii) We say that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is rigid if there exist open subgroups $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$, such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$ and that $\mathfrak{H}_1 \overset{\sigma}{\to} \mathfrak{H}_2$ is strictly rigid. (Here, $\mathfrak{H}_i$ is considered as a quotient of the absolute Galois group that is the inverse image in G_i of $\mathfrak{H}_i \subset \mathfrak{G}_i$.)

(iii) Define $\mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{rig}} \subset \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)$ to be the set of rigid (and hence continuous and open) homomorphisms $\mathfrak{G}_1 \to \mathfrak{G}_2$.

Remark 3.2. (i) Consider a commutative diagram of maps between profinite groups

$$\begin{array}{ccc} \mathfrak{G}_1 & \overset{\sigma}{\longrightarrow} & \mathfrak{G}_2 \\ \downarrow & & \downarrow \\ \mathfrak{G}'_1 & \overset{\sigma'}{\longrightarrow} & \mathfrak{G}'_2, \end{array}$$

where the vertical arrows are surjective. Then if $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid (resp. rigid), $\sigma' : \mathfrak{G}'_1 \to \mathfrak{G}'_2$ is strictly rigid (resp. rigid).

(ii) Let $\mathfrak{H}_2$ be an open subgroup of $\mathfrak{G}_2$ and $\mathfrak{H}_1 \overset{\mathrm{def}}{=} \sigma^{-1}(\mathfrak{H}_2)$. Then if $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid (resp. rigid), the natural homomorphism $\mathfrak{H}_1 \to \mathfrak{H}_2$ induced by σ is strictly rigid (resp. rigid).

(iii) Assume that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid with respect to $\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$. Then if $\tilde{\phi}$ is surjective, σ is surjective. Indeed, this follows immediately from the fact, by Chebotarev's density theorem, that $\mathfrak{G}_2$ is (topologically) generated by its decomposition subgroups.

(iv) As in Proposition 2.2, let $l \neq p_1, p_2$ be a prime number, and assume that (1) $N_2^l = N_2$, or, equivalently, $\tilde{K}_2$ admits no l-cyclic extension; and (2) $\tilde{K}_2$ contains a primitive l-th roots of unity.

If σ is strictly rigid with respect to $\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$, then we must have $\Sigma_{\tilde{X}_1,\sigma,l} = \Sigma_{\tilde{X}_1}$ and $\tilde{\phi} = \tilde{\phi}_{\sigma,l}$. In particular, then $\tilde{\phi}$ is unique and Galois-equivariant with respect to σ, and hence naturally induces a map $\phi\ (= \phi_{\sigma,l}) : \Sigma_{X_1} \to \Sigma_{X_2}$.

If σ is rigid, then we must have $\Sigma_{\tilde{X}_1,\sigma,l} = \Sigma_{\tilde{X}_1}$, and, if we set $\tilde{\phi} \overset{\mathrm{def}}{=} \tilde{\phi}_{\sigma,l}$, then

$$\sigma(\mathfrak{D}_{\tilde{x}_1}) \underset{\text{open}}{\subset} \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$$

for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$. The map $\tilde{\phi}$ is uniquely characterized by this property, and Galois-equivariant with respect to σ, and hence naturally induces a map

$$\phi\ (=\phi_{\sigma,l}) : \Sigma_{X_1} \to \Sigma_{X_2}.$$

In the rest of this section, we assume that Condition 1 holds.

Definition 3.3. (i) Let $\gamma : K_2 \to K_1$ be a homomorphism of fields defining an extension K_1/K_2 of fields. Set $p \overset{\text{def}}{=} p_1 = p_2$. Then we say that γ is admissible if the extension K_1/K_2 appears in the extensions of K_2 corresponding to the open subgroups of $\mathfrak{G}_2$. More precisely, in the profinite case, we say that γ is admissible if the extension K_1/K_2 is finite separable; in the prime-to-characteristic case, we say that γ is admissible if the extension K_1/K_2 is finite separable and the Galois closure of the extension $K_1\bar{k}_1/K_2\bar{k}_2$ is of degree prime to p.

Equivalently, $\gamma : K_2 \to K_1$ is admissible if and only if it extends to an isomorphism $\tilde{\gamma} : \tilde{K}_2 \xrightarrow{\sim} \tilde{K}_1$.

(ii) Define $\mathrm{Hom}(K_2, K_1)^{\mathrm{adm}} \subset \mathrm{Hom}(K_2, K_1)$ to be the set of admissible homomorphisms $K_2 \to K_1$.

Our aim in this section is to prove the following.

Theorem 3.4. *The natural map* $\mathrm{Hom}(K_2, K_1) \to \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)/\mathrm{Inn}(\mathfrak{G}_2)$ *induces a bijection*

$$\mathrm{Hom}(K_2, K_1)^{\mathrm{adm}} \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{rig}}/\mathrm{Inn}(\mathfrak{G}_2).$$

More precisely,

(i) *If $\gamma : K_2 \to K_1$ is an admissible homomorphism between fields, then the homomorphism $\mathfrak{G}_1 \to \mathfrak{G}_2$ induced by γ (up to inner automorphisms) is rigid.*

(ii) *If $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is a rigid homomorphism between profinite groups, then there exists a unique isomorphism $\tilde{\gamma} : \tilde{K}_2 \to \tilde{K}_1$ of fields, such that $\tilde{\gamma} \circ \sigma(g_1) = g_1 \circ \tilde{\gamma}$ for all $g_1 \in \mathfrak{G}_1$, which induces an admissible homomorphism $K_2 \to K_1$.*

Remark 3.5. (i) By local theory for the Isom-form, any isomorphism $\mathfrak{G}_1 \xrightarrow{\sim} \mathfrak{G}_2$ is strictly rigid. In particular, we have $\mathrm{Isom}(\mathfrak{G}_1, \mathfrak{G}_2) \subset \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{rig}}$. Thus, Theorem 3.4 can be viewed as a generalization of the Isom-form:

$$\mathrm{Isom}(K_2, K_1) \xrightarrow{\sim} \mathrm{Isom}(\mathfrak{G}_1, \mathfrak{G}_2)/\mathrm{Inn}(\mathfrak{G}_2),$$

which is the main theorem of [Uchida 1977] in the profinite case, and the main theorem of [Saïdi and Tamagawa 2009] in the prime-to-characteristic case.

(ii) Let

$$\gamma : K_2^{\mathrm{perf}} \to K_1^{\mathrm{perf}}$$

be a homomorphism of fields defining an extension $K_1^{\mathrm{perf}}/K_2^{\mathrm{perf}}$ of fields. Set $p \overset{\text{def}}{=} p_1 = p_2$. We say that γ is admissible if the extension $K_1^{\mathrm{perf}}/K_2^{\mathrm{perf}}$ appears

in the extensions of K_2^{perf} corresponding to the open subgroups of $\mathfrak{G}_2$, which is regarded as a quotient of the absolute Galois group $G_{K_2^{\mathrm{perf}}} = G_{K_2}$. More precisely, in the profinite case γ is always admissible, and in the prime-to-characteristic case γ is admissible if and only if the extension the Galois closure of the extension $K_1^{\mathrm{perf}}\overline{k}_1/K_2^{\mathrm{perf}}\overline{k}_2$ is of degree prime to p. Define

$$\mathrm{Hom}\left(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}}\right)^{\mathrm{adm}} \subset \mathrm{Hom}\left(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}}\right)$$

to be the set of admissible homomorphisms $K_2^{\mathrm{perf}} \to K_1^{\mathrm{perf}}$. Then the natural map $\mathrm{Hom}\left(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}}\right) \to \mathrm{Hom}\left(\mathfrak{G}_1, \mathfrak{G}_2\right)/\mathrm{Inn}(\mathfrak{G}_2)$ induces a bijection

$$\mathrm{Hom}\left(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}}\right)^{\mathrm{adm}}/\mathrm{Frob}^{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Hom}\left(\mathfrak{G}_1, \mathfrak{G}_2\right)^{\mathrm{rig}}/\mathrm{Inn}(\mathfrak{G}_2).$$

Indeed, this follows from Theorem 3.4, since the natural map $\mathrm{Hom}(K_2, K_1) \to \mathrm{Hom}\left(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}}\right)$ induces

$$\mathrm{Hom}(K_2, K_1)^{\mathrm{adm}} \xrightarrow{\sim} \mathrm{Hom}\left(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}}\right)^{\mathrm{adm}}/\mathrm{Frob}^{\mathbb{Z}}.$$

The rest of this section is devoted to the proof of Theorem 3.4.

First, to prove 3.4(i), let $\gamma : K_2 \to K_1$ be an admissible homomorphism. Then, by the definition of admissibility, the extension K_1/K_2 is isomorphic to some extension L/K_2 that corresponds to an open subgroup $\mathfrak{H}_2$ of $\mathfrak{G}_2$. Set $\mathfrak{H}_1 \overset{\mathrm{def}}{=} \mathfrak{G}_1$. Now let $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ be the homomorphism induced by γ (up to conjugacy). Then it is easy to see that σ restricts to an isomorphism $\mathfrak{H}_1 \xrightarrow{\sim} \mathfrak{H}_2$ (corresponding to the isomorphism $L \xrightarrow{\sim} K_1$), which is strictly rigid. Thus, σ is rigid, as desired.

Next, to prove 3.4(ii), let $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ be a rigid homomorphism. By definition, there exist open subgroups $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$, such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$ and that $\mathfrak{H}_1 \xrightarrow{\sigma} \mathfrak{H}_2$ is strictly rigid with respect to, say, $\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$. Then, by Remark 3.2(iv), $\tilde{\phi}$ is Galois-equivariant with respect to $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ (that is, not only with respect to $\sigma : \mathfrak{H}_1 \to \mathfrak{H}_2$), and, for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$, we have $\sigma(\mathfrak{D}_{\tilde{x}_1}) \underset{\mathrm{open}}{\subset} \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$ and $\sigma(\mathfrak{D}_{\tilde{x}_1} \cap \mathfrak{H}_1) = \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)} \cap \mathfrak{H}_2$.

Lemma 3.6. *Condition 2 holds for* $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$.

Proof. By Proposition 2.1(v), we have $\sigma(\mathfrak{I}_{\tilde{x}_1}) \subset \mathfrak{I}_{\tilde{\phi}(\tilde{x}_1)}$ for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$. In particular, we have $\sigma(\mathfrak{I}_1) \subset \mathfrak{I}_2$. Now, the assertion follows from Lemma 2.3. □

Thus, we may apply Lemmas 2.6–2.9 to σ.

Lemma 3.7. *We have* $\sigma(\mathfrak{H}_1) = \mathfrak{H}_2$ *and* $\mathfrak{H}_1 = \sigma^{-1}(\mathfrak{H}_2)$.

Proof. By Lemma 2.9, $\tilde{\phi}$ is surjective, and hence, by Remark 3.2(iii), $\sigma : \mathfrak{H}_1 \to \mathfrak{H}_2$ is surjective, that is, $\sigma(\mathfrak{H}_1) = \mathfrak{H}_2$.

Next, let $X_{1,\mathfrak{H}_1} \to X_{1,\sigma^{-1}(\mathfrak{H}_2)} \to X_1$ and $X_{2,\mathfrak{H}_2} \to X_2$ be (finite, generically étale) covers corresponding to open subgroups $\mathfrak{H}_1 \subset \sigma^{-1}(\mathfrak{H}_2) \subset \mathfrak{G}_1$ and $\mathfrak{H}_2 \subset \mathfrak{G}_2$,

respectively. Suppose that $\mathfrak{H}_1 \subsetneq \sigma^{-1}(\mathfrak{H}_2)$. Then, by Chebotarev's density theorem, there exists $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$ such that

$$k(x_{1,\mathfrak{H}_1}) \supsetneq k(x_{1,\sigma^{-1}(\mathfrak{H}_2)}),$$

where $x_{1,\mathfrak{H}_1}$ and $x_{1,\sigma^{-1}(\mathfrak{H}_2)}$ denote the images of $\tilde{x}_1$ in $\Sigma_{1,\mathfrak{H}_1}$ and $\Sigma_{1,\sigma^{-1}(\mathfrak{H}_2)}$, respectively. Set $\tilde{x}_2 \overset{\text{def}}{=} \tilde{\phi}(\tilde{x}_1) \in \Sigma_{\tilde{X}_2}$. We have $\sigma(\mathfrak{D}_{\tilde{x}_1}) \subset \mathfrak{D}_{\tilde{x}_2}$, and hence

$$\sigma(\mathfrak{D}_{\tilde{x}_1} \cap \mathfrak{H}_1) \subset \sigma(\mathfrak{D}_{\tilde{x}_1} \cap \sigma^{-1}(\mathfrak{H}_2)) \subset \mathfrak{D}_{\tilde{x}_2} \cap \mathfrak{H}_2.$$

Now, since $\mathfrak{H}_1 \overset{\sigma}{\to} \mathfrak{H}_2$ is strictly rigid, we must have

$$\sigma(\mathfrak{D}_{\tilde{x}_1} \cap \mathfrak{H}_1) = \sigma(\mathfrak{D}_{\tilde{x}_1} \cap \sigma^{-1}(\mathfrak{H}_2)) = \mathfrak{D}_{\tilde{x}_2} \cap \mathfrak{H}_2.$$

By Proposition 2.1(iii), this implies that $\sharp(k(x_{1,\mathfrak{H}_1})) = \sharp(k(x_{2,\mathfrak{H}_2})) = \sharp(k(x_{1,\sigma^{-1}(\mathfrak{H}_2)})$, where $x_{2,\mathfrak{H}_2}$ denotes the image of $\tilde{x}_2$ in $\Sigma_{X_{2,\mathfrak{H}_2}}$. This contradicts

$$k(x_{1,\mathfrak{H}_1}) \supsetneq k(x_{1,\sigma^{-1}(\mathfrak{H}_2)}). \qquad \square$$

We treat the special case where $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid (and hence, in particular, surjective).

Lemma 3.8. *Assume that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid.*

(i) *We have $g_1 = g_2$.*

(ii) *The map $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$ is bijective.*

Proof. By Lemma 2.6, the homomorphism σ naturally induces a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(\overline{X}_1)^{p',\mathrm{ab}} & \longrightarrow & \Pi_1 & \longrightarrow & G_{k_1} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \pi_1(\overline{X}_2)^{p',\mathrm{ab}} & \longrightarrow & \Pi_2 & \longrightarrow & G_{k_2} & \longrightarrow & 1, \end{array}$$

where Π_i is the quotient $\pi_1(X_i)^{(p')}/\operatorname{Ker}(\pi_1(\overline{X}_i)^{p'} \twoheadrightarrow \pi_1(\overline{X}_i)^{p',\mathrm{ab}})$, and the maps $\Pi_i \to G_{k_i}$ are the natural projections; $i = 1, 2$. The vertical maps are surjective. In particular, the representation $G_{k_1} \to G_{k_2} \to \mathrm{Aut}(\pi_1(\overline{X}_2)^{p',\mathrm{ab}})$, where $G_{k_2} \to \mathrm{Aut}(\pi_1(\overline{X}_2)^{p',\mathrm{ab}})$ is the natural representation and $G_{k_1} \to G_{k_2}$ is the right vertical map in the above diagram, is a quotient representation of the natural representation $G_{k_1} \to \mathrm{Aut}(\pi_1(\overline{X}_1)^{p',\mathrm{ab}})$. For $i \in \{1, 2\}$, let E_i be the set of eigenvalues, counted with multiplicities, of the Frobenius element φ_{k_i} acting on $\pi_1(\overline{X}_i)^{p',\mathrm{ab}}$. Then $E_2 \subset E_1$, since the map $G_{k_1} \to G_{k_2}$ maps φ_{k_1} to φ_{k_2} (see Lemma 2.8(ii)). We will show that $E_1 = E_2$.

For an integer $n \geq 1$, let $k_{i,n}$ be the unique extension of k_i of degree n; $i = 1, 2$. Then, by the Lefschetz trace formula, $\sharp X_i(k_{i,n}) = 1 - \sum_{\alpha_i \in E_i} \alpha_i^n + q^n$, where $q \overset{\text{def}}{=} \sharp(k_i)$ (see Lemma 2.8(ii) for the equality $\sharp(k_1) = \sharp(k_2)$). Recall that the

map $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$ is surjective (see Lemma 2.9), and if $x_2 = \phi(x_1)$, then the residue fields $k(x_1)$ and $k(x_2)$ have the same cardinality (see Proposition 2.1(iii)). In particular, $\sharp(X_1(k_{1,n})) \geq \sharp(X_2(k_{2,n}))$ for all n. Thus, $\sum_{j=1}^{r} \beta_j^n \leq 0$ for any $n \geq 1$, where

$$E \stackrel{\text{def}}{=} E_1 \smallsetminus E_2 \stackrel{\text{def}}{=} \{\beta_1, \ldots, \beta_r\}$$

($r = 2g_1 - 2g_2 \geq 0$). Write $\beta_j = \rho_j e^{i\theta_j}$ ($\rho_j \in \mathbb{R}_{>0}$, $\theta_j \in [0, 2\pi)$), for $j \in \{1, \ldots, r\}$ (note that $\rho_j = q^{1/2}$ by the Riemann hypothesis for curves). Let $\mathcal{T}$ be the set consisting of the 4 quadrants of $\mathbb{C} = \mathbb{R}^2$. More precisely, $\mathcal{T} = \{T_k \mid k \in \{1, 2, 3, 4\}\}$, where

$$T_k \stackrel{\text{def}}{=} \left\{ \rho e^{i\theta} \;\middle|\; \rho \in \mathbb{R}_{>0}, \theta \in \left[\frac{(k-1)\pi}{2}, \frac{k\pi}{2} \right) \right\}.$$

Thus, each $\alpha \in \mathbb{C}^\times$ belongs to a unique element of $\mathcal{T}$, which we shall denote by $T(\alpha)$. Consider the map $\mu : \mathbb{N} \to \mathcal{T}^r$ that maps an integer n to $\{T(\beta_j^n)\}_{j=1}^r$. Then there must exist integers $m_1 < m_2$ such that $\mu(m_1) = \mu(m_2)$, since $\sharp(\mathcal{T}^r) = 4^r$ is finite. This implies that $e^{im_1\theta_j}$ and $e^{im_2\theta_j}$ belong to the same quadrant of $\mathbb{C} = \mathbb{R}^2$ for all $j \in \{1, \ldots, r\}$. In particular, $\mathrm{Re}(\beta_j^n) = \rho_j^n \cos n\theta_j > 0$, where $n \stackrel{\text{def}}{=} m_2 - m_1 \geq 1$. Suppose that $r > 0$; then this implies that

$$\mathrm{Re}\Big(\sum_{j=1}^{r} \beta_j^n \Big) = \sum_{j=1}^{r} \mathrm{Re}\, \beta_j^n > 0,$$

which contradicts the above fact that $\sum_{j=1}^{r} \beta_j^n \leq 0$, for all n. Thus, $r = 0$, that is, $E = E_1 \smallsetminus E_2$ must be empty, and $E_1 = E_2$.

In particular, the $\hat{\mathbb{Z}}^{p'}$-ranks of $\pi_1(\overline{X}_i)^{p',\mathrm{ab}}$, which equal $2g_i$, are equal; $i = 1, 2$. This completes the proof of Lemma 3.8(i).

Finally, we can conclude that ϕ is injective. For otherwise, there would exist an integer $n \geq 1$ such that $\sharp(X_1(k_n)) > \sharp(X_2(k_n))$, and hence, $E \neq \varnothing$, which is a contradiction. This completes the proof of Lemma 3.8(ii). □

Lemma 3.9. *Assume that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid. Then $\sigma^{(p')} : \mathfrak{G}_1^{(p')} \to \mathfrak{G}_2^{(p')}$ is an isomorphism.* (*In particular, in the prime-to-characteristic case, σ is an isomorphism.*)

Proof. By Lemma 3.8(ii), the map $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$ induced by σ is bijective. For a finite subset S_2 of Σ_{X_2}, let $S_1 \stackrel{\text{def}}{=} \phi^{-1}(S_2)$. Then σ naturally induces a continuous, surjective homomorphism $\tau'_{S_1,S_2} : \pi_1(U_1)^{(p')} \twoheadrightarrow \pi_1(U_2)^{(p')}$, where $\pi_1(U_i)^{(p')}$ is the maximal geometrically prime-to-p quotient of the fundamental group $\pi_1(U_i)$ of $U_i \stackrel{\text{def}}{=} X_i - S_i$; $i = 1, 2$. Further, we have the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \pi_1(\overline{U}_1)^{p'} & \twoheadrightarrow & \pi_1(U_1)^{(p')} & \longrightarrow & G_{k_1} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \tau'_{S_1,S_2}} & & \downarrow & & \\
1 & \longrightarrow & \pi_1(\overline{U}_2)^{p'} & \twoheadrightarrow & \pi_1(U_2)^{(p')} & \longrightarrow & G_{k_2} & \longrightarrow & 1.
\end{array}$$

The surjective homomorphism $\pi_1(\overline{U}_1)^{p'} \twoheadrightarrow \pi_1(\overline{U}_2)^{p'}$ must be an isomorphism by [Fried and Jarden 1986, Proposition 15.4], since $X_i - S_i$ have the same topological type $(g_i, \sharp(\bar{S}_i))$, where $\overline{S}_i$ denotes the inverse image of S_i in $\Sigma_{\overline{X}_i}$; $i = 1, 2$, by Lemma 3.8. (For the bijectivity $\bar{S}_1 \xrightarrow{\sim} \bar{S}_2$, apply Lemma 3.8(ii) to various open subgroups of $\mathfrak{G}_1, \mathfrak{G}_2$ corresponding to constant field extensions.) Thus, the map τ'_{S_1,S_2} is an isomorphism (note that the surjective map $G_{k_1} \to G_{k_2}$ is an isomorphism). Also,

$$\mathfrak{G}_i^{(p')} = \varprojlim_{S_i} \pi_1(X_i - S_i)^{(p')},$$

where the projective limit is taken over all finite subsets S_i of Σ_{X_i}; $i = 1, 2$. Further,

$$\sigma^{(p')} = \varprojlim_{\{S_1,S_2\}} \tau'_{S_1,S_2},$$

where the projective limit is taken over all finite subsets S_1 and S_2 corresponding to each other via ϕ. Thus, $\sigma^{(p')}$ must be an isomorphism. □

Now, return to the general case. As above, let $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ be open subgroups such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$ and the map $\sigma_{\mathfrak{H}_1,\mathfrak{H}_2} : \mathfrak{H}_1 \to \mathfrak{H}_2$ obtained by restricting $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid with respect to $\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$. By Remark 3.2(iv), $\tilde{\phi}$ is Galois-equivariant with respect to $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ (that is, not only with respect to $\sigma_{\mathfrak{H}_1,\mathfrak{H}_2} : \mathfrak{H}_1 \to \mathfrak{H}_2$), and, for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$, we have

$$\sigma(\mathfrak{D}_{\tilde{x}_1}) \underset{\text{open}}{\subset} \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}, \quad \sigma(\mathfrak{D}_{\tilde{x}_1} \cap \mathfrak{H}_1) = \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)} \cap \mathfrak{H}_2.$$

Moreover, by Lemma 3.9, the map $(\sigma_{\mathfrak{H}_1,\mathfrak{H}_2})^{(p')} : \mathfrak{H}_1^{(p')} \to \mathfrak{H}_2^{(p')}$ induced by $\sigma_{\mathfrak{H}_1,\mathfrak{H}_2}$ is an isomorphism.

Now, let us denote the finite separable extension of K_i corresponding to $\mathfrak{H}_i \subset \mathfrak{G}_i$ by $K_{i,\mathfrak{H}_i}$, and the (infinite) Galois extension of $K_{i,\mathfrak{H}_i}$ corresponding to $\mathfrak{H}_i \twoheadrightarrow \mathfrak{H}_i^{(p')}$ by $\tilde{K}_{i,\mathfrak{H}_i}^{(p')}$. By applying the Isom-form proved in [Saïdi and Tamagawa 2009], we see that

$$(\sigma_{\mathfrak{H}_1,\mathfrak{H}_2})^{(p')} : \mathfrak{H}_1^{(p')} \xrightarrow{\sim} \mathfrak{H}_2^{(p')}$$

arises from a unique field isomorphism $\gamma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2}^{(p')} \xrightarrow{\sim} \tilde{K}_{1,\mathfrak{H}_1}^{(p')}$ that induces an isomorphism $K_{2,\mathfrak{H}_2} \xrightarrow{\sim} K_{1,\mathfrak{H}_1}$.

Lemma 3.10. *Let $\mathfrak{H}'_i \subset \mathfrak{H}_i$, $i = 1, 2$ be open subgroups, such that $\sigma(\mathfrak{H}'_1) \subset \mathfrak{H}'_2$ and that $\sigma_{\mathfrak{H}'_1,\mathfrak{H}'_2} : \mathfrak{H}'_1 \to \mathfrak{H}'_2$ is strictly rigid. Then the field isomorphism*

$$\gamma_{(\mathfrak{H}'_1)^{(p')},(\mathfrak{H}'_2)^{(p')}} : \tilde{K}_{2,\mathfrak{H}'_2}^{(p')} \xrightarrow{\sim} \tilde{K}_{1,\mathfrak{H}'_1}^{(p')}$$

restricts to $\gamma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2}^{(p')} \xrightarrow{\sim} \tilde{K}_{1,\mathfrak{H}_1}^{(p')}$.

Proof. This follows formally from the statement of the Isom-form proved in [Saïdi and Tamagawa 2009], as follows, without recalling any construction in that paper.

Take an open subgroup $\mathfrak{H}_2''$ of $\mathfrak{H}_2'$ that is normal in $\mathfrak{H}_2$. Then, by Lemma 3.7,

$$\mathfrak{H}_1'' \overset{\text{def}}{=} \sigma^{-1}(\mathfrak{H}_2'') \subset \sigma^{-1}(\mathfrak{H}_2') = \mathfrak{H}_1',$$

and hence, by Remark 3.2(ii), $\mathfrak{H}_1'' \overset{\sigma}{\to} \mathfrak{H}_2''$ is strictly rigid. Assume that

$$\gamma_{(\mathfrak{H}_1'')^{(p')},(\mathfrak{H}_2'')^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2''}^{(p')} \overset{\sim}{\to} \tilde{K}_{1,\mathfrak{H}_1''}^{(p')}$$

restricts to $\gamma_{(\mathfrak{H}_1')^{(p')},(\mathfrak{H}_2')^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2'}^{(p')} \overset{\sim}{\to} \tilde{K}_{1,\mathfrak{H}_1'}^{(p')}$ and to $\gamma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2}^{(p')} \overset{\sim}{\to} \tilde{K}_{1,\mathfrak{H}_1}^{(p')}$. Then

$$\gamma_{(\mathfrak{H}_1')^{(p')},(\mathfrak{H}_2')^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2'}^{(p')} \overset{\sim}{\to} \tilde{K}_{1,\mathfrak{H}_1'}^{(p')}$$

restricts to

$$\gamma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2}^{(p')} \overset{\sim}{\to} \tilde{K}_{1,\mathfrak{H}_1}^{(p')},$$

as desired. So, it suffices to prove the desired property in the case where $\mathfrak{H}_i' \subset \mathfrak{H}_i$ is normal for $i = 1, 2$, and σ naturally induces an isomorphism $\mathfrak{H}_1/\mathfrak{H}_1' \overset{\sim}{\to} \mathfrak{H}_2/\mathfrak{H}_2'$ between finite groups.

For $i = 1, 2$, let $\mathfrak{J}_i'$ be the image of $\mathfrak{H}_i'$ in $\mathfrak{H}_i^{(p')}$, which is an open normal subgroup of $\mathfrak{H}_i^{(p')}$. Let $\mathfrak{J}_i \subset \mathfrak{H}_i$ be the inverse image of $\mathfrak{J}_i'$ in $\mathfrak{H}_i$. Thus, we have the natural identification $\mathfrak{J}_i^{(p')} = \mathfrak{J}_i'$ and the commutative diagram

$$\begin{array}{ccccccc}
\mathfrak{H}_i' & \subset & \mathfrak{J}_i & \subset & \mathfrak{H}_i & \subset & \mathfrak{G}_i \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
(\mathfrak{H}_i')^{(p')} & \twoheadrightarrow & \mathfrak{J}_i^{(p')} & \hookrightarrow & \mathfrak{H}_i^{(p')} & \to & \mathfrak{G}_i^{(p')},
\end{array}$$

in which the vertical arrows are natural surjective maps.

Since the isomorphism $(\sigma_{\mathfrak{H}_1',\mathfrak{H}_2'})^{(p')} : (\mathfrak{H}_1')^{(p')} \overset{\sim}{\to} (\mathfrak{H}_2')^{(p')}$ is compatible with the natural (conjugate) actions of $\mathfrak{H}_1$ and $\mathfrak{H}_2$ with respect to $\mathfrak{H}_1 \overset{\sigma}{\twoheadrightarrow} \mathfrak{H}_2$, the corresponding field isomorphism

$$\gamma_{(\mathfrak{H}_1')^{(p')},(\mathfrak{H}_2')^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2'}^{(p')} \overset{\sim}{\to} \tilde{K}_{1,\mathfrak{H}_1'}^{(p')}$$

is also compatible with the natural actions of $\mathfrak{H}_1$ and $\mathfrak{H}_2$ with respect to $\mathfrak{H}_1 \overset{\sigma}{\twoheadrightarrow} \mathfrak{H}_2$. In particular, $\gamma_{(\mathfrak{H}_1')^{(p')},(\mathfrak{H}_2')^{(p')}}$ restricts to $K_{2,\mathfrak{H}_2} \overset{\sim}{\to} K_{1,\mathfrak{H}_1}$, and hence induces an isomorphism

$$\alpha : K_{2,\mathfrak{H}_2}^{(p')} \overset{\sim}{\to} K_{1,\mathfrak{H}_1}^{(p')}$$

that is compatible with $\sigma : \mathfrak{H}_1 \twoheadrightarrow \mathfrak{H}_2$, and hence with $\sigma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \mathfrak{H}_1^{(p')} \overset{\sim}{\to} \mathfrak{H}_2^{(p')}$. On the other hand, the isomorphism

$$\gamma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2}^{(p')} \overset{\sim}{\to} \tilde{K}_{1,\mathfrak{H}_1}^{(p')}$$

is also compatible with

$$\sigma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \mathfrak{H}_1^{(p')} \xrightarrow{\sim} \mathfrak{H}_2^{(p')}.$$

Thus, we conclude that, as desired,

$$\alpha = \sigma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}},$$

by the uniqueness of such a Galois-compatible isomorphism. (This is included in the statement of the Isom-form proved in [Saïdi and Tamagawa 2009].) □

Now, consider the set $\mathcal{S}$ ($\subset \mathrm{Sub}(\mathfrak{G}_1) \times \mathrm{Sub}(\mathfrak{G}_2)$) of all pairs of open subgroups $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$, that $\mathfrak{H}_1 \xrightarrow{\sigma} \mathfrak{H}_2$ is strictly rigid, and that $\mathfrak{H}_2$ is normal in $\mathfrak{G}_2$. Then, as in the proof of Lemma 3.10, it follows from Lemma 3.7 and Remark 3.2(ii) that $(\mathfrak{H}_1, \mathfrak{H}_2) \in \mathcal{S}$ implies that $\sigma(\mathfrak{H}_1) = \mathfrak{H}_2$, that $\mathfrak{H}_1 = \sigma^{-1}(\mathfrak{H}_2)$, and that the image of $\mathcal{S}$ in $\mathrm{Sub}(\mathfrak{G}_2)$ is cofinal in the set of open subgroups of $\mathfrak{G}_2$.

For each pair $(\mathfrak{H}_1, \mathfrak{H}_2) \in \mathcal{S}$, we get an isomorphism

$$\sigma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \mathfrak{H}_1^{(p')} \xrightarrow{\sim} \mathfrak{H}_2^{(p')}$$

by Lemma 3.9, which is Galois-compatible with respect to $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$. By the Isom-form proved in [Saïdi and Tamagawa 2009], $\sigma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}}$ induces an isomorphism

$$\gamma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}} : \tilde{K}_{2,\mathfrak{H}_2}^{(p')} \xrightarrow{\sim} \tilde{K}_{1,\mathfrak{H}_1}^{(p')},$$

which is Galois-compatible with respect to $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$. By Lemma 3.10, $\gamma_{\mathfrak{H}_1^{(p')},\mathfrak{H}_2^{(p')}}$ can be patched together and define an isomorphism

$$\tilde{\gamma} : \tilde{K}_2 \xrightarrow{\sim} (\tilde{K}_1)^{\mathfrak{N}},$$

where

$$\mathfrak{N} \stackrel{\mathrm{def}}{=} \mathrm{Ker}(\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2),$$

which is Galois-compatible with respect to $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$.

In the profinite (resp. prime-to-characteristic) case, $\tilde{K}_2$ admits no nontrivial finite separable (resp. geometrically prime-to-p) extension, and hence neither does $(\tilde{K}_1)^{\mathfrak{N}}$ ($\simeq \tilde{K}_2$). This implies that $(\tilde{K}_1)^{\mathfrak{N}} = \tilde{K}_1$, that is, $\mathfrak{N} = \{1\}$. Thus, we obtain $\tilde{\gamma} : \tilde{K}_2 \xrightarrow{\sim} \tilde{K}_1$, which is Galois-compatible with respect to $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$, as desired. Finally, the uniqueness of such $\tilde{\gamma}$ follows formally from the uniqueness in the statement of the Isom-form, proved in [Uchida 1977; Saïdi and Tamagawa 2009]. This finishes the proof of Theorem 3.4. □

Remark 3.11. We have proved Theorem 3.4 by reducing it to the *statement* of the Isom-form, by means of Lemma 3.9. Instead, we could mimic the *proof* of the Isom-form.

4. Proper homomorphisms between Galois groups

In this section we investigate a class of homomorphisms between (geometrically prime-to-characteristic quotients of) absolute Galois groups of function fields of curves over finite fields, which we call *proper*. We follow the notations in Sections 1–3, and in particular, the Notation at the beginning of subsection 2B. We assume that Condition 3 holds.

Definition 4.1 (well-behaved homomorphisms). We say that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is *well-behaved* if there exists a map

$$\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$$

such that $\sigma(\mathfrak{D}_{\tilde{x}_1}) \underset{\text{open}}{\subset} \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}$ for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$.

Remark 4.2. (i) Given a commutative diagram of maps between profinite groups

$$\begin{array}{ccc} \mathfrak{G}_1 & \twoheadrightarrow & \mathfrak{G}_2 \\ \downarrow & & \downarrow \\ \mathfrak{G}'_1 & \twoheadrightarrow & \mathfrak{G}'_2, \end{array}$$

where the vertical arrows are surjective and the map $\mathfrak{G}_1 \to \mathfrak{G}_2$ is well-behaved, then the map $\mathfrak{G}'_1 \to \mathfrak{G}'_2$ is well-behaved.

(ii) Let $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ be open subgroups such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$. Then if $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is well-behaved, the natural homomorphism $\mathfrak{H}_1 \to \mathfrak{H}_2$ induced by σ is well-behaved. (Here, $\mathfrak{H}_i$ is considered as a quotient of the absolute Galois group that is the inverse image in G_i of $\mathfrak{H}_i \subset \mathfrak{G}_i$.)

(iii) If $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is strictly rigid (Definition 3.1), then it is well-behaved.

(iv) As in Proposition 2.2, let $l \neq p_1, p_2$ be a prime number, and assume that (1) $N_2^l = N_2$, or, equivalently, $\tilde{K}_2$ admits no l-cyclic extension; and (2) $\tilde{K}_2$ contains a primitive l-th roots of unity. Then, first, if $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is rigid, then it is well-behaved by Remark 3.2(iv). Second, if $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is well-behaved with respect to $\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$, then we must have

$$\Sigma_{\tilde{X}_1,\sigma,l} = \Sigma_{\tilde{X}_1} \quad \text{and} \quad \tilde{\phi} = \tilde{\phi}_{\sigma,l}.$$

In particular, then $\tilde{\phi}$ is unique and Galois-equivariant with respect to σ, and hence naturally induces a map $\phi\ (= \phi_{\sigma,l}) : \Sigma_{X_1} \to \Sigma_{X_2}$.

Definition 4.3 (proper homomorphisms). We say that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is proper if σ is well-behaved with respect to $\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$, such that $\tilde{\phi}$ is Galois-equivariant with respect to σ, and the map $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$ induced by $\tilde{\phi}$ has finite fibers, that is, for each $x_2 \in \Sigma_{X_2}$, the fiber $\phi^{-1}(x_2)$ is a (possibly empty) finite set.

Remark 4.4. (i) Given a commutative diagram of maps between profinite groups

$$\begin{array}{ccc} \mathfrak{G}_1 & \longrightarrow & \mathfrak{G}_2 \\ \downarrow & & \downarrow \\ \mathfrak{G}'_1 & \longrightarrow & \mathfrak{G}'_2, \end{array}$$

where the vertical arrows are surjective and the map $\mathfrak{G}_1 \to \mathfrak{G}_2$ is proper, the map $\mathfrak{G}'_1 \to \mathfrak{G}'_2$ is proper.

(ii) Let $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ be open subgroups such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$. Then if $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is proper, the natural homomorphism $\mathfrak{H}_1 \to \mathfrak{H}_2$ induced by σ is proper. (Here, $\mathfrak{H}_i$ is considered as a quotient of the absolute Galois group that is the inverse image in G_i of $\mathfrak{H}_i \subset \mathfrak{G}_i$.)

In the rest of this section, we assume that Condition 1 holds. Assume also that the continuous open homomorphism $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is well-behaved with respect to $\tilde{\phi} : \Sigma_{\tilde{X}_1} \to \Sigma_{\tilde{X}_2}$. By Lemma 2.4, we have $p \overset{\text{def}}{=} p_1 = p_2$. Let $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$ and set $\tilde{x}_2 \overset{\text{def}}{=} \tilde{\phi}(\tilde{x}_1)$. Denote by x_1 and x_2 the image of $\tilde{x}_1$ and $\tilde{x}_2$ in Σ_{X_1} and Σ_{X_2}, respectively. Then

$$\mathfrak{D}_{\tilde{x}_1} \overset{\sigma}{\twoheadrightarrow} \sigma(\mathfrak{D}_{\tilde{x}_1}) \underset{\text{open}}{\subset} \mathfrak{D}_{\tilde{x}_2}.$$

By this and Proposition 2.1(v), we have

$$\mathfrak{I}_{\tilde{x}_1} \overset{\sigma}{\twoheadrightarrow} \sigma(\mathfrak{I}_{\tilde{x}_1}) \underset{\text{open}}{\subset} \mathfrak{I}_{\tilde{x}_2}.$$

In particular, σ induces an open injective homomorphism $\tau^{\mathrm{t}}_{\tilde{x}_1} : \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1} \hookrightarrow \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$, where $\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1}$ (resp. $\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$) denotes the inertia subgroup of $\mathfrak{D}^{\mathrm{t}}_{\tilde{x}_1}$ (resp. of $\mathfrak{D}^{\mathrm{t}}_{\tilde{x}_2}$). We have natural identifications

$$M_1 \overset{\sim}{\to} M_{k(x_1)^{\mathrm{sep}}} \overset{\sim}{\to} \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1}, \quad M_2 \overset{\sim}{\to} M_{k(x_2)^{\mathrm{sep}}} \overset{\sim}{\to} \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2},$$

where $M_i \overset{\text{def}}{=} M_{K_i^{\mathrm{sep}}}$ is the (global) module of roots of unity for $i = 1, 2$.

We introduce the following important concept of rigidity of inertia.

Definition 4.5 (inertia-rigid homomorphisms). We say that the well-behaved homomorphism $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is inertia-rigid if there exists an isomorphism

$$\tau : M_1 \overset{\sim}{\to} M_2$$

of $\hat{\mathbb{Z}}^{p'}$-modules such that for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$, there exists a positive integer $e_{\tilde{x}_1}$ such that the following diagram commutes:

$$\begin{array}{ccccc} M_1 & \overset{\sim}{\longrightarrow} & M_{k(x_1)^{\mathrm{sep}}} & \overset{\sim}{\longrightarrow} & \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1} \\ {\scriptstyle e_{\tilde{x}_1}\cdot\tau}\downarrow & & & & \downarrow{\scriptstyle \tau^{\mathrm{t}}_{\tilde{x}_1}} \\ M_2 & \overset{\sim}{\longrightarrow} & M_{k(x_2)^{\mathrm{sep}}} & \overset{\sim}{\longrightarrow} & \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}, \end{array} \tag{4.1}$$

where $\tilde{x}_2 \overset{\text{def}}{=} \tilde{\phi}(\tilde{x}_1)$; x_1 and x_2 are the images of $\tilde{x}_1$ and $\tilde{x}_2$ in Σ_{X_1} and Σ_{X_2}, respectively; and the isomorphisms are the canonical identifications.

Remark 4.6. (i) Given a commutative diagram of maps between profinite groups

$$\begin{array}{ccc} G_1 & \twoheadrightarrow & G_2 \\ \downarrow & & \downarrow \\ G_1^{(p')} & \twoheadrightarrow & G_2^{(p')}, \end{array}$$

where the vertical arrows are natural surjective maps and the map $G_1 \to G_2$ is inertia-rigid, the map $G_1^{(p')} \to G_2^{(p')}$ is inertia-rigid.

(ii) Let $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ be open subgroups such that $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$. Then if $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is inertia-rigid, the natural homomorphism $\mathfrak{H}_1 \to \mathfrak{H}_2$ induced by σ is inertia-rigid. (Here, $\mathfrak{H}_i$ is considered as a quotient of the absolute Galois group that is the inverse image in G_i of $\mathfrak{H}_i \subset \mathfrak{G}_i$.)

Remark 4.7. (i) Set

$$\mathfrak{e}_{\tilde{x}_1} \overset{\text{def}}{=} [\mathfrak{I}_{\tilde{x}_2} : \sigma(\mathfrak{I}_{\tilde{x}_1})], \quad \mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1} \overset{\text{def}}{=} [\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2} : \tau^{\mathrm{t}}_{\tilde{x}_1}(\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1})].$$

Note that $p \nmid \mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$ and there exists an integer $b_{\tilde{x}_1} \geq 0$ such that $\mathfrak{e}_{\tilde{x}_1} = p^{b_{\tilde{x}_1}} \mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$. (In the prime-to-characteristic case, we have $\mathfrak{e}_{\tilde{x}_1} = \mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$ and $b_{\tilde{x}_1} = 0$.) Now, in Definition 4.5, there must exist an integer $a_{\tilde{x}_1} \geq 0$ such that $e_{\tilde{x}_1} = p^{a_{\tilde{x}_1}} \mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$, or, equivalently, $e_{\tilde{x}_1} = p^{c_{\tilde{x}_1}} \mathfrak{e}_{\tilde{x}_1}$, where $c_{\tilde{x}_1} \overset{\text{def}}{=} a_{\tilde{x}_1} - b_{\tilde{x}_1} \in \mathbb{Z}$. Moreover, set

$$a \overset{\text{def}}{=} \min\{a_{\tilde{x}_1} \mid \tilde{x}_1 \in \Sigma_{\tilde{X}_1}\}.$$

Replacing τ by $p^a \tau$ and $e_{\tilde{x}_1}$ by $p^{-a} e_{\tilde{x}_1} = p^{a_{\tilde{x}_1} - a} \mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$, we may assume that $a = 0$.

Assume, moreover, that σ is proper and that we are in the profinite case. Then, in fact, we have $c_{\tilde{x}_1} = 0$ for every $\tilde{x}_1 \in \tilde{X}_1$ eventually, if we choose τ with $a = 0$. (This follows from Theorem 4.8 below and its proof.) Thus, in the profinite case, we may assume $e_{\tilde{x}_1} = \mathfrak{e}_{\tilde{x}_1}$ in Definition 4.5 from the beginning. In the prime-to-characteristic case, however, it seems difficult to specify the value of $e_{\tilde{x}_1}$ a priori. (If we assumed $e_{\tilde{x}_1} = \mathfrak{e}_{\tilde{x}_1}$ in the prime-to-characteristic case, then inertia-rigid homomorphisms would cover only tame homomorphisms $K_2 \to K_1$.)

(ii) In the situation of Definition 4.5, we have

$$\mathfrak{D}_{\tilde{x}_1} \overset{\sigma}{\twoheadrightarrow} \mathfrak{E}_{\tilde{x}_1} \overset{\text{def}}{=} \sigma(\mathfrak{D}_{\tilde{x}_1}) \subset \mathfrak{D}_{\tilde{x}_2}.$$

The subgroup $\mathfrak{E}_{\tilde{x}_1} \subset \mathfrak{D}_{\tilde{x}_2}$ corresponds to a finite extension $L_{x_1}/(K_2)_{x_2}$ of the x_2-adic completion $(K_2)_{x_2}$ of K_2. Thus, the residue field ℓ_{x_1} of L_{x_1} is a finite extension of

the residue field $k(x_2)$ at x_2. We have the commutative diagram

$$\begin{array}{ccc} \mathfrak{D}_{\tilde{x}_1} & \longrightarrow & \mathfrak{E}_{\tilde{x}_1} \\ \downarrow & & \downarrow \\ \mathfrak{D}^{\mathrm{t}}_{\tilde{x}_1} & \longrightarrow & \mathfrak{E}^{\mathrm{t}}_{\tilde{x}_1}, \end{array}$$

where the vertical maps are the canonical surjections onto the maximal tame quotients, and the horizontal maps are naturally induced by σ. Further, the lower horizontal map, which is surjective, naturally induces an isomorphism $\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1} \xrightarrow{\sim} \mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1}$ by Proposition 2.1(v). Here, $\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1}$ and $\mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1}$ denote the inertia subgroups of $\mathfrak{D}^{\mathrm{t}}_{\tilde{x}_1}$ and $\mathfrak{E}^{\mathrm{t}}_{\tilde{x}_1}$, respectively. We have a natural identification $\mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1} \xrightarrow{\sim} \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$, where $\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$ is the inertia subgroup of $\mathfrak{D}^{\mathrm{t}}_{\tilde{x}_2}$, obtained via the natural identifications

$$M_{(K_2)^{\mathrm{sep}}_{x_2}} \xrightarrow{\sim} \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}, \quad M_{L^{\mathrm{sep}}_{x_1}} \xrightarrow{\sim} \mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1}, \quad (K_2)^{\mathrm{sep}}_{x_2} = L^{\mathrm{sep}}_{x_1},$$

which, composed with the natural map $\mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1} \to \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$ induced by the inclusion

$$\mathfrak{E}_{\tilde{x}_1} \to \mathfrak{D}_{\tilde{x}_2},$$

is the $\mathfrak{e}_{\tilde{x}_1}$-th power map $[\mathfrak{e}_{\tilde{x}_1}] : \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2} \to \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$, as is easily verified. We define

$$\tau^{\mathrm{t}}_{\tilde{x}_1,\tilde{x}_2} : \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1} \xrightarrow{\sim} \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$$

to be the natural isomorphism obtained by composing the natural isomorphism

$$\mathfrak{I}^{\mathrm{t}}_{x_1} \xrightarrow{\sim} \mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1}$$

induced by σ (see Proposition 2.1(v)) with the natural identification $\mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1} \xrightarrow{\sim} \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}$.

The inertia-rigidity is equivalent to requiring the commutativity of the diagram

$$\begin{array}{ccccc} M_1 & \xrightarrow{\sim} & M_{(K_1)^{\mathrm{sep}}_{x_1}} & \xrightarrow{\sim} & \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1} \\ {\scriptstyle p^{c_{\tilde{x}_1}}\cdot\tau}\downarrow & & & & \downarrow{\scriptstyle \tau^{\mathrm{t}}_{\tilde{x}_1,\tilde{x}_2}} \\ M_2 & \xrightarrow{\sim} & M_{(K_2)^{\mathrm{sep}}_{x_2}} & \xrightarrow{\sim} & \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}, \end{array}$$

in which both vertical arrows are isomorphisms.

Define $\mathrm{Hom}(K_2, K_1)^{\mathrm{sep}} \subset \mathrm{Hom}(K_2, K_1)$ to be the set of separable homomorphisms $K_2 \to K_1$. Define $\mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{pr,inrig}} \subset \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)$ to be the set of proper (and hence continuous and open) inertia-rigid homomorphisms $\mathfrak{G}_1 \to \mathfrak{G}_2$. Our aim in this section is to prove the following.

Theorem 4.8. *The natural map* $\mathrm{Hom}(K_2, K_1) \to \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)/\mathrm{Inn}(\mathfrak{G}_2)$ *induces a bijection*

$$\mathrm{Hom}(K_2, K_1)^{\mathrm{sep}} \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{pr,inrig}}/\mathrm{Inn}(\mathfrak{G}_2).$$

More precisely:

(i) *If $\gamma : K_2 \to K_1$ is a separable homomorphism between fields, then the homomorphism $\mathfrak{G}_1 \to \mathfrak{G}_2$ induced by γ (up to inner automorphisms) is proper and inertia-rigid.*

(ii) *If $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is a proper, inertia-rigid homomorphism between profinite groups, then there exists a unique homomorphism $\tilde{\gamma} : \tilde{K}_2 \to \tilde{K}_1$ of fields, such that $\tilde{\gamma} \circ \sigma(g_1) = g_1 \circ \tilde{\gamma}$, for all $g_1 \in \mathfrak{G}_1$, which induces a separable homomorphism $K_2 \to K_1$.*

Remark 4.9. (i) Assume that $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ is a rigid homomorphism. Then it follows from Lemma 3.8(ii) that σ is proper. Further, σ is inertia-rigid. This can be reduced to the case where σ is strictly rigid, and then deduced from class field theory as in the arguments preceding Lemma 4.12. (Note that then ϕ is bijective by Lemma 3.8(ii).) Thus, Theorem 4.8 can be viewed as a generalization of Theorem 3.4.

(ii) The natural map $\mathrm{Hom}(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}}) \to \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)/\mathrm{Inn}(\mathfrak{G}_2)$ induces a bijection

$$\mathrm{Hom}(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}})/\mathrm{Frob}^{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{G}_1, \mathfrak{G}_2)^{\mathrm{pr,inrig}}/\mathrm{Inn}(\mathfrak{G}_2).$$

Indeed, this follows from Theorem 4.8, since the natural map $\mathrm{Hom}(K_2, K_1) \to \mathrm{Hom}(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}})$ induces

$$\mathrm{Hom}(K_2, K_1)^{\mathrm{sep}} \xrightarrow{\sim} \mathrm{Hom}(K_2^{\mathrm{perf}}, K_1^{\mathrm{perf}})/\mathrm{Frob}^{\mathbb{Z}}.$$

The rest of this section is devoted to the proof of Theorem 4.8.

First, to prove (i), let $\gamma : K_2 \to K_1$ be a separable homomorphism. Then γ induces naturally an open injective homomorphism $G_1 \hookrightarrow G_2$ (up to $\mathrm{Inn}(G_2)$) and then an open homomorphism $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ (up to $\mathrm{Inn}(\mathfrak{G}_2)$). The map σ is well-behaved with respect to the map $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$ that arises from a finite morphism $X_1 \to X_2$ of schemes corresponding to $\gamma : K_2 \to K_1$. Thus, each fiber of ϕ is finite, and hence σ is proper. Next, if we define $\tau : M_1 \xrightarrow{\sim} M_2$ to be the identification $M_{K_1^{\mathrm{sep}}} \xrightarrow{\sim} M_{K_2^{\mathrm{sep}}}$ (with respect to a suitable extension $K_2^{\mathrm{sep}} \xrightarrow{\sim} K_1^{\mathrm{sep}}$ of $\gamma : K_2 \to K_1$), then diagram (4.1) commutes with $e_{\tilde{x}_1}$ defined to be the ramification index of K_1/K_2 at $\tilde{x}_1$. Thus, σ is inertia-rigid.

Next, to prove (ii), let $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$ be a proper, inertia-rigid homomorphism.

Lemma 4.10. *Condition 2 holds for $\sigma : \mathfrak{G}_1 \to \mathfrak{G}_2$.*

Proof. Same as that of Lemma 3.6. □

Thus, we may apply Lemmas 2.6–2.9 to σ.

Next, let $\tau : M_1 \xrightarrow{\sim} M_2$ be the isomorphism appearing in the definition of inertia-rigid homomorphism, so that diagram (4.1) commutes for each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$ and for some $e_{\tilde{x}_1} \in \mathbb{Z}_{>0}$.

Lemma 4.11. (i) *The isomorphism $\tau : M_1 \xrightarrow{\sim} M_2$ is Galois-equivariant with respect to σ.*

(ii) *The positive integers $e_{\tilde{x}_1}$, $\mathfrak{e}_{\tilde{x}_1}$ and $\mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$ depend only on the image $x_1 \in \Sigma_{X_1}$ of $\tilde{x}_1$.*

Proof. (i) For each $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$, the commutativity of diagram (4.1), together with Proposition 2.1(iv), implies that τ is Galois-equivariant with respect to

$$\mathfrak{D}_{\tilde{x}_1} \xrightarrow{\sigma} \mathfrak{D}_{\tilde{\phi}(\tilde{x}_1)}.$$

Our assertion then follows, since $\mathfrak{G}_1$ is generated by the decomposition subgroups $\mathfrak{D}_{\tilde{x}_1}$ for all $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$, as follows from Chebotarev's density theorem.

(ii) Take another $\tilde{x}'_1 \in \Sigma_{\tilde{X}_1}$ above $x_1 \in \Sigma_{X_1}$ and set $\tilde{x}'_2 \stackrel{\mathrm{def}}{=} \tilde{\phi}(\tilde{x}'_1)$. Fix $\gamma \in \mathfrak{G}_1$ such that $\tilde{x}'_1 = \gamma \tilde{x}_1$. By the Galois-equivariance property of $\tilde{\phi}$ (Remark 4.2(iv)), we have then $\tilde{x}'_2 = \sigma(\gamma)\tilde{x}_2$. Denote by $[\gamma]$ and $[\sigma(\gamma)]$ the inner automorphisms of $\mathfrak{G}_1$ and $\mathfrak{G}_2$ induced by γ and $\sigma(\gamma)$, respectively. We have the commutative diagram

$$\begin{array}{ccc} \mathfrak{I}_{\tilde{x}_1} & \xrightarrow{[\gamma]} & \mathfrak{I}_{\tilde{x}'_1} \\ {\scriptstyle\sigma}\downarrow & & {\scriptstyle\sigma}\downarrow \\ \mathfrak{I}_{\tilde{x}_2} & \xrightarrow{[\sigma(\gamma)]} & \mathfrak{I}_{\tilde{x}'_2}, \end{array}$$

in which both rows are isomorphisms. It follows that $\mathfrak{e}_{\tilde{x}'_1} = \mathfrak{e}_{\tilde{x}_1}$. This commutative diagram induces the commutative diagram

$$\begin{array}{ccc} \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1} & \xrightarrow{[\gamma]} & \mathfrak{I}^{\mathrm{t}}_{\tilde{x}'_1} \\ {\scriptstyle\tau^{\mathrm{t}}_{\tilde{x}_1}}\downarrow & & {\scriptstyle\tau^{\mathrm{t}}_{\tilde{x}'_1}}\downarrow \\ \mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2} & \xrightarrow{[\sigma(\gamma)]} & \mathfrak{I}^{\mathrm{t}}_{\tilde{x}'_2}, \end{array}$$

in which both rows are isomorphisms. It follows that $\mathfrak{e}^{\mathrm{t}}_{\tilde{x}'_1} = \mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$. With (i), this last commutative diagram also implies that $e_{\tilde{x}'_1} = e_{\tilde{x}_1}$. □

From now on, we shall write e_{x_1}, $\mathfrak{e}_{x_1}$ and $\mathfrak{e}^{\mathrm{t}}_{x_1}$ for $e_{\tilde{x}_1}$, $\mathfrak{e}_{\tilde{x}_1}$ and $\mathfrak{e}^{\mathrm{t}}_{\tilde{x}_1}$, respectively. Further, according to this, we shall write a_{x_1}, b_{x_1} and c_{x_1} for the invariants $a_{\tilde{x}_1}$, $b_{\tilde{x}_1}$ and $c_{\tilde{x}_1}$ in Remark 4.7(i), respectively. We may and shall also assume that

$$a\ (= \min\{a_{x_1} \mid x_1 \in \Sigma_{X_1}\}) = 0;$$

see Remark 4.7(i).

We have the commutative diagram of exact sequences

$$\begin{array}{ccccccc} 1 & \longrightarrow & k_1^{\times} & \longrightarrow & \prod_{x_2 \in \Sigma_{X_2}} \Big(\prod_{x_1 \in \phi^{-1}(x_2)} k(x_1)^{\times} \Big) & \longrightarrow & {\mathfrak{G}_1}^{(p'),\mathrm{ab}} \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & k_2^{\times} & \longrightarrow & \prod_{x_2 \in \Sigma_{X_2}} k(x_2)^{\times} & \longrightarrow & {\mathfrak{G}_2}^{(p'),\mathrm{ab}} \end{array}$$

from global class field theory. Here, the map ${\mathfrak{G}_1}^{(p'),\mathrm{ab}} \twoheadrightarrow {\mathfrak{G}_2}^{(p'),\mathrm{ab}}$ is naturally induced by σ. The right horizontal maps are induced by Artin's reciprocity map, and the map

$$\prod_{x_2 \in \Sigma_{X_2}} \Big(\prod_{x_1 \in \phi^{-1}(x_2)} k(x_1)^{\times} \Big) \to \prod_{x_2 \in \Sigma_{X_2}} k(x_2)^{\times}$$

maps each component $k(x_1)^{\times}$ to $k(x_2)^{\times}$ as follows. First, $k(x_1)^{\times}$ maps isomorphically onto $\ell_{x_1}^{\times}$ via the natural identification induced by σ; see Remark 4.7(ii) and Proposition 2.1(iii). Then $\ell_{x_1}^{\times}$ maps to $k(x_2)^{\times}$ by the $\mathfrak{e}_{x_1}$-th power of the norm map.

The above diagram induces, for each $x_2 \in \Sigma_{X_2}$, the commutative diagram

$$\begin{array}{ccccc} k_1^{\times} & \longrightarrow & \prod_{x_1 \in \phi^{-1}(x_2)} k(x_1)^{\times} & \xrightarrow{\sim} & \prod_{x_1 \in \phi^{-1}(x_2)} \ell_{x_1}^{\times} \\ \downarrow & & & & \downarrow \\ k_2^{\times} & \longrightarrow & k(x_2)^{\times}, & & \end{array}$$

where the map $k_2^{\times} \to k(x_2)^{\times}$ is the natural embedding, the map

$$k_1^{\times} \to \prod_{x_1 \in \phi^{-1}(x_2)} k(x_1)^{\times}$$

is the natural diagonal embedding, and the isomorphism

$$\prod_{x_1 \in \phi^{-1}(x_2)} k(x_1)^{\times} \xrightarrow{\sim} \prod_{x_1 \in \phi^{-1}(x_2)} \ell_{x_1}^{\times}$$

and the map

$$\prod_{x_1 \in \phi^{-1}(x_2)} \ell_{x_1}^{\times} \to k(x_2)^{\times}$$

are as above. By passing to various open subgroups corresponding to extensions of the constant fields, and to the projective limit via the norm maps, we obtain the

commutative diagram

$$\begin{array}{ccc} M_{k_1^{\mathrm{sep}}} \twoheadrightarrow \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} M_{k(x_1)^{\mathrm{sep}}} & \overset{\bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} \rho_{x_1}}{\xrightarrow{\sim}} & \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} M_{\ell_{x_1}^{\mathrm{sep}}} \\ \downarrow & & \downarrow \\ M_{k_2^{\mathrm{sep}}} & \twoheadrightarrow & M_{k(x_2)^{\mathrm{sep}}}, \end{array}$$

where

$$\rho_{x_1} : M_{k(x_1)^{\mathrm{sep}}} \xrightarrow{\sim} M_{\ell_{x_1}^{\mathrm{sep}}}$$

is the natural isomorphism induced by σ; see Remark 4.7(ii) and Proposition 2.1(v). Here, $\bar{x}_2 \in \Sigma_{\overline{X}_2}$ is any point above x_2 and $\bar{\phi} : \Sigma_{\overline{X}_1} \to \Sigma_{\overline{X}_2}$ is obtained as the inductive limit of ϕ's for various open subgroups corresponding to extensions of the constant fields. Observe that $\bar{\phi} : \Sigma_{\overline{X}_1} \to \Sigma_{\overline{X}_2}$ has finite fibers, since $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$ has finite fibers, the projection $\Sigma_{\overline{X}_1} \to \Sigma_{X_1}$ has finite fibers, and $\bar{\phi}$ is compatible with ϕ.

This can be rewritten as

$$\begin{array}{ccc} M_1 \twoheadrightarrow \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} M_1 & \overset{\bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} \rho_{x_1}}{\xrightarrow{\sim}} & \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} M_2 \\ \downarrow & & \downarrow \\ M_2 = & & = M_2 \end{array} \tag{4.2}$$

via the natural identifications $M_{k(x_1)^{\mathrm{sep}}} \xrightarrow{\sim} M_1$ and $M_{\ell_{x_1}^{\mathrm{sep}}} \xrightarrow{\sim} M_2$ for $x_1 \in \phi^{-1}(x_2)$; $M_{k(x_2)^{\mathrm{sep}}} \xrightarrow{\sim} M_2$; and $M_{k_i^{\mathrm{sep}}} \xrightarrow{\sim} M_i$, $i = 1, 2$. Thus, in diagram (4.2) the map $M_1 \to \oplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} M_1$ is the natural diagonal embedding, and the map $\oplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} M_2 \to M_2$ is the map $\oplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} [\mathfrak{e}_{x_1}]$. We shall denote by $\tau' : M_1 \to M_2$ the homomorphism that is the left vertical arrow in diagram (4.2) (note that τ' is independent of the choice of $x_2 \in \Sigma_{X_2}$).

Lemma 4.12 (product formula). *The sum $\sum_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} e_{x_1}$ is independent of the choice of $x_2 \in \Sigma_{X_2}$. Set $n \overset{def}{=} \sum_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} e_{x_1} > 0$. Then we have $\tau' = [n] \circ \tau$, where $[n] : M_2 \to M_2$ denotes the map of elevation to the power n in M_2.*

Proof. This follows from the commutativity of diagram (4.2), by observing that the homomorphism σ being inertia-rigid means that the isomorphism ρ_{x_1} in diagram (4.2) equals $p^{c_{x_1}} \tau$ for all $\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)$. □

For the rest of this section, all cohomology groups will be continuous Galois cohomology groups unless otherwise specified.

The Galois-equivariant identification $\tau^{-1} : M_2 \xrightarrow{\sim} M_1$ induces naturally an injective homomorphism $H^1(\mathfrak{G}_2, M_2) \to H^1(\mathfrak{G}_1, M_1)$ between Galois cohomology

groups. Indeed, this homomorphism fits into the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G_{k_2}, M_2) & \twoheadrightarrow & H^1(\mathfrak{G}_2, M_2) & \twoheadrightarrow & H^1(\overline{\mathfrak{G}}_2, M_2) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1(G_{k_1}, M_1) & \twoheadrightarrow & H^1(\mathfrak{G}_1, M_1) & \twoheadrightarrow & H^1(\overline{\mathfrak{G}}_1, M_1), \end{array}$$

where both rows are exact and vertical maps are natural maps induced by (σ, τ^{-1}). Here, the left vertical arrow is injective by $H^0(H_{k_1}, M_2) = 0$, where H_{k_1} stands for the (isomorphic) image of G_{k_1} in G_{k_2}, and the right vertical arrow is injective since M_2 is torsion-free and $[\overline{\mathfrak{G}}_2 : \sigma(\overline{\mathfrak{G}}_1)] < \infty$. Therefore, the middle vertical arrow is also injective.

Further, for each $x_2 \in \Sigma_{X_2}$, the following diagram is commutative:

$$\begin{array}{ccc} H^1(\mathfrak{G}_1, M_1) & \twoheadrightarrow & \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} H^1(\mathfrak{I}_{\tilde{x}_1}, M_1) \xrightarrow{\sim} \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} H^1(\mathfrak{J}_{\tilde{x}_1}, M_2) \\ \uparrow & & \uparrow \\ H^1(\mathfrak{G}_2, M_2) & \longrightarrow & H^1(\mathfrak{I}_{\tilde{x}_2}, M_2), \end{array}$$

where the horizontal maps are the natural restriction maps, the left vertical map is the above map, the map

$$H^1(\mathfrak{I}_{\tilde{x}_2}, M_2) \to \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} H^1(\mathfrak{J}_{\tilde{x}_1}, M_2)$$

is the natural map induced by the inclusion $\mathfrak{J}_{\tilde{x}_1} \subset \mathfrak{I}_{\tilde{x}_2}$ for $\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)$, and the isomorphism $H^1(\mathfrak{I}_{\tilde{x}_1}, M_1) \xrightarrow{\sim} H^1(\mathfrak{J}_{\tilde{x}_1}, M_2)$ is naturally induced by the natural surjective map $\mathfrak{I}_{\tilde{x}_1} \twoheadrightarrow \mathfrak{J}_{\tilde{x}_1}$, which is induced by (σ, τ^{-1}).

We have natural identifications

$$\begin{aligned} H^1(\mathfrak{I}_{\tilde{x}_1}, M_1) &\xrightarrow{\sim} \mathrm{Hom}(\mathfrak{I}_{\tilde{x}_1}, M_1) \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_1}, M_1) \xrightarrow{\sim} \mathrm{Hom}(M_1, M_1) \xrightarrow{\sim} \hat{\mathbb{Z}}^{p'}, \\ H^1(\mathfrak{J}_{\tilde{x}_1}, M_2) &\xrightarrow{\sim} \mathrm{Hom}(\mathfrak{J}_{\tilde{x}_1}, M_2) \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{J}^{\mathrm{t}}_{\tilde{x}_1}, M_2) \xrightarrow{\sim} \mathrm{Hom}(M_2, M_2) \xrightarrow{\sim} \hat{\mathbb{Z}}^{p'}, \\ H^1(\mathfrak{I}_{\tilde{x}_2}, M_2) &\xrightarrow{\sim} \mathrm{Hom}(\mathfrak{I}_{\tilde{x}_2}, M_2) \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{I}^{\mathrm{t}}_{\tilde{x}_2}, M_2) \xrightarrow{\sim} \mathrm{Hom}(M_2, M_2) \xrightarrow{\sim} \hat{\mathbb{Z}}^{p'}. \end{aligned}$$

In light of these identifications, the above diagram can be rewritten as

$$\begin{array}{ccc} H^1(\mathfrak{G}_1, M_1) & \twoheadrightarrow & \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} \hat{\mathbb{Z}}^{p'} \\ \uparrow & & \uparrow \oplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} [e_{x_1}] \\ H^1(\mathfrak{G}_2, M_2) & \longrightarrow & \hat{\mathbb{Z}}^{p'}, \end{array}$$

where the vertical map $\hat{\mathbb{Z}}^{p'} \to \bigoplus_{\bar{x}_1 \in \bar{\phi}^{-1}(\bar{x}_2)} \hat{\mathbb{Z}}^{p'}$ is the map $\bigoplus_{\bar{x}_1 \in \phi^{-1}(\bar{x}_2)} [e_{x_1}]$, and $[e_{x_1}]$ denotes the map of multiplication by e_{x_1} in $\hat{\mathbb{Z}}^{p'}$. By considering all $x_2 \in \Sigma_{X_2}$,

we obtain the following commutative diagram:

$$\begin{array}{ccccc} H^1(\mathfrak{G}_1, M_1) & \twoheadrightarrow & \widehat{\mathrm{Div}}_{\overline{X}_1} \stackrel{\mathrm{def}}{=} \prod_{\bar{x}_1 \in \Sigma_{\overline{X}_1}}{}' \hat{\mathbb{Z}}^{p'} & \stackrel{\sim}{\to} & \prod_{\bar{x}_2 \in \Sigma_{\overline{X}_2}}{}' \left(\bigoplus_{\bar{x}_1 \in \phi^{-1}(\bar{x}_2)} \hat{\mathbb{Z}}^{p'}\right) \\ \uparrow & & & & \uparrow \\ H^1(\mathfrak{G}_2, M_2) & \longrightarrow & \widehat{\mathrm{Div}}_{\overline{X}_2} \stackrel{\mathrm{def}}{=} \prod_{\bar{x}_2 \in \Sigma_{\overline{X}_2}}{}' \hat{\mathbb{Z}}^{p'}. & & \end{array}$$

Here, given an index set Λ, we define $\prod'_{\lambda\in\Lambda} \hat{\mathbb{Z}}^{p'} \stackrel{\mathrm{def}}{=} \varprojlim_{p\nmid n} \left(\bigoplus_{\lambda\in\Lambda} \mathbb{Z}/n\mathbb{Z}\right)$. (Accordingly, one has

$$\bigoplus_{\lambda\in\Lambda} \hat{\mathbb{Z}}^{p'} \subset \prod_{\lambda\in\Lambda}{}' \hat{\mathbb{Z}}^{p'} \subset \prod_{\lambda\in\Lambda} \hat{\mathbb{Z}}^{p'},$$

and the equalities hold if and only if $\sharp(\Lambda) < \infty$.) Thus, the map $\widehat{\mathrm{Div}}_{\overline{X}_2} \to \widehat{\mathrm{Div}}_{\overline{X}_1}$ maps $\bar{x}_2$ to $\sum_{\bar{x}_1\in\phi^{-1}(\bar{x}_2)} e_{x_1}\bar{x}_1$. In particular, the subgroup $\widehat{\mathrm{Div}}_{X_2}$ of $\widehat{\mathrm{Div}}_{\overline{X}_2}$ maps into the subgroup $\widehat{\mathrm{Div}}_{X_1}$ of $\widehat{\mathrm{Div}}_{\overline{X}_1}$. Here, for $i = 1, 2$,

$$\widehat{\mathrm{Div}}_{X_i} \stackrel{\mathrm{def}}{=} \prod_{x_1\in\Sigma_{X_i}}{}' \hat{\mathbb{Z}}^{p'}$$

is naturally embedded into $\widehat{\mathrm{Div}}_{\overline{X}_i}$ and is regarded as a subgroup of $\widehat{\mathrm{Div}}_{\overline{X}_i}$. It follows from various constructions that, for $i = 1, 2$, the image of the map $H^1(\mathfrak{G}_i, M_i) \to \widehat{\mathrm{Div}}_{\overline{X}_i}$ is contained in $\widehat{\mathrm{Div}}_{X_i}$. Thus, we obtain the commutative diagram

$$\begin{array}{ccc} H^1(\mathfrak{G}_1, M_1) & \twoheadrightarrow & \widehat{\mathrm{Div}}_{X_1} \\ \uparrow & & \uparrow \\ H^1(\mathfrak{G}_2, M_2) & \twoheadrightarrow & \widehat{\mathrm{Div}}_{X_2}. \end{array} \tag{4.3}$$

For $i = 1, 2$, set $\mathrm{Div}_{X_i} \stackrel{\mathrm{def}}{=} \bigoplus_{x_i\in\Sigma_{X_i}} \mathbb{Z}$, which is the group of divisors on X_i. Then the subgroup Div_{X_2} of $\widehat{\mathrm{Div}}_{X_2}$ maps into the subgroup

$$\mathrm{Div}_{X_1} = \bigoplus_{x_2\in\Sigma_{X_2}} \Big(\bigoplus_{x_1\in\phi^{-1}(x_2)} \mathbb{Z} \Big)$$

of $\widehat{\mathrm{Div}}_{X_1}$. Thus, we have a natural map

$$\mathrm{Div}_{X_2} \to \mathrm{Div}_{X_1}.$$

We denote by Pri_{X_i} the subgroup of Div_{X_i} which consists of principal divisors. Note that we have a natural map $K_i^\times \to \mathrm{Div}_{X_i}$, which maps a function f_i to its divisor $\mathrm{div}(f_i)$ of zeros and poles. Further, Let J_{X_i} be the Jacobian variety of X_i.

Let $\mathrm{Div}^0_{X_i} \subset \mathrm{Div}_{X_i}$ be the group of degree-zero divisors on X_i. Then there exists a natural isomorphism

$$\mathrm{Div}^0_{X_i} / \mathrm{Pri}_{X_i} = J_{X_i}(k_i).$$

Write D_{X_i} for the kernel of the natural homomorphism $\mathrm{Div}^0_{X_i} \to J_{X_i}(k_i)^{p'}$, with $J_{X_i}(k_i)^{p'}$ standing for the maximal prime-to-p quotient $J_{X_i}(k_i)/(J_{X_i}(k_i)\{p\})$ of $J_{X_i}(k_i)$, where, for an abelian group M, $M\{p\}$ stands for the subgroup of torsion elements a of M of p-power order. Then D_{X_i} sits naturally in the exact sequence

$$0 \to \mathrm{Pri}_{X_i} \to D_{X_i} \to J_{X_i}(k_i)\{p\} \to 0.$$

For $i \in \{1, 2\}$, and a positive integer n prime to p, the Kummer exact sequence

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m \to 1$$

induces a natural isomorphism

$$K_i^\times/(K_i^\times)^n \xrightarrow{\sim} H^1(\mathfrak{G}_i, \mu_n(K_i^{\mathrm{sep}}));$$

see Lemma 1.4. By passing to the projective limit over all integers n prime to p, we obtain a natural isomorphism

$$(K_i^\times)^{\wedge p'} \xrightarrow{\sim} H^1(\mathfrak{G}_i, M_i),$$

where

$$(K_i^\times)^{\wedge p'} \stackrel{\mathrm{def}}{=} \varprojlim_{p\nmid n} K_i^\times/(K_i^\times)^n.$$

Since we have a natural embedding $K_i^\times \hookrightarrow (K_i^\times)^{\wedge p'}$, we get a natural embedding

$$K_i^\times \hookrightarrow H^1(\mathfrak{G}_i, M_i).$$

In what follows we will identify $K_i^\times$ with its image in $H^1(\mathfrak{G}_i, M_i)$; $i = 1, 2$. The natural maps $K_i^\times \to \mathrm{Div}_{X_i}$ and $H^1(\mathfrak{G}_i, M_i) \to \widehat{\mathrm{Div}}_{X_i}$ are compatible with each other, and hence the image of $K_i^\times$ in $\widehat{\mathrm{Div}}_{X_i}$, via the map $H^1(\mathfrak{G}_i, M_i) \to \widehat{\mathrm{Div}}_{X_i}$ in diagram (4.3), coincides with the subgroup Pri_{X_i} of principal divisors.

Lemma 4.13 (recovering the multiplicative group). (i) *The homomorphism*

$$\widehat{\mathrm{Div}}_{X_2} \to \widehat{\mathrm{Div}}_{X_1}$$

in diagram (4.3) *maps* D_{X_2} *into* D_{X_1}.

(ii) *The above map* $H^1(\mathfrak{G}_2, M_2) \to H^1(\mathfrak{G}_1, M_1)$ *induces a natural injective* (*multiplicative*) *homomorphism*

$$\gamma : K_2^\times \hookrightarrow (K_1^\times)^{p^{-n}} = (K_1^{p^{-n}})^\times,$$

where p^n *is the exponent of the* p*-primary finite abelian group* $J_{X_1}(k_1)\{p\}$. *We have* $[\gamma(K_2^\times) : \gamma(K_2^\times) \cap K_1^\times] < \infty$ *and* $[\gamma(K_2^\times) : \gamma(K_2^\times) \cap (K_1^\times)^p] > 1$.

Moreover, this injective homomorphism is functorial in the following sense: *Let* $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ *be open subgroups such that* $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$, *and, for* $i = 1, 2$, *let* L_i/K_i *be the finite separable extension corresponding to* $\mathfrak{H}_i \subset \mathfrak{G}_i$, Y_i *the integral closure of* X_i *in* L_i, *and* ℓ_i *the constant field of* L_i (*that is, the algebraic closure of* k_i *in* L_i). *Then we have a commutative diagram*

$$\begin{array}{ccc} L_2^{\times} & \twoheadrightarrow & (L_1^{\times})^{p^{-m}} \\ \uparrow & & \uparrow \\ K_2^{\times} & \twoheadrightarrow & (K_1^{\times})^{p^{-n}}, \end{array}$$

where $p^m \geq p^n$ *is the exponent of the* p*-primary finite abelian group* $J_{Y_1}(\ell_1)\{p\}$, *and the vertical arrows are the natural embeddings.*

Proof. (i) We have the diagram of maps

$$\begin{array}{ccc} \mathrm{Div}_{X_1} & \twoheadrightarrow & H^2(\pi_1(X_1)^{(p')}, M_1) \\ \uparrow & & \uparrow \\ \mathrm{Div}_{X_2} & \twoheadrightarrow & H^2(\pi_1(X_2)^{(p')}, M_2), \end{array}$$

where the map $\mathrm{Div}_{X_2} \to \mathrm{Div}_{X_1}$ is the one induced by the map $\widehat{\mathrm{Div}}_{X_2} \to \widehat{\mathrm{Div}}_{X_1}$ in diagram (4.3). For $i \in \{1, 2\}$, the group $H^2(\pi_1(X_i)^{(p')}, M_i)$ denotes the second cohomology group of the profinite group $\pi_1(X_i)^{(p')}$ with coefficients in the (continuous) $\pi_1(X_i)^{(p')}$-module M_i.

First, we shall treat the special case that $(g_1 \geq) g_2 > 0$. In this case, we have a natural isomorphism $H^2(\pi_1(X_i)^{(p')}, M_i) \xrightarrow{\sim} H^2_{\mathrm{et}}(X_i, M_i)$ ([Mochizuki 2007, Proposition 1.1]), where $H^2_{\mathrm{et}}(X_i, M_i)$ denotes the second étale cohomology group of X_i with coefficients in M_i. We will identify the groups $H^2(\pi_1(X_i)^{(p')}, M_i)$ and $H^2_{\mathrm{et}}(X_i, M_i)$ via the above identifications. Further, the map $H^2(\pi_1(X_2)^{(p')}, M_2) \to H^2(\pi_1(X_1)^{(p')}, M_1)$ is the map induced by the natural map $\pi_1(X_1)^{(p')} \to \pi_1(X_2)^{(p')}$ between fundamental groups, which is induced by σ (see Lemma 2.6), and the Galois-equivariant identification $\tau^{-1} : M_2 \xrightarrow{\sim} M_1$. The map

$$\mathrm{Div}_{X_i} \to H^2(\pi_1(X_i)^{(p')}, M_i)$$

maps a divisor D to its first arithmetic (étale) Chern class $c_1(D)$, and is naturally induced by the Kummer exact sequence

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m \to 1$$

in étale topology (see [Mochizuki 2003, 4.1]). In particular, the map $\mathrm{Div}_{X_i} \to H^2(\pi_1(X_i)^{(p')}, M_i)$ factors as

$$\mathrm{Div}_{X_i} \to \mathrm{Pic}(X_i)/(J_{X_i}(k_i)\{p\}) \hookrightarrow H^2(\pi_1(X_i)^{(p')}, M_i),$$

where $\mathrm{Pic}(X_i) \stackrel{\mathrm{def}}{=} H^1_{\mathrm{et}}(X_i, \mathbb{G}_m)$ is the Picard group of X_i. Note that the kernel of the above map $\mathrm{Div}_{X_i} \to H^2(\pi_1(X_i)^{(p')}, M_i)$ coincides with D_{X_i}. We claim that the above diagram is commutative. Thus, it induces a natural map $D_{X_2} \to D_{X_1}$, as desired (in the case that $g_2 > 0$).

To prove this claim, let $x_2 \in \Sigma_{X_2}$. We shall investigate the images of $x_2 \in \mathrm{Div}_{X_2}$ in $H^2(\pi_1(X_1)^{(p')}, M_1)$ under the two (composite) maps in the above diagram. First, consider the special case where $x_2 \in \Sigma_{X_2}$ is k_2-rational and each point of $\phi^{-1}(x_2) \subset \Sigma_{X_1}$ is k_1-rational. Then the image $c_1(x_2)$ of the divisor $x_2 \in \mathrm{Div}_{X_2}$ in $H^2(\pi_1(X_2)^{(p')}, M_2)$ coincides with the class of the extension $1 \to M_2 \to \pi_1(\mathbb{L}_{x_2}^{\times})^{(p')} \to \pi_1(X_2)^{(p')} \to 1$, where $\pi_1(\mathbb{L}_{x_2}^{\times})^{(p')}$ is the geometrically prime-to-p fundamental group of the line bundle $\mathbb{L}_{x_2}$ corresponding to the invertible sheaf $\mathbb{O}_{X_2}(x_2)$ with the zero section removed [Mochizuki 2005, Lemma 4.2; Mochizuki 2003, 4.1]. Further, $\pi_1(\mathbb{L}_{x_2}^{\times})^{(p')}$ is naturally identified with the maximal cuspidally central quotient $\pi_1(X_2 \smallsetminus \{x_2\})^{(p'),\text{c-cn}}$ of $\pi_1(X_2 \smallsetminus \{x_2\})^{(p')}$. Here, for a nonempty open subscheme $U_i \subset X_i$, we define the maximal (geometrically prime-to-p) cuspidally central quotient $\pi_1(U_i)^{(p'),\text{c-cn}}$ to be the maximal quotient of $\pi_1(U_i)^{(p')}$ in which the image of $\mathrm{Ker}(\pi_1(\overline{U}_i) \to \pi_1(\overline{X}_i))$ lies in the center of the image of $\pi_1(\overline{U}_i)$ [Mochizuki 2005, Lemma 4.2(iii)]. Similarly, the maximal cuspidally central quotient $\pi_1(X_1 \smallsetminus \phi^{-1}(x_2))^{(p'),\text{c-cn}}$ of $\pi_1(X_1 \smallsetminus \phi^{-1}(x_2))^{(p')}$ gives the extension of $\pi_1(X_1)^{(p')}$ by $\bigoplus_{x_1 \in \phi^{-1}(x_2)} M_1$ that corresponds to

$$(c_1(x_1))_{x_1 \in \phi^{-1}(x_2)} \in \bigoplus_{x_1 \in \phi^{-1}(x_2)} H^2(\pi_1(X_1)^{(p')}, M_1) = H^2\Big(\pi_1(X_1)^{(p')}, \bigoplus_{x_1 \in \phi^{-1}(x_2)} M_1\Big).$$

Being well-behaved (with respect to $\tilde{\phi}$), σ induces naturally a homomorphism $\pi_1(X_1 \smallsetminus \phi^{-1}(x_2))^{(p')} \to \pi_1(X_2 \smallsetminus \{x_2\})^{(p')}$, which is a lifting of $\pi_1(X_1)^{(p')} \to \pi_1(X_2)^{(p')}$ and which further induces a homomorphism $\pi_1(X_1 \smallsetminus \phi^{-1}(x_2))^{(p'),\text{c-cn}} \to \pi_1(X_2 \smallsetminus \{x_2\})^{(p'),\text{c-cn}}$. These homomorphisms fit into the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \bigoplus_{x_1 \in \phi^{-1}(x_2)} M_1 & \twoheadrightarrow & \pi_1(X_1 \smallsetminus \phi^{-1}(x_2))^{(p'),\text{c-cn}} & \twoheadrightarrow & \pi_1(X_1)^{(p')} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & M_2 & \longrightarrow & \pi_1(X_2 \smallsetminus \{x_2\})^{(p'),\text{c-cn}} & \longrightarrow & \pi_1(X_2)^{(p')} & \longrightarrow & 1,
\end{array}$$

in which both rows are exact and the left vertical arrow is $\bigoplus_{x_1 \in \phi^{-1}(x_2)} e_{x_1}\tau$, by the inertia-rigidity of σ. The commutativity of this last diagram implies that the image of the extension class of the top row (that is, $(c_1(x_1))_{x_1 \in \phi^{-1}(x_2)}$) under the map $H^2(\pi_1(X_1)^{(p')}, \bigoplus_{x_1 \in \phi^{-1}(x_2)} M_1) \to H^2(\pi_1(X_1)^{(p')}, M_1)$ induced by $\bigoplus_{x_1 \in \phi^{-1}(x_2)} [e_{x_1}]$ coincides with the image of the extension class of the bottom row (that is, $c_1(x_2)$) under the map $H^2(\pi_1(X_2)^{(p')}, M_2) \to H^2(\pi_1(X_1)^{(p')}, M_1)$ induced by σ and τ^{-1}. In other words, the image of $c_1(x_2)$ in $H^2(\pi_1(X_1)^{(p')}, M_1)$

coincides with $\sum_{x_1 \in \phi^{-1}(x_2)} e_{x_1} c_1(x_1)$. From this follows the claim (in the special case), since the divisor x_2 maps to $\sum_{x_1 \in \phi^{-1}(x_2)} e_{x_1} x_1$ via the above map $\mathrm{Div}_{X_1} \to \mathrm{Div}_{X_2}$. Finally, consider the general case where x_2 may not be k_2-rational and each point of $\phi^{-1}(x_2)$ may not be k_1-rational. But this is reduced to the special case by considering suitable open subgroups of $\mathfrak{G}_i$, $i = 1, 2$, corresponding to constant field extensions k_i' of k_i. (Here, use the fact that the natural map $H^2(\pi_1(X_i)^{(p')}, M_i) \to H^2(\pi_1(X_i \times_{k_i} k_i')^{(p')}, M_i)$ is injective, which follows from the injectivity of the natural map $J_{X_i}(k_i) \to J_{X_i}(k_i') = J_{X_i \times_{k_i} k_i'}(k_i')$.) Thus, the claim follows.

Next, to treat the general case that we may possibly have $g_2 = 0$, consider any open subgroup $\mathfrak{H}_2$ of $\mathfrak{G}_2$ and set $\mathfrak{H}_1 \overset{\text{def}}{=} \sigma^{-1}(\mathfrak{H}_2)$, which is an open subgroup of $\mathfrak{G}_1$. For each $i = 1, 2$, let Y_i be the cover of X_i corresponding to the open subgroup $\mathfrak{H}_i \subset \mathfrak{G}_i$, and ℓ_i the constant field of Y_i (that is, the algebraic closure of k_i in the function field of Y_i). Now, assume that the genus of Y_2 is positive. Then it follows from the preceding argument that the homomorphism $\mathrm{Div}_{Y_1} \to \mathrm{Div}_{Y_2}$ maps D_{Y_1} into D_{Y_2}. In particular, by functoriality, the image of D_{X_1} in Div_{X_2} is mapped into $D_{Y_2} \subset \mathrm{Div}_{Y_2}$ under the natural map $\mathrm{Div}_{X_2} \to \mathrm{Div}_{Y_2}$. Or, equivalently, the image of D_{X_1} in $\mathrm{Div}_{X_2}/D_{X_2}$ lies in the kernel of $\mathrm{Div}_{X_2}/D_{X_2} \to \mathrm{Div}_{Y_2}/D_{Y_2}$. This last map is identified with the natural map

$$\mathrm{Pic}_{X_2}/(J_{X_2}(k_2)\{p\}) \to \mathrm{Pic}_{Y_2}/(J_{Y_2}(\ell_2)\{p\})$$

induced by the pull-back of line bundles. Thus, by considering the norm map, we see that the kernel in question is killed by the degree $[\mathfrak{G}_2 : \mathfrak{H}_2]$ of the cover $Y_2 \to X_2$, and hence so is the image of D_{X_1} in $\mathrm{Div}_{X_2}/D_{X_2}$.

Observe that the greatest common divisor of $[\mathfrak{G}_2 : \mathfrak{H}_2]$, where $\mathfrak{H}_2$ runs over all open subgroups of $\mathfrak{G}_2$ such that the corresponding cover has positive genus, is 1. (Indeed, if $g_2 > 0$, this is trivial, and, if $g_2 = 0$, this follows, for example, from Kummer theory.) Thus, the image of D_{X_1} in $\mathrm{Div}_{X_2}/D_{X_2}$ must be trivial, as desired.

(ii) For $i = 1, 2$, let $\tilde{D}_{X_i}$ denote the inverse image of $D_{X_i} \subset \mathrm{Div}_{X_i}$ ($\subset \widehat{\mathrm{Div}}_{X_i}$) in $H^1(\mathfrak{G}_i, M_i)$. It follows from (i) and the commutativity of diagram (4.3) that the natural injective homomorphism $H^1(\mathfrak{G}_2, M_2) \hookrightarrow H^1(\mathfrak{G}_1, M_1)$ induces a natural injective homomorphism $\tilde{D}_{X_2} \hookrightarrow \tilde{D}_{X_1}$. Since $K_i^\times$ is the inverse image of $\mathrm{Pri}_{X_i} \subset \mathrm{Div}_{X_i}$ in $H^1(\mathfrak{G}_i, M_i)$ [Mochizuki 2007, Proposition 2.1(ii)], we have

$$\tilde{D}_{X_i}/K_i^\times \overset{\sim}{\to} D_{X_i}/\mathrm{Pri}_{X_i} \overset{\sim}{\to} J_{X_i}(k_i)\{p\}.$$

Thus, the injective homomorphism $\tilde{D}_{X_2} \hookrightarrow \tilde{D}_{X_1}$ induces $(K_2^\times)^{p^n} \hookrightarrow K_1^\times$, or, equivalently, $K_2^\times \hookrightarrow (K_1^\times)^{p^{-n}}$.

Since $\gamma(K_2^\times)/(\gamma(K_2^\times) \cap K_1^\times)$ is injectively mapped into $\tilde{D}_{X_1}/K_1^\times \overset{\sim}{\to} J_{X_1}(k_1)\{p\}$, which is finite, $\gamma(K_2^\times) \cap K_1^\times$ is of finite index in $\gamma(K_2^\times)$. Next, suppose that

$\gamma(K_2^\times) = \gamma(K_2^\times) \cap (K_1^\times)^p$, or, equivalently, $\gamma(K_2^\times) \subset (K_1^\times)^p$. By the assumption that $a = 0$, there exists an $x_1 \in \Sigma_{X_1}$ such that $e_{x_1} = \mathfrak{e}^{\mathrm{t}}_{x_1}$. In particular, e_{x_1} is prime to p. Set $x_2 \overset{\text{def}}{=} \phi(x_1) \in \Sigma_{X_2}$ and take any $g \in K_2^\times$ such that $\mathrm{ord}_{x_2}(g) = 1$. Then, by the commutativity of diagram (4.3), we have $\mathrm{ord}_{x_1}(\gamma(g)) = e_{x_1}\,\mathrm{ord}_{x_2}(g) = e_{x_1}$, which is prime to p. On the other hand, since $\gamma(g) \in (K_1^\times)^p$, $\mathrm{ord}_{x_1}(\gamma(g))$ must be divisible by p, which is absurd.

Finally, the desired commutativity of diagram follows easily from the functoriality of Kummer theory. □

Next, let $x_1 \in \Sigma_{X_1}$ and set $x_2 \overset{\text{def}}{=} \phi(x_1) \in \Sigma_{X_2}$. Then (by choosing $\tilde{x}_1 \in \Sigma_{\tilde{X}_1}$ above x_1 and $\tilde{x}_2 \in \Sigma_{\tilde{X}_2}$ above x_2 such that $\tilde{\phi}(\tilde{x}_1) = \tilde{x}_2$) we have the natural commutative diagram

$$\begin{array}{ccccc} H^1(\mathfrak{G}_1, M_1) & \to & H^1(\mathfrak{D}_{\tilde{x}_1}, M_1) & \to & H^1(\mathfrak{I}_{\tilde{x}_1}, M_1) \\ \uparrow & & \uparrow & & \uparrow \\ H^1(\mathfrak{G}_2, M_2) & \to & H^1(\mathfrak{D}_{\tilde{x}_2}, M_2) & \to & H^1(\mathfrak{I}_{\tilde{x}_2}, M_2), \end{array}$$

where the horizontal arrows are natural restriction maps and the vertical arrows are induced by (σ, τ^{-1}). By Kummer theory, this diagram can be identified with the natural commutative diagram

$$\begin{array}{ccccc} (K_1^\times)^{\wedge p'} & \to & ((K_1)_{x_1}^\wedge)^{\wedge p'} & \xrightarrow{\mathrm{ord}_{x_1}} & \hat{\mathbb{Z}}^{p'} \\ \uparrow & & \uparrow & & \uparrow \\ (K_2^\times)^{\wedge p'} & \to & ((K_2)_{x_2}^\times)^{\wedge p'} & \xrightarrow{\mathrm{ord}_{x_2}} & \hat{\mathbb{Z}}^{p'}, \end{array} \tag{4.4}$$

where the left horizontal arrows in the two rows arise from natural field homomorphisms $K_1 \to (K_1)_{x_1}$ and $K_2 \to (K_2)_{x_2}$ and the vertical arrows are induced by (σ, τ^{-1}). Further, the kernels of

$$((K_1)_{x_1}^\times)^{\wedge p'} \xrightarrow{\mathrm{ord}_{x_1}} \hat{\mathbb{Z}}^{p'} \quad \text{and} \quad ((K_2)_{x_2}^\times)^{\wedge p'} \xrightarrow{\mathrm{ord}_{x_2}} \hat{\mathbb{Z}}^{p'}$$

are naturally identified with

$$H^1(G_{k(x_1)}, M_1) = (k(x_1)^\times)^{\wedge p'} = k(x_1)^\times \text{ and } H^1(G_{k(x_2)}, M_2) = (k(x_2)^\times)^{\wedge p'} = k(x_2)^\times,$$

respectively. Thus, in particular, the homomorphism $((K_2)_{x_2}^\times)^{\wedge p'} \to ((K_1)_{x_1}^\times)^{\wedge p'}$ naturally induces a homomorphism $\iota_{x_1} : k(x_2)^\times \to k(x_1)^\times$ that is identified with the homomorphism $H^1(G_{k(x_2)}, M_2) \to H^1(G_{k(x_1)}, M_1)$ induced by (σ, τ^{-1}). Here, the last homomorphism is injective by the fact $H^0(H_{k(x_1)}, M_2) = 0$, where $H_{k(x_1)}$ stands for the (isomorphic) image of $G_{k(x_1)}$ in $G_{k(x_2)}$, which is open in $G_{k(x_2)}$.

We have two natural field homomorphisms $K_1 \to K_1^{p^{-n}}$: the first one is a natural embedding $i : K_1 \hookrightarrow K_1^{p^{-n}}$ of degree p^n and the second one is the isomorphism $j : K_1 \xrightarrow{\sim} K_1^{p^{-n}}$ induced by the p^{-n}-th power map. According to these, we obtain

two scheme morphisms $X_1^{p^{-n}} \to X_1$, where $X_1^{p^{-n}}$ stands for the integral closure of X_1 in $K_1^{p^{-n}}$. First, for closed points, these two morphisms give the same bijection

$$\pi : \Sigma_{X_1^{p^{-n}}} \xrightarrow{\sim} \Sigma_{X_1}.$$

Let $x_1 \in \Sigma_{X_1}$ and set $x_1^{p^{-n}} \overset{\text{def}}{=} \pi^{-1}(x_1)$. The two field homomorphisms i and j induce two isomorphisms $k(x_1) \to k(x_1^{p^{-n}})$ of residue fields, which we shall denote by $\bar{i}(x_1)$ and $\bar{j}(x_1)$, respectively. Then we have $\bar{i}(x_1) = F^n \circ \bar{j}(x_1)$, where F stands for the pth power Frobenius map. Now, for valuations of functions, we have

$$\mathrm{ord}_{x_1^{p^{-n}}} \circ i = p^n \,\mathrm{ord}_{x_1}, \quad \mathrm{ord}_{x_1^{p^{-n}}} \circ j = \mathrm{ord}_{x_1}.$$

Finally, for values of functions, we have

$$i(f)(x_1^{p^{-n}}) = \bar{i}(x_1)(f(x_1)), \quad j(f)(x_1^{p^{-n}}) = \bar{j}(x_1)(f(x_1))$$

for each $f \in K_1^\times$ with $\mathrm{ord}_{x_1}(f) \geq 0$. Thus, in particular, $i(f)(x_1^{p^{-n}}) = j(f)(x_1^{p^{-n}})^{p^n}$.

Lemma 4.14. *Let $\gamma : K_2^\times \hookrightarrow (K_1^\times)^{p^{-n}}$ be the injective homomorphism in Lemma 4.13. Let $x_1 \in \Sigma_{X_1}$ and set $x_2 \overset{\text{def}}{=} \phi(x_1) \in \Sigma_{X_2}$. Then*:

(i) *For each $g \in K_2^\times$, we have*

$$\mathrm{ord}_{x_1^{p^{-n}}}(\gamma(g)) = p^n e_{x_1} \,\mathrm{ord}_{x_2}(g).$$

(*Namely, γ is order-preserving with respect $\pi^{-1} \circ \phi$. See Definition 5.1.*)

(ii) *For each $g \in K_2^\times$ with $\mathrm{ord}_{x_2}(g) = 0$, we have $(\gamma(g))(x_1^{p^{-n}}) = i(x_1)(\iota_{x_1}(g(x_2)))$.* (*Namely, γ is value-preserving with respect $\pi^{-1} \circ \phi$ and*

$$\{i(x_1) \circ \iota_{x_1}\}_{x_1^{p^{-n}} \in \Sigma_{X_1^{p^{-n}}}}.$$

See Definition 5.2.)

Proof. (i) and (ii) follow immediately from the commutativity of diagrams (4.3) and (4.4). □

Fix a prime number $l \neq p$. For each $i = 1, 2$, let k_i^l be the (unique) $\mathbb{Z}_l$-extension of k_i, set $K_i^l \overset{\text{def}}{=} K_i k_i^l$, and write X_i^l for the normalization of X_i in K_i^l. (Thus, $X_i^l = X_i \times_{k_i} k_i^l$.) Then the p-primary abelian subgroup $J_{X_i}(k_i^l)\{p\}$ of $J_{X_i}(k_i^l)$ is finite for $i = 1, 2$. (See, for example, [Rosen 2002, Theorem 11.6] or [Saïdi and Tamagawa 2009, proof of Theorem 3.7].) So, write p^{n_0} for the exponent of $J_{X_1}(k_1^l)\{p\}$. By passing to the limit over the finite extensions of k_i contained in k_i^l for $i = 1, 2$ (see Lemma 4.13(ii)), we get a natural embedding $(K_2^l)^\times \hookrightarrow ((K_1^l)^\times)^{p^{-n_0}}$. Now we apply a result from Section 5. (Observe that there are no vicious circles since the discussion of Section 5 does not depend on the contents of earlier sections.) More specifically, by Lemma 4.14 and Proposition 5.3,

the embedding $(K_2^l)^\times \hookrightarrow ((K_1^l)^\times)^{p^{-n_0}}$ above arises from a (uniquely determined) embedding $K_2^l \hookrightarrow (K_1^l)^{p^{-n_0}}$ of fields. This embedding of fields restricts to the original embedding of multiplicative groups $K_2^\times \hookrightarrow (K_1^\times)^{p^{-n}}$. Thus, we conclude that this original embedding also arises from a (uniquely determined) embedding $K_2 \hookrightarrow K_1^{p^{-n}}$ of fields.

Define the subfields $K_2 \supset K_2' \supset K_2''$ to be the inverse images of the subfields $K_1^{p^{-n}} \supset K_1 \supset K_1^p$ in K_2. By Lemma 4.13(ii), there exists a finite subset $S \subset K_2$ such that $K_2 = \bigcup_{\alpha \in S} K_2'\alpha$. Since K_2 is an infinite field, this implies that K_2' is also an infinite field and that K_2 must be of dimension 1 as a K_2'-vector space. Namely, $K_2 = K_2'$, or, equivalently, the above field homomorphism $K_2 \hookrightarrow K_1^{p^{-n}}$ induces a field homomorphism $\gamma : K_2 \hookrightarrow K_1$. Next, again by Lemma 4.13(ii), we have $[K_2^\times : (K_2'')^\times] > 1$, that is, $K_2 \supsetneq K_2''$. Equivalently, the field homomorphism $K_2 \hookrightarrow K_1$ is separable.

Passing to the open subgroups $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ with $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$ and applying the above arguments to $\mathfrak{H}_1 \overset{\sigma}{\to} \mathfrak{H}_2$, we obtain naturally a (separable) field homomorphism $\tilde{\gamma} : \tilde{K}_2 \to \tilde{K}_1$ which restricts to the above (separable) field homomorphism $K_2 \to K_1$.

Lemma 4.15 (compatibility with the Galois action). *Let* $g_1 \in \mathfrak{G}_1$, *and let* $g_2 \overset{def}{=} \sigma(g_1) \in \mathfrak{G}_2$. *Then the following diagram is commutative*:

$$\begin{array}{ccc} \tilde{K}_2 & \xrightarrow{\tilde{\gamma}} & \tilde{K}_1 \\ {\scriptstyle g_2}\uparrow & & \uparrow{\scriptstyle g_1} \\ \tilde{K}_2 & \xrightarrow{\tilde{\gamma}} & \tilde{K}_1. \end{array}$$

Proof. Let $\mathfrak{H}_2 \subset \mathfrak{G}_2$ be an open normal subgroup and set

$$\mathfrak{H}_1 \overset{\text{def}}{=} \sigma^{-1}(\mathfrak{H}_2),$$

which is an open normal subgroup of $\mathfrak{G}_1$. For $i = 1, 2$, let F_i/K_i be the finite Galois subextension of $\tilde{K}_i/K_i$ corresponding to $\mathfrak{H}_i \subset \mathfrak{G}_i$, and denote by Y_i the integral closure of X_i in F_i. We have commutative diagrams

$$\begin{array}{ccc} H^1(\mathfrak{H}_2, M_2) & \to & H^1(\mathfrak{H}_1, M_1) \\ {\scriptstyle g_2}\uparrow & & \uparrow{\scriptstyle g_1} \\ H^1(\mathfrak{H}_2, M_2) & \to & H^1(\mathfrak{H}_1, M_1), \end{array}$$

where $g_i : H^1(\mathfrak{H}_i, M_i) \to H^1(\mathfrak{H}_i, M_i)$ denotes the automorphism induced by the action of g_i on $\mathfrak{H}_i$, and the horizontal maps are naturally induced by (σ, τ^{-1}) (see

Lemma 4.11(i)), and

$$\begin{array}{ccc} \widehat{\mathrm{Div}}_{Y_2} & \longrightarrow & \widehat{\mathrm{Div}}_{Y_1} \\ {\scriptstyle g_2}\uparrow & & \uparrow{\scriptstyle g_1} \\ \widehat{\mathrm{Div}}_{Y_2} & \longrightarrow & \widehat{\mathrm{Div}}_{Y_1}, \end{array}$$

where the map $g_i : \widehat{\mathrm{Div}}_{Y_i} \to \widehat{\mathrm{Div}}_{Y_i}$ is the automorphism naturally induced by the action of g_i on Y_i (see Remark 4.2(iv)). Further, the above diagrams commute with each other, via the maps $H^1(\mathfrak{H}_i, M_i) \to \widehat{\mathrm{Div}}_{Y_i}$ in diagram (4.3) for $i = 1, 2$. Note that in the above diagrams the map $g_i : H^1(\mathfrak{H}_i, M_i) \to H^1(\mathfrak{H}_i, M_i)$ restricted to $F_i^\times$ coincides with the automorphism $g_i : F_i^\times \to F_i^\times$. Therefore, we deduce this commutative diagram, from which the assertion follows:

$$\begin{array}{ccc} F_2^\times & \xrightarrow{\tilde{\gamma}} & F_1^\times \\ {\scriptstyle g_2}\uparrow & & \uparrow{\scriptstyle g_1} \\ F_2^\times & \xrightarrow{\tilde{\gamma}} & F_1^\times. \end{array}$$

□

Finally, we shall prove the uniqueness of the field homomorphism $\tilde{\gamma} : \tilde{K}_2 \to \tilde{K}_1$ that is Galois-compatible with respect to σ and restricts to a separable homomorphism $K_2 \to K_1$. In the profinite case, this uniqueness follows formally from the uniqueness in the assertion of the Isom-form proved in [Uchida 1977], as in the case of rigid homomorphisms in Section 3. (Observe that $\tilde{\gamma} : \tilde{K}_2 \to \tilde{K}_1$ is then an isomorphism.) In general, however, we need some arguments which are not entirely formal, as follows.

So, let $\tilde{\gamma}' : \tilde{K}_2 \to \tilde{K}_1$ be another such field homomorphism. The field homomorphisms $\tilde{\gamma}$ and $\tilde{\gamma}'$ induce field isomorphisms $\bar{k}_2 \xrightarrow{\sim} \bar{k}_1$, say, $\bar{\gamma}$ and $\bar{\gamma}'$, respectively, which are Galois-compatible with respect to σ. We may write $\bar{\gamma}' = \varphi_1^\alpha \circ \bar{\gamma}$ for some $\alpha \in \hat{\mathbb{Z}}$, where $\varphi_1 \in \mathrm{Gal}(\bar{k}_1/\mathbb{F}_p)$ stands for the pth power Frobenius element. Further, the isomorphisms $\bar{\gamma}$ and $\bar{\gamma}'$ induce $\hat{\mathbb{Z}}^{p'}$-module isomorphisms $M_2 \xrightarrow{\sim} M_1$, say, τ^{-1} and $(\tau')^{-1}$, respectively, which are Galois-compatible with respect to σ. Thus, we have $(\tau')^{-1} = [p^\alpha] \circ \tau^{-1}$. By Kummer theory, we have the commutative diagrams

$$\begin{array}{ccc} K_1^\times & \hookrightarrow & H^1(\mathfrak{G}_1, M_1) \\ {\scriptstyle \gamma}\uparrow & & \uparrow{\scriptstyle (\sigma, \tau^{-1})} \\ K_2^\times & \hookrightarrow & H^1(\mathfrak{G}_2, M_2), \end{array} \quad \text{and} \quad \begin{array}{ccc} K_1^\times & \hookrightarrow & H^1(\mathfrak{G}_1, M_1) \\ {\scriptstyle \gamma'}\uparrow & & \uparrow{\scriptstyle (\sigma, (\tau')^{-1})} \\ K_2^\times & \hookrightarrow & H^1(\mathfrak{G}_2, M_2). \end{array}$$

Thus, for each $g \in K_2^\times$, we have $\gamma'(g) = \gamma(g)^{p^\alpha}$ in $(K_1^\times)^{\wedge p'}$. Since both γ and γ' are field homomorphisms, we deduce that $p^\alpha \in \mathbb{Q}_{>0}$, by taking a nonconstant function g and considering valuations at suitable points. Thus, $\alpha \in \mathbb{Z}$, by [Chevalley

1951, théorème 1]. Exchanging γ and γ' if necessary, we may assume that $\alpha \geq 0$. Thus, $\gamma' = F^{\alpha} \circ \gamma$, where F stands for the pth power Frobenius map. Since γ' is separable, we conclude $\alpha = 0$, and hence $\gamma' = \gamma$. Passing to the open subgroups $\mathfrak{H}_1 \subset \mathfrak{G}_1$, $\mathfrak{H}_2 \subset \mathfrak{G}_2$ with $\sigma(\mathfrak{H}_1) \subset \mathfrak{H}_2$, we conclude that $\tilde{\gamma} : \tilde{K}_2 \to \tilde{K}_1$ is unique.

Thus, the proof of Theorem 4.8 is completed. □

5. Recovering the additive structure

This section is devoted to the proof of Proposition 5.3, which was used in the proof of Theorem 4.8. We shall first axiomatize the set-up. We will use the following notations. For $i \in \{1, 2\}$, let X_i be a proper, smooth, geometrically connected curve over a field k_i of characteristic $p_i \geq 0$. Let $K_i = K_{X_i}$ be the function field of X_i, and Σ_{X_i} the set of closed points of X_i. Let

$$\iota : K_2^{\times} \hookrightarrow K_1^{\times}$$

be an embedding between multiplicative groups, which we extend to an embedding $\iota : K_2 \hookrightarrow K_1$ between multiplicative monoids by setting $\iota(0) = 0$. We assume that we are given a map

$$\phi : \Sigma_{X_1} \to \Sigma_{X_2}$$

that has finite fibers, that is, for any $x_2 \in X_2$, the inverse image $\phi^{-1}(x_2) \subset \Sigma_{X_1}$ is a finite set.

Definition 5.1 (order-preserving maps). The map $\iota : K_2 \to K_1$ is called order-preserving with respect to the map ϕ if, for any $x_2 \in \Sigma_{X_2}$ and any $x_1 \in \phi^{-1}(x_2)$, there exists a positive integer $e_{x_1x_2} > 0$ such that the following diagram commutes:

$$\begin{array}{ccc} K_1 & \xrightarrow{\mathrm{ord}_{x_1}} & \mathbb{Z} \cup \{\infty\} \\ {\scriptstyle \iota}\uparrow & & \uparrow{\scriptstyle [e_{x_1x_2}]} \\ K_2 & \xrightarrow{\mathrm{ord}_{x_2}} & \mathbb{Z} \cup \{\infty\}. \end{array}$$

Here, $[e_{x_1x_2}]$ denotes the map of multiplication by $e_{x_1x_2}$ in $\mathbb{Z}$, which we extend naturally to $\mathbb{Z} \cup \{\infty\}$ by mapping ∞ to ∞.

Next, we assume that the map $\iota : K_2 \to K_1$ is order-preserving with respect to the map $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$. Further, we assume that we are given an embedding

$$\iota_{x_1x_2} : k(x_2)^{\times} \hookrightarrow k(x_1)^{\times}$$

between multiplicative groups for any $x_2 \in \Sigma_{X_2}$ and any $x_1 \in \phi^{-1}(x_2)$.

Definition 5.2 (value-preserving maps). The map $\iota : K_2 \hookrightarrow K_1$ is called value-preserving with respect to the map ϕ and the embeddings $\{\iota_{x_1x_2}\}_{(x_1,x_2)}$, where

(x_1, x_2) runs over all pairs of points $x_2 \in \Sigma_{X_2}$ and $x_1 \in \phi^{-1}(x_2)$ if, for any $f_2 \in K_2^\times$ and any point $x_2 \in \Sigma_{X_2}$ such that $x_2 \cap \mathrm{Supp}\,\mathrm{div}(f_2) = \varnothing$, we have

$$\iota_{x_1,x_2}(f_2(x_2)) = \iota(f_2)(x_1),$$

where $f_2(x_2)$ denotes the value of f_2 at x_2 and $\iota(f_2)(x_1)$ the value of $\iota(f_2)$ at x_1.

If $\iota : K_2 \hookrightarrow K_1$ is value-preserving, it particularly fits into the commutative diagram

$$\begin{array}{ccc} k(x_2)^\times & \xrightarrow{\iota_{x_1x_2}} & k(x_1)^\times \\ \uparrow & & \uparrow \\ k_2^\times & \xrightarrow{\iota} & k_1^\times, \end{array}$$

where the vertical maps are the natural embeddings. (Observe that ι maps k_2 into k_1, by the order-preserving assumption.)

Proposition 5.3 (recovering the additive structure). *Assume that the embedding $\iota : K_2 \hookrightarrow K_1$ is order-preserving with respect to the map ϕ, and value-preserving with respect to the map ϕ and the embeddings $\{\iota_{x_1x_2}\}_{(x_1,x_2)}$, where the pair (x_1, x_2) runs over all points $x_2 \in \Sigma_{X_2}$ and $x_1 \in \phi^{-1}(x_2)$. Assume further that $X_2(k_2)$ is an infinite set. Then the map ι is additive* (*and hence, a homomorphism of fields*).

Proof. First, we shall prove that $\iota^{-1}(k_1) = k_2$. (Namely, $f \in K_2$ is constant if and only if $\iota(f) \in K_1$ is constant.) Indeed, set $F_2 \overset{\text{def}}{=} \iota^{-1}(k_1)$. Note that $k_i^\times$ coincides with the set of functions in $K_i^\times$ with neither zeroes nor poles (or, equivalently, with no poles) anywhere in Σ_{X_i}. Now, by the order-preserving property of ι, $F_2 \smallsetminus \{0\}$ coincides with the set of functions in $K_2^\times$ with neither zeroes nor poles (or, equivalently, with no poles) in $\phi(\Sigma_{X_1}) \subset \Sigma_{X_2}$. It follows easily from this characterization that F_2 is a subfield of K_2 containing k_2. Since K_2 is a function field of one variable over k_2 and since k_2 is algebraically closed in K_2, we have either $F_2 = k_2$ or that F_2 is also a function field of one variable over k_2. Suppose the latter, and let W_2 be the (proper, smooth, geometrically connected) curve over k_2 with function field F_2. Take any point $x_1 \in \Sigma_{X_1}$ and let $w \in \Sigma_{W_2}$ be the image of x_1 under the composite map

$$\Sigma_{X_1} \xrightarrow{\phi} \Sigma_{X_2} \to \Sigma_{W_2},$$

where the second map arises from the cover $X_2 \to W_2$ corresponding to the extension L_2/F_2. Now, by the Riemann–Roch theorem, there exists a function $f \in F_2$ having a pole at w. By the order-preserving property of ι, the function $\iota(f) \in K_1$ must have a pole at x_1. This contradicts the definition of F_2. Therefore, we must have $F_2 = k_2$, as desired.

We prove that $\phi : \Sigma_{X_1} \to \Sigma_{X_2}$ is surjective. Suppose otherwise and take $x_2 \in \Sigma_{X_2} \smallsetminus \phi(\Sigma_{X_1}) \neq \varnothing$. By the Riemann–Roch theorem, there exists a nonconstant

function $f \in K_2$ such that the pole divisor of f is supported on $x_2 \in \Sigma_{X_2}$. Then, by the order-preserving property of ι, the function $\iota(f) \in K_1$ admits no poles, and hence $\iota(f) \in k_1$. As $\iota^{-1}(k_1) = k_2$, we thus have $f \in k_2$, which is absurd.

The rest of the proof is similar to the proof of [Saïdi and Tamagawa 2009, Proposition 4.4], where ϕ is a bijection. We first prove that ι restricted to k_2 is additive. Again by the Riemann–Roch theorem, there exists a nonconstant function $f \in K_2$ such that the pole divisor $\mathrm{div}(f)_\infty$ of f is supported on a unique point $x_2 \in \Sigma_{X_2}$: $\mathrm{div}(f)_\infty = nx_2$, with $n > 0$. For a nonzero constant $\alpha \in k_2$ we analyze the divisor of the function $\iota(f+\alpha) - \iota(f)$. We claim that

$$\mathrm{Supp}\ \mathrm{div}(\iota(f+\alpha) - \iota(f)) \subset \phi^{-1}(x_2).$$

Indeed, if $y_1 \in \Sigma_{X_1}$ is such that $y_2 \overset{\mathrm{def}}{=} \phi(y_1) \neq x_2$, then $\mathrm{ord}_{y_1}(\iota(f+\alpha)) \geq 0$, and $\mathrm{ord}_{y_1}(\iota(f)) \geq 0$. Moreover, $\iota(f+\alpha)(y_1) \neq \iota(f)(y_1)$, as follows from the value-preserving assumption, since $(f+\alpha)(y_1) \neq f(y_1)$. Thus,

$$y_1 \notin \mathrm{Supp}\ \mathrm{div}(\iota(f+\alpha) - \iota(f))$$

and our claim follows. Further, if $x_1 \in \phi^{-1}(x_2)$ is a pole of $\iota(f+\alpha) - \iota(f)$, we have $|\mathrm{ord}_{x_1}(\iota(f+\alpha) - \iota(f))| \leq ne_{x_1x_2}$. We deduce easily from this that there are only finitely many possibilities for the divisor $\mathrm{div}(\iota(f+\alpha) - \iota(f))$. Since k_2 is infinite ($X_2(k_2)$ being infinite), there exists an infinite subset $A \subset k_2^\times$ such that $\mathrm{div}(\iota(f+\alpha) - \iota(f))$ is constant, for all $\alpha \in A$.

Let $\alpha \neq \beta$ be elements of A. Then $\mathrm{div}(\iota(f+\alpha) - \iota(f)) = \mathrm{div}(\iota(f+\beta) - \iota(f))$, which implies

$$\frac{\iota(f+\beta) - \iota(f)}{\iota(f+\alpha) - \iota(f)} = c \in k_1^\times.$$

Observe that $\iota(f+\alpha) - \iota(f) \neq 0$, by the injectivity of ι. Further, $c = \iota(\beta)/\iota(\alpha)$, as is easily seen by evaluating the function

$$\frac{\iota(f+\beta) - \iota(f)}{\iota(f+\alpha) - \iota(f)}$$

at a zero of the nonconstant function $\iota(f)$. Thus, we have $\iota(\beta)(\iota(f+\alpha) - \iota(f)) = \iota(\alpha)(\iota(f+\beta) - \iota(f))$, which is equivalent to

$$\iota(f)(\iota(\alpha) - \iota(\beta)) = \iota(\alpha)\iota(f+\beta) - \iota(\beta)\iota(f+\alpha).$$

Let

$$g \overset{\mathrm{def}}{=} \frac{\beta(f+\alpha)}{(\alpha-\beta)f} = \frac{\beta(1+\alpha f^{-1})}{(\alpha-\beta)}.$$

Note that g is a nonconstant function, since f is nonconstant. We have

$$g + 1 = \frac{\beta(f+\alpha)}{(\alpha-\beta)f} + \frac{(\alpha-\beta)f}{(\alpha-\beta)f} = \frac{\beta\alpha + \alpha f}{\alpha f - \beta f} = \frac{\alpha(\beta+f)}{(\alpha-\beta)f}.$$

Dividing this equality by $\iota(\alpha-\beta)\iota(f)\neq 0$, we obtain

$$\frac{\iota(\alpha)-\iota(\beta)}{\iota(\alpha-\beta)}=\frac{\iota(\alpha)\iota(f+\beta)-\iota(\beta)\iota(\alpha+f)}{\iota(\alpha-\beta)\iota(f)}.$$

Thus,

$$\frac{\iota(\alpha)-\iota(\beta)}{\iota(\alpha-\beta)}=\frac{\iota(\alpha)\iota(f+\beta)}{\iota(\alpha-\beta)\iota(f)}-\frac{\iota(\beta)\iota(\alpha+f)}{\iota(\alpha-\beta)\iota(f)},$$

which equals $\iota(g+1)-\iota(g)$. Further,

$$\frac{\iota(\alpha)-\iota(\beta)}{\iota(\alpha-\beta)}=1,$$

as follows by evaluating the function $\iota(g+1)-\iota(g)$ at a zero of the nonconstant function $\iota(g)$. Thus,

$$\iota(g+1)=\iota(g)+1.$$

Take any $\zeta\in k_2$. Then, evaluating this equation at a zero of $\iota(g-\zeta)$, we obtain $\iota(\zeta+1)=\iota(\zeta)+1$. Now, for any $\xi,\eta\in k_2$, we have $\iota(\xi+\eta)=\iota(\xi)+\iota(\eta)$. Indeed, if $\eta=0$, this follows from $\iota(0)=0$. If $\eta\neq 0$, we have

$$\iota(\xi+\eta)=\iota\Big(\frac{\xi}{\eta}+1\Big)\iota(\eta)=\Big(\iota\Big(\frac{\xi}{\eta}\Big)+1\Big)\iota(\eta)=\iota(\xi)+\iota(\eta).$$

Thus, $\iota|_{k_2}$ is additive.

From this it follows easily that ι itself is additive. Indeed, let h and l be any elements of K_2, and let us prove $\iota(h+l)=\iota(h)+\iota(l)$. Take any $x_2\in X_2(k_2)$ which is neither a pole of h nor a pole of l. Then, evaluating at any $x_1\in\phi^{-1}(x_2)$, we obtain

$$\begin{aligned}(\iota(h+l))(x_1)&=\iota_{x_1x_2}((h+l)(x_2))\\&=\iota_{x_1x_2}(h(x_2)+l(x_2))\\&=\iota(h(x_2)+l(x_2))\\&=\iota(h(x_2))+\iota(l(x_2))\\&=\iota_{x_1x_2}(h(x_2))+\iota_{x_1x_2}(l(x_2))\\&=(\iota(h))(x_1)+(\iota(l))(x_1)\\&=(\iota(h)+\iota(l))(x_1),\end{aligned}$$

where the first and the sixth equalities follow from the value-preserving property, the second and the last equalities follow from the additivity of the evaluation maps, the third and the fifth equalities follow from the value-preserving property and the fact that $h(x_2), l(x_2)\in k_2$ (since $x_2\in X_2(k_2)$), and the fourth equality follows from the additivity of $\iota|_{k_2}$. Now, since there are infinitely many such x_1 by assumption, the equality $\iota(h+l)=\iota(h)+\iota(l)$ must hold. Thus, Proposition 5.3 is proved. □

Acknowledgement

This work was done during a visit of Saïdi's to the Research Institute for Mathematical Sciences of Kyoto University, whose staff he would very much like to thank for their hospitality.

References

[Chevalley 1951] C. Chevalley, "Deux théorèmes d'arithmétique", *J. Math. Soc. Japan* **3** (1951), 36–44. MR 13,440a Zbl 0044.03001

[Engler and Koenigsmann 1998] A. J. Engler and J. Koenigsmann, "Abelian subgroups of pro-p Galois groups", *Trans. Amer. Math. Soc.* **350**:6 (1998), 2473–2485. MR 98h:12004 Zbl 0999.12004

[Engler and Nogueira 1994] A. J. Engler and J. B. Nogueira, "Maximal abelian normal subgroups of Galois pro-2-groups", *J. Algebra* **166**:3 (1994), 481–505. MR 95h:12004 Zbl 0809.12004

[Fried and Jarden 1986] M. D. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Math. und ihrer Grenzgebiete (3) **11**, Springer, Berlin, 1986. MR 89b:12010 Zbl 0625.12001

[Grothendieck and Raynaud 1971] A. Grothendieck and M. Raynaud, *Revêtements étales et groupe fondamantal*, edited by A. Grothendieck, Lecture Notes in Mathematics **224**, Springer, Berlin, 1971. MR 50 #7129 Zbl 0234.14002

[Harbater 1995] D. Harbater, "Fundamental groups and embedding problems in characteristic p", pp. 353–369 in *Recent developments in the inverse Galois problem* (Seattle, 1993), edited by M. D. Fried et al., Contemp. Math. **186**, Amer. Math. Soc., Providence, RI, 1995. MR 97b:14035 Zbl 0858.14013

[Koenigsmann 2003] J. Koenigsmann, "Encoding valuations in absolute Galois groups", pp. 107–132 in *Valuation theory and its applications* (Saskatoon, SK, 1999), vol. 2, edited by F.-V. Kuhlmann et al., Fields Institute Commun. **33**, Amer. Math. Soc., Providence, 2003. MR 2004m:12012 Zbl 1050.12004

[Mochizuki 1999] S. Mochizuki, "The local pro-p anabelian geometry of curves", *Invent. Math.* **138**:2 (1999), 319–423. MR 2000j:14037 Zbl 0935.14019

[Mochizuki 2003] S. Mochizuki, "Topics surrounding the anabelian geometry of hyperbolic curves", pp. 119–165 in *Galois groups and fundamental groups* (Berkeley, 1999), edited by L. Schneps, Math. Sci. Res. Inst. Publ. **41**, Cambridge Univ. Press, 2003. MR 2004m:14052 Zbl 1053.14029

[Mochizuki 2005] S. Mochizuki, "Galois sections in absolute anabelian geometry", *Nagoya Math. J.* **179** (2005), 17–45. MR 2006d:14022 Zbl 1129.14042

[Mochizuki 2007] S. Mochizuki, "Absolute anabelian cuspidalizations of proper hyperbolic curves", *J. Math. Kyoto Univ.* **47**:3 (2007), 451–539. MR 2009d:14024 Zbl 1143.14305

[Neukirch 1969a] J. Neukirch, "Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper", *Invent. Math.* **6** (1969), 296–314. MR 39 #5528 Zbl 0192.40102

[Neukirch 1969b] J. Neukirch, "Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen", *J. Reine Angew. Math.* **238** (1969), 135–147. MR 41 #3450 Zbl 0201.05901

[Pop 1994] F. Pop, "On Grothendieck's conjecture of birational anabelian geometry", *Ann. of Math.* (2) **139**:1 (1994), 145–182. MR 94m:12007 Zbl 0814.14027

[Pop 1995] F. Pop, "Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture", *Invent. Math.* **120**:3 (1995), 555–578. MR 96k:14011 Zbl 0842.14017

[Pop 2002] F. Pop, "The birational anabelian conjecture revisited", preprint, 2002, available at http://www.math.upenn.edu/~pop/Research/files-Res/finit-mf.pdf.

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer, New York, 2002. MR 2003d:11171 Zbl 1043.11079

[Saïdi and Tamagawa 2009] M. Saïdi and A. Tamagawa, "A prime-to-p version of Grothendieck's anabelian conjecture for hyperbolic curves over finite fields of characteristic $p > 0$", *Publ. Res. Inst. Math. Sci.* **45**:1 (2009), 135–186. MR 2010j:14046 Zbl 1188.14016

[Serre 1967] J.-P. Serre, "Local class field theory", pp. 128–161 in *Algebraic number theory: Proceedings of an instructional conference* (Brighton, 1965), Academic Press, London, 1967. MR 36 #3753

[Serre 1968] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968. MR 50 #7096 Zbl 1095.11504

[Serre 1994] J.-P. Serre, *Cohomologie galoisienne*, 5th ed., Lecture Notes in Math. **5**, Springer, Berlin, 1994. MR 96b:12010 Zbl 0812.12002

[Szamuely 2004] T. Szamuely, "Groupes de Galois de corps de type fini (d'après Pop)", exposé 923, pp. 403–431 in *Séminaire Bourbaki* 2002/2003, Astérisque **294**, Soc. math. de France, Paris, 2004. MR 2005k:12004 Zbl 1148.12300

[Tamagawa 1997] A. Tamagawa, "The Grothendieck conjecture for affine curves", *Compositio Math.* **109**:2 (1997), 135–194. MR 99a:14035 Zbl 0899.14007

[Uchida 1976] K. Uchida, "Isomorphisms of Galois groups", *J. Math. Soc. Japan* **28**:4 (1976), 617–620. MR 55 #5580 Zbl 0329.12013

[Uchida 1977] K. Uchida, "Isomorphisms of Galois groups of algebraic function fields", *Ann. Math.* (2) **106**:3 (1977), 589–598. MR 57 #273 Zbl 0372.12017

[Uchida 1981] K. Uchida, "Homomorphisms of Galois groups of solvably closed Galois extensions", *J. Math. Soc. Japan* **33**:4 (1981), 595–604. MR 83i:12011 Zbl 0464.12004

Communicated by Hélène Esnault
Received 2009-12-02 Revised 2010-05-01 Accepted 2010-06-06

M.Saidi@exeter.ac.uk *University of Exeter, School of Engineering, Computing and Mathematics, Exeter EX44QF, United Kingdom*

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

ALGEBRA AND NUMBER THEORY 5:2(2011)

msp

Local positivity, multiplier ideals, and syzygies of abelian varieties

Robert Lazarsfeld, Giuseppe Pareschi and Mihnea Popa

We use the language of multiplier ideals in order to relate the syzygies of an abelian variety in a suitable embedding with the local positivity of the line bundle inducing that embedding. This extends to higher syzygies a result of Hwang and To on projective normality.

Introduction

Hwang and To [2010] observed that there is a relation between local positivity on an abelian variety A and the projective normality of suitable embeddings of A. The purpose of this note is to extend their result to higher syzygies, and to show that the language of multiplier ideals renders the computations extremely quick and transparent.

Turning to details, let A be an abelian variety of dimension g, and let L be an ample line bundle on A. Recall that the *Seshadri constant* $\varepsilon(A, L)$ is a positive real number that measures the local positivity of L at any given point $x \in A$: for example, it can be defined by counting asymptotically the number of jets that the linear series $|kL|$ separates at x as $k \to \infty$. We refer to [Lazarsfeld 2004, Chapter 5] for a general survey of the theory, and in particular to Section 5.3 of that book for a discussion of local positivity on abelian varieties.

Our main result is this:

Theorem A. *Assume that*

$$\varepsilon(A, L) > (p+2)g.$$

Then L satisfies property (N_p).

The reader may consult for instance [Lazarsfeld 2004, Chapter 1.8.D], [Green and Lazarsfeld 1987] or [Eisenbud 2005] for the definition of property (N_p) and

The first author's research was partially supported by NSF grant DMS-0652845. The third author's research was partially supported by NSF grant DMS-0758253 and a Sloan Fellowship.
MSC2000: primary 14K05; secondary 14Q20, 14F17.
Keywords: Syzygies, abelian varieties, local positivity, multiplier ideals.

further references. Suffice it to say here that (N_0) holds when L defines a projectively normal embedding of A, while (N_1) means that the homogeneous ideal of A in this embedding is generated by quadrics. For $p > 1$ the condition is that the first p modules of syzygies among these quadrics are generated in minimal possible degree. The result of Hwang and To [2010] is essentially the case $p = 0$ of Theorem A.

In general it is difficult to control Seshadri constants. However, it was shown in [Lazarsfeld 1996] that on an abelian variety they are related to a metric invariant introduced in [Buser and Sarnak 1994]. Specifically, write $A = V/\Lambda$, where V is a complex vector space of dimension g and $\Lambda \subseteq V$ is a lattice. Then L determines a hermitian form $h = h_L$ on V, and the Buser–Sarnak invariant is (the square of) the minimal length with respect to h of a nonzero period of Λ:

$$m(A, L) := \min_{0 \neq \ell \in \Lambda} h_L(\ell, \ell).$$

The main result of [Lazarsfeld 1996] is that

$$\varepsilon(A, L) \geq \frac{\pi}{4} \cdot m(A, L).$$

On the other hand, one can estimate $m(A, L)$ for very general (A, L). In fact, suppose that the polarization L has elementary divisors

$$d_1 \mid d_2 \mid \cdots \mid d_g,$$

and put $d = d(L) = d_1 \cdot \cdots \cdot d_g$. By adapting an argument of Buser–Sarnak in the case of principal polarizations, Bauer [1998] showed that if (A, L) is very general, then

$$m(A, L) \geq \frac{2^{1/g}}{\pi} \sqrt[g]{d \cdot g!}.$$

Therefore we obtain:

Corollary B. *Assume that*

$$d(L) > \frac{4^g (p+2)^g g^g}{2g!}.$$

Then (N_p) holds for very general (A, L) of the given type.

The essential interest in statements of this sort occurs when L is primitive (that is, $d_1 = 1$), or at least when d_1 is small: as far as we know, our result is the first to give statements for higher syzygies of primitive line bundles in large dimension. By contrast, if L is a suitable multiple of some ample line bundle, then much stronger statements are known. Most notably, the second author proved in [Pareschi 2000] that (N_p) always holds as soon as $d_1 \geq p + 3$. This was strengthened and systematized in [Pareschi and Popa 2003; 2004], while (for $p = 0$) other statements appear in [Iyer 2003] and [Fuentes García 2005].

We conclude this introduction by sketching a proof of the theorem of [Hwang and To 2010] via the approach of the present paper. Following a time-honored device, one considers the diagonal $\Delta \subseteq A \times A$, with ideal sheaf $\mathcal{I}_\Delta$. Writing

$$L \boxtimes L = \mathrm{pr}_1^* L \otimes \mathrm{pr}_2^* L$$

for the exterior product of L with itself, the essential point is to prove

$$H^1\big(A \times A, L \boxtimes L \otimes \mathcal{I}_\Delta\big) \;=\; 0. \tag{*}$$

Hwang and To [2010] achieve this by establishing a somewhat delicate upper bound on the volume of a one-dimensional analytic subvariety of a tubular neighborhood of Δ (or, more generally, of a tubular neighborhood of any subtorus of an abelian variety). This allows them to control the positivity required to apply vanishing theorems on the blow-up of $A \times A$ along Δ. While their calculation is of substantial independent interest, for the task at hand it is considerably quicker to deduce (*) directly from Nadel vanishing.

Specifically, using the hypothesis that $\varepsilon(A, L) > 2g$, a standard argument (see Lemma 1.2) shows that for suitable $0 < c \ll 1$, one can construct an effective $\mathbb{Q}$-divisor

$$E_0 \equiv_{\mathrm{num}} \frac{1-c}{2} L$$

on A whose multiplier ideal vanishes precisely at the origin: $\mathcal{J}(A, E_0) = \mathcal{I}_0$. Now consider the difference map

$$\delta : A \times A \to A, \qquad (x, y) \mapsto x - y,$$

and set $E = \delta^* E_0$. Since forming multiplier ideals commutes with pullback under smooth morphisms, we have on the one hand

$$\mathcal{J}(A \times A, E) = \delta^* \mathcal{J}(A, E_0) = \mathcal{I}_\Delta.$$

On the other hand, one knows that

$$L^2 \boxtimes L^2 = \delta^*(L) \otimes N \tag{**}$$

for a suitable nef line bundle N on $A \times A$. Thanks to our choice of E_0, this implies that $(L \boxtimes L)(-E)$ is ample. Therefore Nadel vanishing gives (*), as required.

The proof of the general case of Theorem A proceeds along similar lines. Following an idea going back to Green [1984], one works on the $(p+2)$-fold product of A, where one has to check a vanishing involving the ideal sheaf of a union of pairwise diagonals.[1] To realize this as a multiplier ideal, we pull back a suitable

[1]The possibility of applying vanishing theorems on a blow-up to verify Green's criterion was noted already in [Bertram et al. 1991, Remark on p. 600]. Nowadays one can invoke the theory of [Li 2009] to control the blow-ups involved: the pairwise diagonals $\Delta_{0,1}, \ldots, \Delta_{0,p+1}$ form a building

divisor under a multisubtraction map: this is carried out in Section 1. The positivity necessary for Nadel vanishing is verified using an analogue of (∗∗) established in Section 2. Finally, Section 3 contains some complements and variants, including a criterion for L to define an embedding in which the homogeneous coordinate ring of A is Koszul.

For applications of Nadel vanishing, one typically has to estimate the positivity of formal twists of line bundles by $\mathbb{Q}$-divisors. To this end, we allow ourselves to be a little sloppy in mixing additive and multiplicative notation. Thus, given a $\mathbb{Q}$-divisor D and a line bundle L, the statement $D \equiv_{\text{num}} bL$ is intended to mean that D is numerically equivalent to $b \cdot c_1(L)$. Similarly, to say that $(bL)(-D)$ is ample indicates that $b \cdot c_1(L) - D$ is an ample numerical class. We trust that no confusion will result.

1. Proof of Theorem A

As in the Introduction, let A be an abelian variety of dimension g, and let L be an ample line bundle on A.

We start by recalling a geometric criterion that guarantees property (N_p) in our setting. Specifically, form the $(p+2)$-fold product $X = A^{\times(p+2)}$ of A with itself, and inside X consider the reduced algebraic set

$$\Sigma = \big\{(x_0, \ldots, x_{p+1}) \,|\, x_0 = x_i \text{ for some } 1 \le i \le p+1\big\} = \Delta_{0,1} \cup \Delta_{0,2} \cup \ldots \cup \Delta_{0,p+1}$$

arising as the union of the indicated pairwise diagonals. Thus Σ has $p+1$ irreducible components, each of codimension g in X.

It was observed by Green [1984, §3] that property (N_p) for L is implied by a vanishing on X involving the ideal sheaf of $\mathcal{I}_\Sigma$, generalizing the condition (*) for projective normality. We refer to [Inamdar 1997] for a statement and careful discussion of the criterion in general.[2] In the present situation, it shows that Theorem A is a consequence of the following:

Proposition 1.1. *Assume that $\varepsilon(A, L) > (p+2)g$. Then*

$$H^i\Big(A^{\times(p+2)}, \overset{p+2}{\boxtimes} L \otimes Q \otimes \mathcal{I}_\Sigma\Big) = 0$$

for any nef line bundle Q on X and all $i > 0$.[3]

---

set in the sense of [Li 2009] on the $(p+2)$-fold self product of a smooth variety. However, in the case of abelian varieties treated here, elementary properties of multiplier ideals are used to obviate the need for any blow-ups.

[2] The argument appearing in [Green 1984] is somewhat oversimplified.

[3] As explained in [Inamdar 1997] one actually needs the vanishings

$$H^1\big(A^{\times(p'+2)}, L^q \boxtimes L \boxtimes \cdots \boxtimes L \otimes \mathcal{I}_\Sigma\big) = 0$$

The plan is to deduce the proposition from Nadel vanishing. To this end, it suffices to produce an effective $\mathbb{Q}$-divisor E on X having two properties:

$$\mathcal{J}(X, E) = \mathcal{I}_\Sigma. \tag{1-1}$$

$$\Big(\overset{p+2}{\boxtimes} L\Big)(-E) \text{ is ample.} \tag{1-2}$$

The rest of this section is devoted to the construction of E and the verification of these requirements.

The first point is quite standard:

Lemma 1.2. *Assuming that $\varepsilon(A, L) > (p+2)g$, there exists an effective $\mathbb{Q}$-divisor F_0 on A having the properties that*

$$F_0 \equiv_{\text{num}} \frac{1-c}{p+2} L$$

for some $0 < c \ll 1$, and

$$\mathcal{J}(A, F_0) = \mathcal{I}_0.$$

Here naturally $\mathcal{I}_0 \subseteq \mathcal{O}_A$ denotes the ideal sheaf of the origin $0 \in A$.

Proof of Lemma 1.2. We claim that for suitable $0 < c \ll 1$ and sufficiently divisible $k \gg 0$, there exists a divisor $D \in |k(1-c)L|$ with

$$\text{mult}_0(D) = (p+2)gk,$$

where, in addition, D has a smooth tangent cone at the origin $0 \in A$ and is non-singular away from 0. Granting this, it suffices to put $F_0 = (1/(p+2)k)D$. As for the existence of D, let

$$\rho : A' = \text{Bl}_0(A) \to A$$

be the blowing up of A at 0, with exceptional divisor $T \subseteq A'$. Then, by definition of $\varepsilon(A, L)$, the class $(1-c)\rho^*L - (p+2)gT$ is ample on A' for $0 < c \ll 1$. If D' is a general divisor in the linear series corresponding to a large multiple of this class, Bertini's theorem on A' implies that $D = \rho_*(D')$ has the required properties. □

Now form the $(p+1)$-fold product $Y = A^{\times(p+1)}$ of A with itself, and write $\text{pr}_i : Y \to A$ for the i-th projection. Consider the reduced algebraic subset

$$\Lambda = \bigcup_{i=1}^{p+1} \text{pr}_i^{-1}(0) = \big\{(y_1, \ldots, y_{p+1}) \mid y_i = 0 \text{ for some } 1 \le i \le p+1\big\}.$$

---

for $0 \le p' \le p$ and $q \ge 1$, but these are all implied by the assertion of Proposition 1.1.

We wish to realize $\mathcal{I}_\Lambda$ as a multiplier ideal, to which end we simply consider the *exterior sum* of the divisors F_0 just constructed. Specifically, put

$$E_0 = \sum_{i=1}^{p+1} \mathrm{pr}_i^*(F_0).$$

Thanks to [Lazarsfeld 2004, 9.5.22], one has

$$\mathcal{J}(Y, E_0) = \prod_{i=1}^{p+1} \mathrm{pr}_i^* \mathcal{J}(A, F_0) = \prod_{i=1}^{p+1} \mathrm{pr}_i^* \mathcal{I}_0,$$

that is, $\mathcal{J}(Y, E_0) = \mathcal{I}_\Lambda$, as desired.

Next, consider the map

$$\begin{aligned} &\delta = \delta_{p+1} : A^{\times(p+2)} \to A^{\times(p+1)}, \\ &(x_0, x_1, \ldots, x_{p+1}) \mapsto (x_0 - x_1, \ldots, x_0 - x_{p+1}), \end{aligned} \tag{1-3}$$

and note that $\Sigma = \delta^{-1}\Lambda$ (scheme-theoretically). Set

$$E = \delta^*(E_0).$$

Forming multiplier ideals commutes with pulling back under smooth morphisms [Lazarsfeld 2004, 9.5.45]; hence

$$\mathcal{J}(X, E) = \delta^* \mathcal{J}(Y, E_0) = \delta^* \mathcal{I}_\Lambda = \mathcal{I}_\Sigma,$$

and thus (1-1) is satisfied.

In order to verify (1-2), we use the following assertion, which will be established in the next section.

Proposition 1.3. *There is a nef line bundle N on $X = A^{\times(p+2)}$ such that*

$$\delta^*\Big(\boxtimes^{p+1} L\Big) \otimes N = \boxtimes^{p+2} L^{p+2}. \tag{1-4}$$

Granting this, the property (1-2) — and with it, Proposition 1.1 — follows easily. Indeed,

$$E \equiv_{\mathrm{num}} \frac{1-c}{p+2} \cdot \Big(\delta^*\Big(\boxtimes^{p+1} L\Big)\Big).$$

Therefore (1-4) implies that

$$\Big(\boxtimes^{p+2} L\Big)(-E) \equiv_{\mathrm{num}} c \cdot \Big(\boxtimes^{p+2} L\Big) + \frac{1-c}{p+2} \cdot N,$$

which is ample. This completes the proof of Theorem A.

2. Proof of Proposition 1.3

Let A be an abelian variety and p a nonnegative integer. Define the maps

$$b : A^{\times(p+2)} \to A, \qquad (x_0, x_1, \ldots, x_{p+1}) \mapsto x_0 + x_1 + \cdots + x_{p+1},$$

and for any $0 \le i < j \le p+1$,

$$d_{ij} : A^{\times(p+2)} \to A, \qquad (x_0, x_1, \ldots, x_{p+1}) \mapsto x_i - x_j.$$

Recall the map δ from the previous section:

$$\delta : A^{\times(p+2)} \to A^{\times(p+1)}, \qquad (x_0, x_1, \ldots, x_{p+1}) \mapsto (x_0 - x_1, \ldots, x_0 - x_{p+1}).$$

Proposition 1.3 follows from the following more precise statement.[4]

Proposition 2.1. *For any ample line bundle L on A, we have*

$$\delta^*\Big(\boxtimes^{p+1} L\Big) \otimes (b^*L) \otimes \Big(\bigotimes_{1\le i<j} d_{ij}^* L\Big) = \boxtimes_{k=0}^{p+1} \big(L^{p+2-k} \otimes (-1)^* L^k\big).$$

Let

$$a : A \times A \to A \qquad \text{and} \qquad d : A \times A \to A$$

be the addition and subtraction maps, $\mathcal{P}$ be a normalized Poincaré line bundle on $A \times \widehat{A}$, and $\phi_L : A \to \widehat{A}$ be the isogeny induced by L. We use the notation

$$P = (1 \times \phi_L)^* \mathcal{P} \qquad \text{and} \qquad P_{ij} = \mathrm{pr}_{ij}^* P,$$

where $\mathrm{pr}_{ij} : A^{\times(p+2)} \to A \times A$ is the projection on the (i, j)-factor. We will use repeatedly the following standard facts.

Lemma 2.2. *The following identities hold*:

(i) $a^*L \cong (L \boxtimes L) \otimes P$;

(ii) $d^*L \cong (L \boxtimes (-1)^*L) \otimes P^{-1}$;

(iii) $\mathrm{pr}_{13}^* P \otimes \mathrm{pr}_{23}^* P \cong (a \times 1)^* P$ *on the triple product* $A \times A \times A$.

Proof. Identity (i) is well known (see for example [Mumford 1970, p. 78]) and follows from the seesaw principle. Identity (ii) can then be deduced similarly using the seesaw principle, or from (i) by noting that $d = a \circ (1, -1)$. This gives

$$\begin{aligned} d^*L &\cong (1 \times (-1))^*\big((L \boxtimes L) \otimes (1 \times \phi_L)^* \mathcal{P}\big) \\ &\cong (L \boxtimes (-1)^*L) \otimes (1 \times ((-1) \circ \phi_L))^* \mathcal{P} \\ &\cong (L \boxtimes (-1)^*L) \otimes (1 \times \phi_{(-1)^*L})^* (1, -1)^* \mathcal{P} \\ &\cong (L \boxtimes (-1)^*L) \otimes (1 \times \phi_L)^* \mathcal{P}^{-1}, \end{aligned}$$

[4] Note that L and $(-1)^*L$ differ by a topologically trivial line bundle.

where the last isomorphism follows from the well-known identity

$$((-1)\times 1)^*\mathcal{P} \cong (1\times(-1))^*\mathcal{P} \cong \mathcal{P}^{-1}.$$

Identity (iii) follows from the formula

$$\mathrm{pr}_{13}^*\mathcal{P} \otimes \mathrm{pr}_{23}^*\mathcal{P} \cong (a, 1)^*\mathcal{P}$$

on $A \times A \times \widehat{A}$, which in turn is easily verified using the seesaw principle (see, for example, the proof of Mukai's inversion theorem [1981, Theorem 2.2]). □

Proposition 2.1 follows by putting together the formulas in the next Lemma.

Lemma 2.3. *If L is an ample line bundle on A, the following identities hold*:

(i) $b^*L \;\cong\; \Big(\overset{p+2}{\boxtimes} L\Big) \otimes \Big(\bigotimes_{i<j} P_{ij}\Big)$;

(ii) $d_{ij}^*L \;\cong\; \Big(\mathcal{O}_A \boxtimes \cdots \boxtimes \underset{i}{L} \boxtimes \cdots \boxtimes (-1)^*\underset{j}{L} \boxtimes \cdots \boxtimes \mathcal{O}_A\Big) \otimes P_{ij}^{-1}$ *for all* $i < j$;

(iii) $\delta^*\Big(\overset{p+1}{\boxtimes} L\Big) \;\cong\; \big(L^{p+1} \boxtimes (-1)^*L \boxtimes \cdots \boxtimes (-1)^*L\big) \otimes P_{01}^{-1} \otimes \cdots \otimes P_{0,p+1}^{-1}$.

Proof. (i) If $p = 0$ this is Lemma 2.2(i). We can inductively obtain the formula for some $p > 0$ from that for $p-1$ by noting that $b\ (= b_{p+2}) = (a, \mathrm{id}) \circ b_{p+1}$, where b_k denotes the addition map for k factors, a is the addition map on the first two factors, and id is the identity on the last p factors. Therefore, inductively we have

$$b^*L \cong (a, \mathrm{id})^*\Big(\Big(\overset{p+1}{\boxtimes} L\Big) \otimes \Big(\bigotimes_{i<j} P_{ij}\Big)\Big).$$

The formula follows then by using Lemma 2.2(i) for the addition map a on the first two factors, and Lemma 2.2(iii) for the combination of the first two factors with any of the other p factors.

(ii) This follows simply by noting that $d_{ij} = d \circ p_{ij}$, where p_{ij} is the projection on the (i, j) factors and d is the difference map. We then apply Lemma 2.2(ii).

(iii) Note that $\delta = (d_{01}, \ldots, d_{0,p+1})$. Therefore

$$\delta^*\Big(\overset{p+1}{\boxtimes} L\Big) \cong d_{01}^*L \otimes \cdots \otimes d_{0,p+1}^*L.$$

One then applies the formula in (ii). □

In order to discuss the Koszul property in the next section, we will need a variant of these results. Specifically, fix $k \geq 2$ and consider the mapping

$$\gamma : A^{\times k} \to A^{\times(k-1)}, \qquad (x_0, x_1, \ldots, x_k) \mapsto (x_0 - x_1, x_1 - x_2, \ldots, x_{k-1} - x_k).$$

Consider also for any $0 \le i < j \le k$ the maps

$$a_{ij} : A^{\times k} \to A, \qquad (x_0, x_1, \ldots, x_k) \mapsto x_i + x_j.$$

Variant 2.4. *For any ample line bundle L on A we have*

$$\gamma^*\Big(\overset{k-1}{\boxtimes} L\Big) \otimes \Big(\bigotimes_{0\le i\le k-1} a_{i,i+1}^* L\Big) = L^2 \boxtimes \big(L^2 \otimes (-1)^* L\big) \boxtimes \ldots \boxtimes \big(L^2 \otimes (-1)^* L\big) \boxtimes \big(L \otimes (-1)^* L\big).$$

Proof. Noting that $a_{ij} = a \circ \mathrm{pr}_{ij}$, where pr_{ij} is the projection on the (i, j) factors and a is the difference map, and using Lemma 2.2(i), we have

$$a_{ij}^* L \cong \Big(\mathcal{O}_A \boxtimes \cdots \boxtimes \underset{i}{L} \boxtimes \cdots \boxtimes \underset{j}{L} \boxtimes \cdots \boxtimes \mathcal{O}_A\Big) \otimes P_{ij}\,.$$

On the other hand, $\gamma = (d_{01}, d_{12}, \ldots, d_{k-1,k})$ and using Lemma 2.3(ii) for each of the factors, we have

$$\gamma^*\Big(\overset{k-1}{\boxtimes} L\Big) \cong \big(L \boxtimes (L \otimes (-1)^* L) \boxtimes \ldots \boxtimes (L \otimes (-1)^* L) \boxtimes (-1)^* L\big) \otimes P_{01}^{-1} \otimes \ldots \otimes P_{k-1,k}^{-1}. \quad \square$$

Corollary 2.5. *There is a nef line bundle N on $A^{\times k}$ such that*

$$\gamma^*\Big(\overset{k-1}{\boxtimes} L\Big) \otimes N = \overset{k}{\boxtimes} L^3.$$

3. Complements

This section contains a couple of additional results that are established along the same lines as those above. As before, A is an abelian variety of dimension g, and L is an ample line bundle on A.

We start with a criterion for L to define an embedding in which A satisfies the Koszul property (for a definition and discussion of this property see for instance [Brion and Kumar 2005, §1.5]).

Proposition 3.1. *Assume that $\varepsilon(A, L) > 3g$. Then under the embedding defined by L, the homogeneous coordinate ring of A is a Koszul algebra.*

Sketch of Proof. Fix $k \ge 2$, and consider the k-fold self product $A^{\times k}$ of A. By analogy to Green's criterion, it is known that the Koszul property is implied by the vanishings (for all $k \ge 2$)

$$H^1\Big(A^{\times k}, \overset{k}{\boxtimes} L \otimes Q \otimes \mathcal{J}_\Gamma\Big) = 0, \tag{3-1}$$

where Q is a nef bundle on $A^{\times k}$, and Γ is the reduced algebraic set

$$\Gamma = \Delta_{1,2} \cup \Delta_{2,3} \cup \cdots \cup \Delta_{k-1,k}$$

(see [Inamdar and Mehta 1994, Proposition 1.9]). As above, this is established by realizing Γ as a multiplier ideal and applying Nadel vanishing. For the first point, one constructs (as in the case $p = 2$ of Theorem A) a divisor $F_0 \equiv_{\text{num}} ((1-c)/3)L$ on A, takes its exterior sum on $A^{\times(k-1)}$, and then pulls back under the map $\gamma : A^{\times k} \to A^{\times(k-1)}$ appearing at the end of the last section. The required positivity follows from Corollary 2.5. □

We record an analogue of the result of Hwang and To for Wahl [1992] maps.

Proposition 3.2. *Let L be an ample line bundle on A, and assume that $\varepsilon(A, L) > 2(g+m)$ for some integer $m \geq 0$. Then*

$$h^1\big(A \times A, L \boxtimes L \otimes \mathcal{I}_\Delta^{m+1}\big) = 0.$$

In particular, the m-th Wahl (or Gaussian) map

$$\gamma_L^m : h^0\big(A \times A, L \boxtimes L \otimes \mathcal{I}_\Delta^m\big) \to h^0\big(A \times A, L \boxtimes L \otimes \mathcal{I}_\Delta^m \otimes \mathcal{O}_\Delta\big) \cong h^0\big(A, L^2 \otimes S^m \Omega_A^1\big)$$

is surjective.

Sketch of Proof. One proceeds as in the proof outlined in the Introduction, except that the stronger numerical hypothesis on $\varepsilon(A, L)$ allows one to take $E_0 \equiv_{\text{num}} ((1-c)/2)L$ with $\mathcal{J}(A, E_0) = \mathcal{I}_0^{m+1}$. For the rest one argues as before. □

Remark 3.3. Proposition 3.2, combined with Bauer's result mentioned in the Introduction and with [Colombo et al. 2011, Theorem B], implies the surjectivity of the first Wahl map of curves of genus g sitting on very general abelian surfaces for all $g > 145$. This provides a "nondegenerational" proof — in the range $g > 145$ — of the surjectivity of the map $\gamma_{K_C}^1$ for general curves of genus g, which holds for all $g \geq 12$ and $g = 10$ [Ciliberto et al. 1988].

Acknowledgements

We are grateful to Thomas Bauer, Jun-Muk Hwang and Sam Payne for valuable discussions.

References

[Bauer 1998] T. Bauer, "Seshadri constants and periods of polarized abelian varieties", *Math. Ann.* **312**:4 (1998), 607–623. MR 2000a:14054 Zbl 0933.14025

[Bertram et al. 1991] A. Bertram, L. Ein, and R. Lazarsfeld, "Vanishing theorems, a theorem of Severi, and the equations defining projective varieties", *J. Amer. Math. Soc.* **4**:3 (1991), 587–602. MR 92g:14014 Zbl 0762.14012

[Brion and Kumar 2005] M. Brion and S. Kumar, *Frobenius splitting methods in geometry and representation theory*, Progress in Mathematics **231**, Birkhäuser, Boston, 2005. MR 2005k:14104 Zbl 1072.14066

[Buser and Sarnak 1994] P. Buser and P. Sarnak, "On the period matrix of a Riemann surface of large genus", *Invent. Math.* **117**:1 (1994), 27–56. MR 95i:22018 Zbl 0814.14033

[Ciliberto et al. 1988] C. Ciliberto, J. Harris, and R. Miranda, "On the surjectivity of the Wahl map", *Duke Math. J.* **57**:3 (1988), 829–858. MR 89m:14010 Zbl 0684.14009

[Colombo et al. 2011] E. Colombo, P. Frediani, and G. Pareschi, "Hyperplane sections of abelian surfaces", 2011. To appear in *J. Alg. Geom.* arXiv 0903.2781

[Eisenbud 2005] D. Eisenbud, *The geometry of syzygies*, Graduate Texts in Mathematics **229**, Springer, New York, 2005. MR 2005h:13021 Zbl 1066.14001

[Fuentes García 2005] L. Fuentes García, "Some results about the projective normality of abelian varieties", *Arch. Math.* (*Basel*) **85**:5 (2005), 409–418. MR 2006j:14062 Zbl 1082.14046

[Green 1984] M. L. Green, "Koszul cohomology and the geometry of projective varieties, II", *J. Differential Geom.* **20**:1 (1984), 279–289. MR 86j:14011 Zbl 0559.14009

[Green and Lazarsfeld 1987] M. Green and R. Lazarsfeld, "Deformation theory, generic vanishing theorems, and some conjectures of Enriques, Catanese and Beauville", *Invent. Math.* **90**:2 (1987), 389–407. MR 89b:32025 Zbl 0659.14007

[Hwang and To 2010] J.-M. Hwang and W.-K. To, "Buser–Sarnak invariant and projective normality of abelian varieties", preprint, 2010. arXiv 1003.0742

[Inamdar 1997] S. P. Inamdar, "On syzygies of projective varieties", *Pacific J. Math.* **177**:1 (1997), 71–76. MR 98a:14010 Zbl 0898.14015

[Inamdar and Mehta 1994] S. P. Inamdar and V. B. Mehta, "Frobenius splitting of Schubert varieties and linear syzygies", *Amer. J. Math.* **116**:6 (1994), 1569–1586. MR 96a:14054 Zbl 0817.14032

[Iyer 2003] J. N. Iyer, "Projective normality of abelian varieties", *Trans. Amer. Math. Soc.* **355**:8 (2003), 3209–3216. MR 2004e:14070 Zbl 1016.14024

[Lazarsfeld 1996] R. Lazarsfeld, "Lengths of periods and Seshadri constants of abelian varieties", *Math. Res. Lett.* **3**:4 (1996), 439–447. MR 98e:14044 Zbl 0890.14025

[Lazarsfeld 2004] R. Lazarsfeld, *Positivity in algebraic geometry, I*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **48**, Springer, Berlin, 2004. MR 2005k:14001a Zbl 1093.14501

[Li 2009] L. Li, "Wonderful compactification of an arrangement of subvarieties", *Michigan Math. J.* **58**:2 (2009), 535–563. MR 2011f:14086 Zbl 1187.14060

[Mukai 1981] S. Mukai, "Duality between $D(X)$ and $D(\hat{X})$ with its application to Picard sheaves", *Nagoya Math. J.* **81** (1981), 153–175. MR 82f:14036 Zbl 0417.14036

[Mumford 1970] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Oxford University Press, London, 1970. MR 44 #219 Zbl 0223.14022

[Pareschi 2000] G. Pareschi, "Syzygies of abelian varieties", *J. Amer. Math. Soc.* **13**:3 (2000), 651–664. MR 2001f:14086 Zbl 0956.14035

[Pareschi and Popa 2003] G. Pareschi and M. Popa, "Regularity on abelian varieties, I", *J. Amer. Math. Soc.* **16**:2 (2003), 285–302. MR 2004c:14086 Zbl 1022.14012

[Pareschi and Popa 2004] G. Pareschi and M. Popa, "Regularity on abelian varieties, II: Basic results on linear series and defining equations", *J. Algebraic Geom.* **13**:1 (2004), 167–193. MR2005a:14059 Zbl 1073.14061

[Wahl 1992] J. Wahl, "Introduction to Gaussian maps on an algebraic curve", pp. 304–323 in *Complex projective geometry* (Trieste/Bergen, 1989), edited by G. Ellingsrud et al., London Math. Soc. Lecture Note Ser. **179**, Cambridge Univ. Press, London, 1992. MR 93m:14029 Zbl 0790.14014

Communicated by David Eisenbud
Received 2010-03-11 Revised 2010-04-23 Accepted 2010-05-22

rlaz@umich.edu *Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, United States*
http://www.math.lsa.umich.edu/~rlaz

pareschi@mat.uniroma2.it *Dipartimento di Matematica, Università di Roma, Tor Vergata, V.le Della Ricerca Scientifica, I-00133 Roma, Italy*
http://www.mat.uniroma2.it/~pareschi

mpopa@math.uic.edu *Department of Mathematics, University of Illinois at Chicago, 851 S. Morgan Street, Chicago, IL 60607, United States*
http://www.math.uic.edu/~mpopa

ALGEBRA AND NUMBER THEORY 5:2(2011)

msp

Elliptic nets and elliptic curves

Katherine Stange

An elliptic divisibility sequence is an integer recurrence sequence associated to an elliptic curve over the rationals together with a rational point on that curve. In this paper we present a higher-dimensional analogue over arbitrary base fields. Suppose E is an elliptic curve over a field K, and $P_1, \ldots, P_n$ are points on E defined over K. To this information we associate an n-dimensional array of values in K satisfying a nonlinear recurrence relation. Arrays satisfying this relation are called *elliptic nets*. We demonstrate an explicit bijection between the set of elliptic nets and the set of elliptic curves with specified points. We also obtain Laurentness/integrality results for elliptic nets.

Introduction

An *elliptic divisibility sequence* is an integer sequence W_n satisfying

$$W_{n+m}W_{n-m} = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2. \tag{1}$$

This definition was introduced by Morgan Ward [1948]. Let $\Psi_n(x, y)$ be the n-th division polynomial associated to an elliptic curve (the n-th division polynomial vanishes at the n torsion points). Ward showed that division polynomials satisfy

This work was supported by NSERC Awards PGS D2 331379 and PDF 373333.

MSC2000: primary 11G05, 11G07, 11B37; secondary 11B39, 14H52.

Keywords: elliptic net, elliptic curve, Laurentness, elliptic divisibility sequence, recurrence sequence.

the recurrence (1) and furthermore that all elliptic divisibility sequences have the form

$$W_n = \lambda^{n^2-1}\Psi_n(x, y)$$

for some constant λ, elliptic curve (or singular cubic) and point $P = (x, y)$ on the curve. This rich structure has led to number-theoretic results [Ayad 1993; Everest et al. 2006; Ingram 2009; Silverman 2004; 2005; Swart 2003] and to applications to Hilbert's Tenth Problem [Cornelissen and Zahidi 2007; Eisenträger and Everest 2009; Poonen 2003], to integrable systems [Hone 2005], and to cryptography [Chudnovsky and Chudnovsky 1986; Shipsey 2001; Stange 2007]. For a bibliography, see [Everest et al. 2003, Chapter 10].

There have been several attempts to generalize this theory. *Translated elliptic divisibility sequences* were studied in [Swart 2003; van der Poorten 2005; van der Poorten and Swart 2006]. Mazur and Tate [1991] generalize division polynomials to arbitrary endomorphisms in the p-adic setting, and Streng [2008] uses their definition to generalize to the endomorphism ring of an elliptic curve with complex multiplication. Elliptic divisibility sequences are closely related to the denominators of the multiples $[n]P$ of a fixed point P; questions have been asked about the collection of denominators of the linear combinations $[n]P + [m]Q$ by Everest, Miller and Stephens [2004]. The hope of defining higher-rank elliptic divisibility sequences via a recurrence relation was discussed in correspondence by Elkies, Propp and Somos [Propp 2001].

The primary purpose of this paper is to generalize from integer sequences to multidimensional arrays with values in any field, which we call *elliptic nets*. A substantial part of the difficulty lies in finding the correct recurrence and defining a generalized division polynomial.

We define an *elliptic net* to be a function $W : A \to R$ from a finite-rank free abelian group A to an integral domain R satisfying the properties that $W(0) = 0$ and that

$$\begin{aligned} &W(p+q+s)\,W(p-q)\,W(r+s)\,W(r) \\ &\quad + W(q+r+s)\,W(q-r)\,W(p+s)\,W(p) \\ &\quad + W(r+p+s)\,W(r-p)\,W(q+s)\,W(q) = 0 \end{aligned}$$

for all $p, q, r, s \in A$. If $A = R = \mathbb{Z}$, this is an equivalent definition of an elliptic divisibility sequence (this is not immediately obvious, but it is a consequence of results in this paper). By the *rank* of an elliptic net we shall mean the rank of A (this bears no relation to the *rank of apparition* defined in [Ward 1948] for elliptic divisibility sequences). Section 1 covers the basic definitions and gives examples.

Our primary interest is the relationship between elliptic curves and elliptic nets.

Main Theorem (introductory version). *For each field K and integer n, there is an explicit bijection of sets*

$$\left\{\begin{array}{l}\text{scale equivalence classes}\\ \text{of nondegenerate elliptic}\\ \text{nets } W : \mathbb{Z}^n \to K\end{array}\right\}$$

$$\Updownarrow$$

$$\left\{\begin{array}{l}\text{tuples } (C, P_1, \ldots, P_n) \text{ where } C \text{ is a cubic}\\ \text{curve in Weierstrass form defined over } K,\\ \text{considered modulo unihomothetic changes}\\ \text{of variables, and such that } \{P_i\} \in C_{\mathrm{ns}}(K)^n\\ \text{is appropriate}\end{array}\right\}.$$

For a description of the relevant terminology, see Section 5 (appropriate), page 221 (scale equivalent, nondegenerate) and page 222 (unihomothetic). See Theorem 7.4 for a more detailed statement. The isomorphism itself is described explicitly in Definition 5.1 (depending on Theorem 4.6) and Theorem 6.7. For ranks 1 and 2, explicit formulae can be found in Propositions 3.8, 6.3 and 6.4. For an example, see (4).

The other main aspect of elliptic nets studied in this paper is Laurentness. These results are needed for the proof of the main theorem, but are of independent interest. One property of elliptic divisibility sequences of particular interest is that they are integer sequences: if the sequence begins $1, a, b, ac, \ldots$ $(a, b, c \in \mathbb{Z})$, then it will consist entirely of integers [Ward 1948]. This result has been studied in the more general framework of the Laurent phenomenon of [Fomin and Zelevinsky 2002].

Laurentness results are found in Section 2, which is devoted to the inductive structure of elliptic nets: how some terms are determined by others via the recurrence relation. We define a universal ring $\mathcal{W}_A$ for elliptic nets on A, such that elliptic nets $W : A \to R$ are in bijection with homomorphisms $\mathcal{W}_A \to R$. We obtain results on the structure of this ring, and in turn, these imply integrality results. See Theorem 2.2 for the case $n = 1$, Theorem 2.5 for $n = 2$, and Theorem 2.8 for $n \geq 3$. The proofs in this section are elementary but somewhat tedious. The author has not been successful in replacing them with methods similar to those of [Fomin and Zelevinsky 2002], although the possibility remains.

The next two sections define the higher-rank generalization of division polynomials called *net polynomials*: rational functions on the n-fold product E^n of an elliptic curve E, which vanish on tuples $(P_1, \ldots, P_n)$ satisfying a linear relation $[v_1]P_1 + \cdots + [v_n]P_n = \mathbb{O}$ for fixed coefficients v_i. In Section 3, we work with the complex uniformization of an elliptic curve defined over $\mathbb{C}$. In Section 4 we

generalize the definition to arbitrary fields by analysing the arithmetic properties of net polynomials. The main result here is Theorem 4.4.

The last three sections describe the bijection in the main theorem. Section 5 makes explicit the production of an elliptic net from any cubic Weierstrass curve using the net polynomials. Section 6 determines exactly those cubic curves which produce a given elliptic net. Finally, Section 7 puts together the results of the previous sections to prove the main theorem, stated in its full form as Theorem 7.4.

Computer software. The explicit isomorphism described in this paper has been implemented for Pari/GP and SAGE in ranks 1 and 2; see [Stange 2010].

1. Elliptic nets

Definition 1.1. Let A be a free finitely-generated abelian group and R an integral domain. An *elliptic net* is any map $W : A \to R$ with

$$W(0) = 0, \tag{2}$$

and such that, for all $p, q, r, s \in A$,

$$\begin{aligned} &W(p+q+s)\,W(p-q)\,W(r+s)\,W(r) \\ &\quad + W(q+r+s)\,W(q-r)\,W(p+s)\,W(p) \\ &\quad + W(r+p+s)\,W(r-p)\,W(q+s)\,W(q) = 0. \end{aligned} \tag{3}$$

Functions $W : A \to R$ which satisfy (3) but not (2) can only appear in characteristic 3 (to see this, take $p = q = r = s = 0$ in (3)). Any constant function in characteristic 3 is an example. By definition, these are not elliptic nets.

We refer to the rank of A as the *rank* of the elliptic net. Suppose that $B \subset A$ is a subgroup of A. Then the restriction to B of an elliptic net $W : A \to R$ is also an elliptic net. We refer to this elliptic net as *the subnet associated to* B and write $W|_B : B \to R$.

Example 1.2. Let R be an integral domain. The following are elliptic nets.

- The *zero net* $W : \mathbb{Z}^n \to R$ defined by $W(\boldsymbol{v}) = 0$ for all $\boldsymbol{v}$.
- The identity map $W_{id} : \mathbb{Z} \to \mathbb{Z}$ given by $W(v) = v$.
- Let $W' : \mathbb{Z} \to R$ be an elliptic net. Then for each $1 \leq i \leq n$, we may define $W_i : \mathbb{Z}^n \to R$ by $W_i(v_1, \ldots, v_n) = W'(v_i)$, and this will also be an elliptic net.
- More generally, if $W : A \to R$ is an elliptic net and $f : B \to A$ is a homomorphism of finitely generated free abelian groups, then $W \circ f : B \to R$ is also an elliptic net.
- If $W : A \to R$ is an elliptic net and $g : R \to S$ is a homomorphism of integral domains, then $g \circ W : A \to S$ is also an elliptic net.

- $W_{\mathrm{Leg}} : \mathbb{Z} \to \mathbb{Z}$ given by $W(v) = \left(\frac{v}{3}\right)$, the Legendre symbol of v over 3. This can be verified by a finite examination of cases; observe that at least one of p, q, r, $p-q$, $q-r$, and $r-p$ is divisible by 3. See also [Ward 1948, p. 31].
- $W_{\mathrm{Fib}} : \mathbb{Z} \to \mathbb{Z}$ given by

$$W(v) = \begin{cases} F_{2v} & \text{if } v > 0, \\ -F_{2v} & \text{if } v < 0, \\ 0 & \text{if } v = 0, \end{cases}$$

  where F_{2v} is the $2v$-th Fibonacci number. One checks this example using the closed form for terms of the Fibonacci sequence. See also [Ward 1948, p. 31].
- Here is a portion of an elliptic net of rank 2, displayed as an array:

$$\begin{array}{cccccccccc} & 3269 & -2869 & 4335 & 5959 & 12016 & -55287 & 23921 & 1587077 & -7159461 \\ & -127 & -299 & 94 & 479 & 919 & -2591 & 13751 & 68428 & 424345 \\ & -44 & -27 & -31 & 53 & -33 & -350 & 493 & 6627 & 48191 \\ & -1 & -7 & -5 & 8 & -19 & -41 & -151 & 989 & -1466 \\ & 3 & -2 & 1 & 3 & -1 & -13 & -36 & 181 & -1535 \\ & 1 & -1 & 1 & 1 & 2 & -5 & 7 & 89 & -149 \\ & -1 & -1 & 0 & 1 & 1 & -3 & 11 & 38 & 249 \\ \uparrow & -2 & -1 & -1 & 1 & -1 & -4 & 1 & 47 & 185 \\ Q & 1 & -3 & -1 & 2 & -3 & -5 & -17 & 63 & -184 \\ & P \rightarrow & & & & & & & & \end{array} \tag{4}$$

  This example arises from the curve $y^2 + y = x^3 + x^2 - 2x$ over $\mathbb{Q}$ and the two points $P = (0, 0)$, $Q = (1, 0)$; see Example 5.3. The origin is at the term with value 0. Each axis forms an elliptic divisibility sequence, e.g., $0, 1, 1, -3, 11, 38, 249, \ldots$.

2. Laurentness and integrality

In this section we ask which terms of an elliptic net determine the others via the recurrence relation. In the case of $n = 1$, Ward [1948] showed that the terms $W(1), \ldots, W(4)$ sufficed to determine the rest of the net (unless too many of these terms were zero). Our method also demonstrates Laurentness and integrality results. The main theorems of this section are used in Section 6.

Laurentness. Let I be a group, in additive notation, called the *indexing group*, whose elements are called *indices*. To each $i \in I$, we associate the symbol T_i. In what follows, the indexing group will be $I \cong \mathbb{Z}^n$ for some n.

Consider the ideal $\mathcal{M}$ in the ring $\mathbb{Z}[T_i]_{i \in I}$ generated by T_0 and all polynomials encoding property (3), i.e., those of the form

$$T_{p+q+s} T_{p-q} T_{r+s} T_r + T_{q+r+s} T_{q-r} T_{p+s} T_p + T_{r+p+s} T_{r-p} T_{q+s} T_q \tag{5}$$

as p, q, r, s range over I. Polynomials of the form (5) will be called *recurrence relations*. Consider the ring $\mathcal{W}_I$ obtained from $\mathbb{Z}[T_i]_{i\in I}/\mathcal{M}$ as a quotient by its own nilradical. For each integral domain R, there is a bijection between elliptic nets $W : I \to R$ and homomorphisms $\mathcal{W}_I \to R$ (defined by taking $T_i \mapsto W(i)$).

Taking $p = q = i, r = s = 0$ shows that $T_i^3(T_i + T_{-i}) \in \mathcal{M}$ for each $i \in I$. In particular, $T_{-i}^3(T_i + T_{-i}) \in \mathcal{M}$ also. Therefore, any prime ideal containing $\mathcal{M}$ contains $T_i + T_{-i}$; for if it did not, then it must contain T_i and T_{-i}, a contradiction. Therefore $T_{-i} = -T_i$ in $\mathcal{W}_I$. This implies the following.

Proposition 2.1. *Let $W : A \to R$ be an elliptic net. Then $W(-z) = -W(z)$ for all $z \in A$.*

The purpose of this section is to find a finite subset $0 \notin J \subset I$ such that the localisation $\mathcal{W}_I[T_i^{-1}]_{i\in J}$ is finitely generated as a $\mathbb{Z}$-algebra, and to give the generators. (The localisation is not the trivial ring $(1 = 0)$ by the existence of a homomorphism from it to $\mathbb{Q}$ given by Example 1.2, where one uses part (3) with $W' = W_{id}$ of part (2).) From this we show that every T_i can be expressed as a Laurent polynomial in integer coefficients in a finite number of terms T_j. This implies that any elliptic net which does not take zero values at the T_j is entirely determined by those values.

To illustrate, consider the rank-one case, which is essentially a result of Morgan Ward.

Theorem 2.2 [Ward 1948, Theorem 4.1]. *The ring $\mathcal{W}_{\mathbb{Z}}[T_1^{-1}, T_2^{-1}]$ is generated as a $\mathbb{Z}$-algebra by the six elements*

$$T_1, \quad T_1^{-1}, \quad T_2, \quad T_2^{-1}, \quad T_3, \quad T_4.$$

Furthermore, each T_i is expressible as a $\mathbb{Z}$-coefficient polynomial in

$$T_1, \quad T_1^{-1}, \quad T_2, \quad T_3, \quad T_4T_2^{-1}.$$

In particular, let $W : \mathbb{Z} \to \mathbb{Q}$ be an elliptic net. If $W(1) = 1$, $W(2) \neq 0$, $W(i)$ is an integer for $i = 2, 3, 4$, and $W(2)$ divides $W(4)$, then the elliptic net consists entirely of integers.

Proof. Recall that $T_{-n} = -T_n$, so it suffices to prove the first two statements for positive n. Taking $(p, q, r, s) = (n+1, n, 1, 0)$ and $(n+1, n-1, 1, 0)$ respectively, in $\mathcal{W}_I$ we have

$$T_{2n+1}T_1^3 + T_{n-1}T_{n+1}^3 + T_{n+2}T_{-n}T_n^2 = 0, \tag{6}$$

$$T_{2n}T_2T_1^2 + T_nT_{n-2}T_{n+1}^2 + T_{n+2}T_{-n}T_{n-1}^2 = 0. \tag{7}$$

The equations (6) and (7) prove the first statement by induction. The base case consists of $0 \leq n \leq 4$; for $n > 4$, we have $2n > n + 2$.

For even i, it can be shown by induction on (7) that T_i is expressible as a $\mathbb{Z}$-coefficient polynomial in T_1, T_1^{-1}, T_2, T_2^{-1}, T_3, and T_4 in such a way that the combined degree of T_2 and T_4 in each monomial is positive. For $i = 2, 4$ this is clear. To complete the induction in general, observe that in (7), each of the rightmost two terms is divisible by at least two T_k where k is even and $k < 2n$.

For even i, the second statement of the theorem concerning the expressibility of all T_i in terms of T_1, T_1^{-1}, T_2, T_3 and $T_4T_2^{-1}$ follows from the observation of the previous paragraph. The statement also holds for $i = 1, 3$. Consequently, it holds for odd i by induction on (6). □

Proofs by induction. The inductive proofs in this section will be based on the following definitions. Consider finite sets S, $J \subset I$ where $0, i \notin S \cup J$. We say that an index $i \in I$ is *S-integrally implied by J* if there exists a $\mathbb{Z}$-coefficient monomial $P(T_s)$ (in variables indexed by S) and $\mathbb{Z}$-coefficient polynomial $Q(T_j)$ (in variables indexed by J) such that

$$T_i P(T_s) = Q(T_j) \tag{8}$$

in $\mathcal{W}_I$. A set $K \subset I$ is *S-integrally implied by* the set J if every index in K is S-integrally implied by J.

As an example (see Proposition 2.1 and the paragraph which precedes it), $-i$ is S-integrally implied by any J containing i (for any S). In what follows, this fact will often be used tacitly.

A set $B \subset I$ *is an S-integral baseset for* $\mathcal{W}_I$ if all of I is S-integrally implied by B. If $B \subset I$ is an S-integral baseset, then each T_i can be expressed as a polynomial with integer coefficients in the set of variables $\{T_b\}_{b\in B} \cup \{T_s^{-1}\}_{s\in S}$ (when considered in the appropriate localisation).

It is straightforward to verify that if i is S-integrally implied by J and every $j \in J$ is S-integrally implied by J', then i is S-integrally implied by J'. To show that B is an S-integral baseset for I, the proofs in this section show the following: for each index $i \in I$, there is a finite sequence $J_0 \subset J_1 \subset \cdots \subset J_n$ such that $B = J_0$, $i \in J_n$ and for each $1 \leq k \leq n$, J_k is S-integrally implied by J_{k-1}. At each stage, we show that each index of J_i is S-integrally implied by J_{i-1}. Recall that implication is simply the existence of an relation of the form (8), and in fact we simply give a relevant element of the form (5).

These elements are cumbersome to write out. For example, taking in the case $n = 3$, $\boldsymbol{p} = (1, 0, 0)$, $\boldsymbol{q} = (0, 1, 0)$, $\boldsymbol{r} = (0, 0, 1)$, $\boldsymbol{s} = (0, 0, 0)$, we obtain

$$\begin{aligned} &T_{(1,1,0)}T_{(1,-1,0)}T_{(0,0,1)}T_{(0,0,1)} \\ &\quad + T_{(0,1,1)}T_{(0,1,-1)}T_{(1,0,0)}T_{(1,0,0)} \\ &\quad + T_{(1,0,1)}T_{(-1,0,1)}T_{(0,1,0)}T_{(0,1,0)}. \end{aligned}$$

For this information, let us instead use the more convenient notation

$$\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]. \tag{9}$$

In this notation, the columns to the left of the brackets correspond to the columns of p, q, r and s, while the indices of the terms of the recurrence appear as the columns within the brackets.

To demonstrate that an index i is (S-integrally) implied by a set of indices J, it suffices to write down an appropriate such array. Notice that any array of the form (9) is a recurrence if each row is a recurrence. Therefore we may construct examples row by row.

The following definition will be useful for ordering inductions.

Definition 2.3. Let

$$N(\boldsymbol{v}) = \max_{i=1,\dots,n} |v_i|$$

be the *sup-norm* of the vector $\boldsymbol{v}$.

Basesets for rank 2. For the rank-two case, we require a lemma.

Lemma 2.4. *The ring $\mathcal{W}_{\mathbb{Z}^2}[T_{(1,0)}^{-1}, T_{(0,1)}^{-1}, T_{(1,1)}^{-1}]$ is generated as a $\mathbb{Z}$-algebra by the elements*

$$\{T_{\boldsymbol{v}} : N(\boldsymbol{v}) \leq 4\} \cup \{T_{(1,0)}^{-1}, T_{(0,1)}^{-1}, T_{(1,1)}^{-1}\}.$$

Proof. Let $S = \{(1,0),(0,1),(1,1)\}$ and $B = \{\boldsymbol{v} \in \mathbb{Z}^2 : N(\boldsymbol{v}) \leq 4\}$. This proof proceeds by induction on the sup-norm. Trivially, any $\boldsymbol{v}$ with $N(\boldsymbol{v}) \leq 4$ is S-integrally implied by B. Let $N_0 > 4$ and suppose that all terms with indices with sup-norm less than N_0 are S-integrally implied by B. Call the set of such indices K_{N_0}. Suppose $\boldsymbol{v}$ is an index of sup-norm N_0. We construct a recurrence demonstrating that $\boldsymbol{v}$ is S-integrally implied by K_{N_0} row by row. For $i = 1, 2$, define $w_i = \lceil v_i/2 \rceil$.

<u>*Case I*</u>: *$\boldsymbol{v}$ has one odd entry and one even entry.* For the odd entry, we use the row

$$w_i \;\; w_i{-}1 \;\; 0 \;\; 0 \;\left[\; v_i \;\; 1 \;\; 0 \;\; 0 \;\middle|\; w_i{-}1 \;\; w_i{-}1 \;\; w_i \;\; w_i \;\middle|\; w_i \;\; -w_i \;\; w_i{-}1 \;\; w_i{-}1 \;\right]$$

For the even entry, we use the row

$$w_i \;\; w_i \;\; 1 \;\; 0 \;\left[\; v_i \;\; 0 \;\; 1 \;\; 1 \;\middle|\; w_i{+}1 \;\; w_i{-}1 \;\; w_i \;\; w_i \;\middle|\; w_i{+}1 \;\; -w_i{+}1 \;\; w_i \;\; w_i \;\right]$$

<u>*Case II*</u>: *$\boldsymbol{v}$ has two odd entries.* Use the rows

$$\begin{array}{cccc} w_1 & w_1{-}1 & 0 & 0 \\ w_2 & w_2{-}1 & 1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} v_1 & 1 & 0 & 0 & w_1{-}1 & w_1{-}1 & w_1 & w_1 & w_1 & -w_1 & w_1{-}1 & w_1{-}1 \\ v_2 & 1 & 1 & 1 & w_2 & w_2{-}2 & w_2 & w_2 & w_2{+}1 & -w_2{+}1 & w_2{-}1 & w_2{-}1 \end{array}\right]$$

Case III: $\boldsymbol{v}$ has two even entries. Use the rows

$$\begin{array}{cccc|cccc|cccc}
w_1 & w_1{-}1 & 0 & 1 & v_1 & 1 & 1 & 0 & w_1 & w_1{-}1 & w_1{+}1 & w_1 & w_1{+}1 & -w_1 & w_1 & w_1{-}1 \\
w_2 & w_2 & 1 & 0 & v_2 & 0 & 1 & 1 & w_2{+}1 & w_2{-}1 & w_2 & w_2 & w_2{+}1 & -w_2{+}1 & w_2 & w_2
\end{array}$$

For even v_i, either $|v_i| \le 2$ or $|v_i| > 3$. In the former case, $|w_i| + 1 \le 2 < N_0$. In the latter case, we have $|w_i| + 1 \le (|v_i| + 2)/2 < |v_i| \le N_0$. For odd $\boldsymbol{v}_i$, either $|v_i| \le 3$ or $|v_i| > 4$. In the former case $|w_i| + 2 \le 4 < N_0$. In the latter case, we have $|w_i| + 2 \le (|v_i| + 5)/2 < |v_i| \le N_0$.

Therefore all the vectors in the recurrence have sup-norm less than N_0 with the exception of $\boldsymbol{v}$. In the monomial of $\boldsymbol{v}$ in the recurrence, the other indices are $(1, 0)$, $(0, 1)$ or $(1, 1)$. This demonstrates that $\boldsymbol{v}$ is S-integrally implied by K_{N_0} and hence by B. □

Theorem 2.5. *The ring ${}^{\mathcal{W}}_{\mathbb{Z}^2}[T_{(1,1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}]$ is generated as a $\mathbb{Z}$-algebra by the eleven elements*

$$T_{(1,1)},\ T_{(1,0)},\ T_{(0,1)},\ T_{(1,1)}^{-1},\ T_{(1,0)}^{-1},\ T_{(0,1)}^{-1},\ T_{(2,1)},\ T_{(1,2)},\ T_{(2,0)},\ T_{(0,2)},\ T_{(2,2)},$$

and the following identities hold:

$$T_{(1,-1)}T_{(1,1)}^3 = T_{(1,0)}^3 T_{(1,2)} - T_{(0,1)}^3 T_{(2,1)},$$
$$T_{(2,2)}T_{(1,-1)}T_{(1,0)}T_{(0,1)} = T_{(1,1)}\left(T_{(0,2)}T_{(2,1)}T_{(1,0)} - T_{(0,1)}T_{(2,0)}T_{(1,2)}\right).$$

In particular, if $W : \mathbb{Z}^2 \to \mathbb{Q}$ is an elliptic net for which

(a) $W(1, 0) = W(0, 1) = W(1, 1) = 1$,

(b) $W(2, 0)$, $W(0, 2)$, $W(1, 2) \ne W(2, 1)$ *are integers, and*

(c) $W(1, 2) - W(2, 1)$ *divides* $W(0, 2)W(2, 1) - W(2, 0)W(1, 2)$,

then all terms of the elliptic net are determined by these seven values and are integers.

Proof. The first and second stated identities are the recurrences

$$\begin{array}{cccc|cccc|cccc}
1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array},$$
$$\begin{array}{cccc|cccc|cccc}
1 & 1 & -1 & 0 & 2 & 0 & -1 & -1 & 0 & 2 & 1 & 1 & 0 & -2 & 1 & 1 \\
1 & 2 & 1 & -1 & 2 & -1 & 0 & 1 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 2
\end{array}. \qquad (10)$$

Let $S = \{(1, 0), (0, 1), (1, 1)\}$, and $B = \{\boldsymbol{v} \in \mathbb{Z}^2 : N(\boldsymbol{v}) \le 4\}$. By Lemma 2.4, it suffices to show that B is S-integrally implied by the set

$$\{(1, 0), (0, 1), (1, 1), (2, 0), (0, 2), (2, 1), (1, 2), (2, 2)\}.$$

We list the relevant recurrences in order. As each index is implied, it may be used to imply later indices. It is assumed that as (a, b) is implied, so is $(-a, -b)$. To begin, the index $(1, -1)$ is implied by (10). We then write

$$
\begin{array}{ll}
(2,-1): & \left[\begin{array}{cccc|cccc|cccc} -1 & 0 & 1 & 1 & 0 & -1 & 2 & 1 & 2 & -1 & 0 & -1 & 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \end{array}\right], \\
(-1,2): & \left[\begin{array}{cccc|cccc|cccc} 0 & -1 & -1 & 0 & -1 & 1 & -1 & -1 & -2 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \end{array}\right], \\
(2,-2): & \left[\begin{array}{cccc|cccc|cccc} 1 & 1 & -1 & 0 & 2 & 0 & -1 & -1 & 0 & 2 & 1 & 1 & 0 & -2 & 1 & 1 \\ -1 & -2 & -1 & 1 & -2 & 1 & 0 & -1 & -2 & -1 & 0 & -1 & -1 & 0 & -1 & -2 \end{array}\right].
\end{array}
$$

At this point we have implied all indices of sup-norm at most 2. Next we have

$$
\begin{array}{ll}
(3,0): & \left[\begin{array}{cccc|cccc|cccc} 2 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & -2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right], \\
(3,1): & \left[\begin{array}{cccc|cccc|cccc} 2 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & -2 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \end{array}\right], \\
(3,2): & \left[\begin{array}{cccc|cccc|cccc} 2 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & -2 & 1 & 1 \\ 1 & 1 & 1 & 0 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 1 \end{array}\right], \\
(3,3): & \left[\begin{array}{cccc|cccc|cccc} 2 & 1 & 1 & 0 & 3 & 1 & 1 & 1 & 2 & 0 & 2 & 2 & 3 & -1 & 1 & 1 \\ 2 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & -2 & 1 & 1 \end{array}\right].
\end{array}
\tag{11}
$$

Simply by switching top rows with bottom rows, we similarly imply $(0,3)$, $(1,3)$, and $(2,3)$. And by putting negatives on the second row of (11), we imply the index $(3,-2)$ (and $(-2,3)$ by switching top and bottom). Next,

$$
\begin{array}{ll}
(3,-1): & \left[\begin{array}{cccc|cccc|cccc} 2 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & -2 & 1 & 1 \\ -1 & -1 & -2 & 2 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 0 & 0 & -2 \end{array}\right], \\
(3,-3): & \left[\begin{array}{cccc|cccc|cccc} 1 & 2 & 1 & 0 & 3 & -1 & 1 & 1 & 3 & 1 & 1 & 1 & 2 & 0 & 2 & 2 \\ -2 & -1 & 0 & 0 & -3 & -1 & 0 & 0 & -1 & -1 & -2 & -2 & -2 & 2 & -1 & -1 \end{array}\right].
\end{array}
$$

Again by switching top and bottom we get $(-1,3)$. We have now implied all indices with sup-norm at most 3. We continue with

$$
\begin{array}{ll}
(4,0): & \left[\begin{array}{cccc|cccc|cccc} 2 & 1 & 0 & 1 & 4 & 1 & 1 & 0 & 2 & 1 & 3 & 2 & 3 & -2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right], \\
(4,1): & \left[\begin{array}{cccc|cccc|cccc} 3 & 2 & 1 & -1 & 4 & 1 & 0 & 1 & 2 & 1 & 2 & 3 & 3 & -2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right], \\
(4,2): & \left[\begin{array}{cccc|cccc|cccc} 3 & 2 & 1 & -1 & 4 & 1 & 0 & 1 & 2 & 1 & 2 & 3 & 3 & -2 & 1 & 2 \\ 1 & 1 & 1 & 0 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 1 \end{array}\right], \\
(4,3): & \left[\begin{array}{cccc|cccc|cccc} 2 & 2 & 1 & 0 & 4 & 0 & 1 & 1 & 3 & 1 & 2 & 2 & 3 & -1 & 2 & 2 \\ 2 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & -2 & 1 & 1 \end{array}\right], \\
(4,4): & \left[\begin{array}{cccc|cccc|cccc} 3 & 2 & 1 & -1 & 4 & 1 & 0 & 1 & 2 & 1 & 2 & 3 & 3 & -2 & 1 & 2 \\ 2 & 2 & 1 & 0 & 4 & 0 & 1 & 1 & 3 & 1 & 2 & 2 & 3 & -1 & 2 & 2 \end{array}\right].
\end{array}
$$

Again by switching top rows with bottom rows, we similarly imply $(0,4)$, $(1,4)$, $(2,4)$ and $(3,4)$. And by putting negatives on the second rows, we imply the indices $(4,-1)$, $(-1,4)$, $(4,-3)$ and $(-3,4)$. There remains to consider the

indices

$$(4,-2): \quad \begin{array}{cccc} 2 & 1 & -1 & 1 \\ -1 & -1 & -1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} 4 & 1 & 0 & -1 & 1 & 2 & 3 & 2 & 2 & -3 & 2 & 1 \\ -2 & 0 & -1 & -1 & -2 & 0 & -1 & -1 & -2 & 0 & -1 & -1 \end{array}\right],$$

$$(4,-4): \quad \begin{array}{cccc} 2 & 1 & -1 & 1 \\ -2 & -2 & -1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} 4 & 1 & 0 & -1 & 1 & 2 & 3 & 2 & 2 & -3 & 2 & 1 \\ -4 & 0 & -1 & -1 & -3 & -1 & -2 & -2 & -3 & 1 & -2 & -2 \end{array}\right].$$

By switching rows, we imply $(-2, 4)$. We have now demonstrated the calculation of all terms of index with sup-norm at most 4. The second part of the statement follows immediately from the first. □

Basesets for ranks $n \geq 3$. Let $\boldsymbol{e}_i$ denote the standard basis vectors.

Lemma 2.6. *Define subsets of $\mathbb{Z}^3$ by*

$$L_2 = \{\boldsymbol{e}_i\}_i \cup \{\boldsymbol{e}_i \pm \boldsymbol{e}_j\}_{i \neq j} \cup \{2\boldsymbol{e}_i\}_i,$$
$$L_2' = \{a_i \boldsymbol{e}_i + a_j \boldsymbol{e}_j : a_i \in \mathbb{Z}, 1 \leq i \leq j \leq 3\}.$$

Then all indices $\boldsymbol{v} \in \mathbb{Z}^3$ with $N(\boldsymbol{v}) \leq 2$ are L_2-integrally implied by L_2'.

Proof. We make use of the recurrences

$$\begin{array}{ccccc} 1 & 1 & 0 & -1 \\ 0 & 0 & -1 & 1 \\ 1 & 0 & 1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & -1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \end{array}\right], \tag{12}$$

$$\begin{array}{ccccc} 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} -1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & 1 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \\ 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right], \tag{13}$$

$$\begin{array}{ccccc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & -1 \end{array} \left[\begin{array}{cccc|cccc|cccc} 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \end{array}\right]. \tag{14}$$

Permute the rows of (12) by the cyclic permutations (123) and (132), calling the results $(12)'$ and $(12)''$ respectively; for example, the rightmost column of $(12)'$ is $(0, 1, 0)$. Do the same for (13) and (14).

Consider the equation obtained by the combination

$$\begin{aligned} &(12) \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(1,-1,0)} T_{(0,1,0)}^2 + (12)' \times T_{(1,1,1)} T_{(1,0,0)} T_{(0,1,-1)} T_{(0,1,0)}^2 T_{(0,0,1)} \\ &+(14) \times T_{(1,-1,0)} T_{(0,1,0)}^2 T_{(0,1,1)} T_{(0,0,1)} T_{(1,0,1)}^2 + (14)' \times T_{(0,1,-1)} T_{(1,0,0)}^2 T_{(0,0,1)} T_{(1,0,1)} T_{(1,1,0)} \\ &+(13) \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(0,1,0)}^2 T_{(1,1,0)} + (13)' \times T_{(1,1,1)} T_{(0,1,0)}^2 T_{(1,0,0)} T_{(0,1,1)} T_{(0,0,1)} \\ &+(13)'' \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(1,0,1)} T_{(0,1,0)} T_{(0,0,1)}. \end{aligned}$$

The result has the form $aT_{(1,1,1)} + b = 0$, where a and b are polynomials in $T_{\boldsymbol{v}}$ where every $\boldsymbol{v}$ has at least one zero coordinate. In particular,

$$a = T_{(1,0,0)}^3 T_{(0,1,0)} T_{(0,0,1)}^2 T_{(1,0,1)} T_{(0,2,0)} T_{(1,0,-1)}.$$

Thus $T_{(1,1,1)}$ is L_2-integrally implied by L_2'. To imply the terms $T_{(-1,1,1)}$, $T_{(1,-1,1)}$, and $T_{(1,1,-1)}$, use (12), (12)′, and (12)″. This covers all terms of sup-norm at most 1.

We have the following recurrence:

$$\left[\begin{array}{cccc|cccc|cccc}
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & -1 & 1 & 1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 \\
2 & 1 & 1 & -1 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 2 \\
0 & 1 & 0 & 1 & 2 & -1 & 1 & 0 & 2 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}\right]
\begin{array}{c}
\left[\begin{array}{cccc} 1 & 0 & 1 & 0 \end{array}\right] \\
\left[\begin{array}{cccc} 0 & -1 & 1 & 0 \end{array}\right] \\
\left[\begin{array}{cccc} 2 & -1 & 0 & 1 \end{array}\right] \\
\left[\begin{array}{cccc} 1 & 0 & 2 & 1 \end{array}\right] \\
\left[\begin{array}{cccc} 1 & -1 & 1 & 1 \end{array}\right]
\end{array}.$$

If $\boldsymbol{v}$ has exactly one coordinate of value ± 2 (the rest ± 1), then we imply $\boldsymbol{v}$ by taking the first three rows in the recurrence above (possibly taking negatives and permutations of rows as necessary). If $\boldsymbol{v}$ has exactly two ± 2's, use the middle three rows in the same way. If $\boldsymbol{v}$ has exactly three ± 2's, use the last three rows (this relies on the previous cases). □

Remark 2.7. The four equations (12), (12)′, (12)″ and (13) in the four unknowns $T_{(1,1,1)}$, $T_{(-1,1,1)}$, $T_{(1,-1,1)}$ and $T_{(1,1,-1)}$, are linear with coefficients consisting of monomials in $T_{\boldsymbol{v}}$ where $\boldsymbol{v}$ has at least one zero coordinate. The determinant of the system is

$$2T_{(1,0,0)}T_{(0,1,0)}T_{(0,0,1)}^2T_{(1,1,0)}T_{(1,0,1)}^2T_{(0,1,1)}^2T_{(1,-1,0)}T_{(1,0,-1)}T_{(0,1,-1)}.$$

This observation is useful for calculations where 2 is invertible.

Theorem 2.8. *Let $n \geq 2$. For each ℓ in the set*

$$L = \{0, 1\}^n \setminus \{(0, 0, \ldots, 0), (1, 1, \ldots, 1)\},$$

choose a vector $\boldsymbol{x}_\ell$ having $N(\boldsymbol{x}_\ell) = 1$ and having nonzero entries exactly where ℓ does. Let $G_n = \{\boldsymbol{x}_\ell\}_{\ell \in L}$. Let

$$H_n = G_n \cup \{\boldsymbol{e}_i\} \cup \{\boldsymbol{e}_i \pm \boldsymbol{e}_j, i \neq j\} \cup \{2\boldsymbol{e}_i\},$$
$$H_n' = H_n \cup \{2\boldsymbol{e}_i + \boldsymbol{e}_j, i \neq j\}.$$

Then $\mathbb{Z}^n$ is H_n-integrally implied by H_n'.

Proof. The proof is by induction on n. The base case is $n = 2$, which is a consequence of Theorem 2.5.

Fixing any $1 \leq i \leq n$, we can identify H_{n-1} with a subset of H_n (and H_{n-1}' with a subset of H_n') by adding a zero between the $(i-1)$-th and i-th positions of each vector of H_{n-1} (or H_{n-1}'). By this identification and by the inductive hypothesis (for $n-1$), any $\boldsymbol{v} \in \mathbb{Z}^n$ with a zero in the i-th position is H_n-integrally implied by H_n'. Therefore it suffices to imply those $\boldsymbol{v} \in \mathbb{Z}^n$ having no zero coordinate.

The inductive step is itself an induction on the sup-norm of $\boldsymbol{v}$. The base cases are $N(\boldsymbol{v}) = 1$ and $N(\boldsymbol{v}) = 2$. Both of these for $n = 3$ are provided by Lemma 2.6,

so for the base cases, we may assume $n \geq 4$. To imply $\boldsymbol{v}$, we construct a recurrence row by row, so that the first column is exactly $\boldsymbol{v}$. For the first three rows, use the following, multiplied by -1 as necessary.

$$\begin{array}{ccc} 1\ 0\ 0\ 0 & \left[\begin{array}{cc|cc|cc} 1 & 1\ 0\ 0 & 0\ 0\ 1\ 1 & 1\ \text{-}1\ 0\ 0 \\ 1\ \text{-}1\ 0\ 0 & 1\ 1\ 0\ 0 & 0\ 0\ 1\ 1 \end{array}\right. \\ 0\ 1\ 0\ 0 & \\ 0\ 0\ 0\ 1 & \left.\begin{array}{cc|cc|cc} 1\ 0\ 1\ 0 & 1\ 0\ 1\ 0 & 1\ 0\ 1\ 0 \end{array}\right] \end{array}.$$

For all subsequent rows, use one of the following two recurrences (shown together in an array), multiplied by -1 as appropriate:

$$\begin{array}{cc} 1\ 1\ 1\ \text{-}1 & \left[\begin{array}{ccc|ccc|ccc} 1\ 0\ 0\ 1 & 1\ 0\ 0\ 1 & 1\ 0\ 0\ 1 \end{array}\right. \\ 0\ 0\ \text{-}1\ 1 & \left.\begin{array}{ccc|ccc|ccc} 1\ 0\ 0\ \text{-}1 & 0\ 1\ 1\ 0 & 0\ \text{-}1\ 1\ 0 \end{array}\right] \end{array}.$$

For each row, the choice between the two possibilities can be made in such a way that the fourth column of the recurrence lies in G_n. Columns 2 and 4 have at most two nonzero entries (which are ± 1) and so are in H_n. The other columns, numbered 5 though 12, have at least one zero entry, and so are already implied by the inductive step. This completes the case $N(\boldsymbol{v}) = 1$.

For the remainder of the proof, we will repeatedly use the following recurrences. Let $w_i = \lceil v_i/2 \rceil$. If v_i is even, we call the recurrences shown in the following array (E1) through (E4):

$$\begin{array}{cccc} w_i{-}1 & w_i & 0 & 1 \\ w_i & w_i{-}1 & 0 & 1 \\ w_i & w_i & 0 & 0 \\ w_i & w_i & 1 & 0 \end{array} \left[\begin{array}{cccc|cccc|cccc} v_i & -1 & 1 & 0 & w_i{+}1 & w_i & w_i & w_i{-}1 & w_i & -w_i{+}1 & w_i{+}1 & w_i \\ v_i & 1 & 1 & 0 & w_i & w_i{-}1 & w_i{+}1 & w_i & w_i{+}1 & -w_i & w_i & w_i{-}1 \\ v_i & 0 & 0 & 0 & w_i & w_i & w_i & w_i & w_i & -w_i & w_i & w_i \\ v_i & 0 & 1 & 1 & w_i{+}1 & w_i{-}1 & w_i & w_i & w_i{+}1 & -w_i{+}1 & w_i & w_i \end{array}\right]$$

If v_i is odd, we call the following recurrences (O1) through (O5).

$$\begin{array}{cccc} w_i & w_i{-}1 & 0 & 0 \\ w_i{-}1 & w_i & 0 & 0 \\ w_i{-}1 & w_i & 1 & 0 \\ w_i & w_i & 0 & -1 \\ w_i & w_i & 1 & -1 \end{array} \left[\begin{array}{cccc|cccc|cccc} v_i & 1 & 0 & 0 & w_i{-}1 & w_i{-}1 & w_i & w_i & w_i & -w_i & w_i{-}1 & w_i{-}1 \\ v_i & -1 & 0 & 0 & w_i & w_i & w_i{-}1 & w_i{-}1 & w_i{-}1 & 1{-}w_i & w_i & w_i \\ v_i & -1 & 1 & 1 & w_i{+}1 & w_i{-}1 & w_i{-}1 & w_i{-}1 & w_i & -w_i & w_i & w_i \\ v_i & 0 & -1 & 0 & w_i{-}1 & w_i & w_i{-}1 & w_i & w_i{-}1 & -w_i & w_i{-}1 & w_i \\ v_i & 0 & 0 & 1 & w_i & w_i{-}1 & w_i{-}1 & w_i & w_i & 1{-}w_i & w_i{-}1 & w_i \end{array}\right]$$

The second base case is $N(\boldsymbol{v}) = 2$ ($n \geq 4$ still). Since we may assume $v_i \neq 0$ (this is covered by previous cases in the induction on n), the other v_i have $|v_i| = \pm 1$. There are three cases:

Case I: $\boldsymbol{v}$ has at least three odd v_i. Use for the first three odd v_i the recurrences (O1), (O4) and (O5) respectively. Use (E3) for all the even v_i. In this case, all the columns besides the first contain only digits 0 and ± 1 and so were implied in the case $N(\boldsymbol{v}) = 1$. Columns 2, 3, and 4 contain only one nonzero term each, and so are in H_n.

Case II: $\boldsymbol{v}$ has one or two odd v_i. Use (O3) for one odd coordinate and (O1) for the other (if it exists). Use (E3) for all even coordinates. Then, columns 2–4 contain one or two nonzero entries, and columns 5–12 may contain at most one ± 2; but such a column was implied in the Case I.

Case III: $\boldsymbol{v}$ has no odd v_i. Use (E1) and (E4) for the first two rows, and (E3) for all others. Columns 2–4 contain one or two nonzero entries and 5–12 at most two ± 2's; but such a column was implied in Case I or II.

This completes the $N(\boldsymbol{v}) = 2$ base case.

Now suppose $N(\boldsymbol{v}) = N_0 \geq 3$ and $n \geq 3$. This is the inductive step; we will assume we have implied all indices of sup-norm less than N_0. As before, $v_i \neq 0$. For $|v_i| = 3$, (O1), (O2), (O4), and (O5) have entries less than N_0 in columns 5–12. For $1 \leq |v_i| \leq 2$, and $3 < |v_i| \leq N_0$, all applicable recurrences have entries less than N_0 in those columns. We have two cases:

Case I: $\boldsymbol{v}$ has at least one even entry. Use (E4) for the first even coordinate, and choose from (E1) and (E2) for the second even coordinate (if it exists). We use (E3) for all other even coordinates. We will use (O1) or (O2) for all odd entries (and make the choice between (E1) and (E2) above) in such a way that the second column is in G_n.

Case II: $\boldsymbol{v}$ has no even entry. Use (O4) and (O5) for the first two odd coordinates, and (O1) or (O2) for all others, according so that the second column is an element of G_n. □

3. Net polynomials over $\mathbb{C}$

Fix an elliptic curve E defined over $\mathbb{C}$. Our purpose is to define rational functions $\Omega_{\boldsymbol{v}} : E^n \to \mathbb{C}$ for all $\boldsymbol{v} \in \mathbb{Z}^n$ such that for each $\boldsymbol{P} \in E^n$, the map

$$W_{E,\boldsymbol{P}} : \mathbb{Z}^n \to \mathbb{C}, \quad \boldsymbol{v} \mapsto \Omega_{\boldsymbol{v}}(\boldsymbol{P})$$

is an elliptic net. In this section we associate a lattice $\Lambda \subset \mathbb{C}$ to the elliptic curve E and consider the complex uniformization $\mathbb{C}/\Lambda$.

Elliptic functions over $\mathbb{C}$. For a complex lattice Λ, let $\eta : \Lambda \to \mathbb{C}$ be the quasiperiod homomorphism, and define a quadratic form $\lambda : \Lambda \to \{\pm 1\}$ by

$$\lambda(\omega) = \begin{cases} 1 & \text{if } \omega \in 2\Lambda, \\ -1 & \text{if } \omega \notin 2\Lambda. \end{cases}$$

Recall that the Weierstrass sigma function $\sigma : \mathbb{C}/\Lambda \to \mathbb{C}$ satisfies the following transformation formula for all $z \in \mathbb{C}$ and $\omega \in \Lambda$:

$$\sigma(z + \omega; \Lambda) = \lambda(\omega) e^{\eta(\omega)(z + \frac{1}{2}\omega)} \sigma(z; \Lambda). \tag{15}$$

Definition 3.1. Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. For $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$, define a function $\Omega_{\boldsymbol{v}}$ on $\mathbb{C}^n$ in variables $\boldsymbol{z} = (z_1, \ldots, z_n)$ as follows:

$$\Omega_{\boldsymbol{v}}(\boldsymbol{z}; \Lambda) = \frac{\sigma(v_1 z_1 + \cdots + v_n z_n; \Lambda)}{\prod_{i=1}^{n} \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} \sigma(z_i + z_j; \Lambda)^{v_i v_j}}.$$

(If $\boldsymbol{v} = \boldsymbol{0}$, we set $\Omega_{\boldsymbol{v}} \equiv 0$.) In particular, we have for each $n \in \mathbb{Z}$, a function Ω_n on $\mathbb{C}$ in the variable z, namely

$$\Omega_n(z; \Lambda) = \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}},$$

and for each pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, a function $\Omega_{m,n}$ on $\mathbb{C} \times \mathbb{C}$ in variables z and w:

$$\Omega_{m,n}(z, w; \Lambda) = \frac{\sigma(mz + nw; \Lambda)}{\sigma(z; \Lambda)^{m^2 - mn} \sigma(z + w; \Lambda)^{mn} \sigma(w; \Lambda)^{n^2 - mn}}.$$

Remark 3.2. Compare the proof of Lemma 4.5 to this definition.

Proposition 3.3. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. The functions $\Omega_{\boldsymbol{v}}$ are elliptic functions in each variable.*

Proof. Let $\omega \in \Lambda$. We show the function is elliptic in the first variable. Let $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ and $\boldsymbol{z} = (z_1, \ldots, z_n)$, $\boldsymbol{w} = (\omega, 0, \ldots, 0) \in \mathbb{C}^n$. Using (15), we calculate

$$\frac{\Omega_{\boldsymbol{v}}(\boldsymbol{z} + \boldsymbol{w}; \Lambda)}{\Omega_{\boldsymbol{v}}(\boldsymbol{z}; \Lambda)} = \frac{\lambda(v_1 \omega)}{\lambda(\omega)^{v_1^2}} = 1$$

where the last equality holds because λ is a quadratic form. Thus $\Omega_{\boldsymbol{v}}$ is invariant under adding a period to the variable z_1. Similarly $\Omega_{\boldsymbol{v}}$ is elliptic in each variable on $(\mathbb{C}/\Lambda)^n$. □

Proposition 3.4. *Fix a lattice $\Lambda \in \mathbb{C}$. Let $\boldsymbol{v} \in \mathbb{Z}^m$ and $\boldsymbol{z} \in \mathbb{C}^n$. Let T be an $n \times m$ matrix with entries in $\mathbb{Z}$ and transpose T^{tr}. Then*

$$\Omega_{\boldsymbol{v}}(T^{tr}(\boldsymbol{z}); \Lambda) = \frac{\Omega_{T(\boldsymbol{v})}(\boldsymbol{z}; \Lambda)}{\prod_{i=1}^{n} \Omega_{T(\boldsymbol{e}_i)}(\boldsymbol{z}; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} \Omega_{T(\boldsymbol{e}_i + \boldsymbol{e}_j)}(\boldsymbol{z}; \Lambda)^{v_i v_j}}.$$

Proof. A straightforward calculation using Definition 3.1. □

Let $\wp$ and ζ denote the usual Weierstrass functions.

Lemma 3.5.

(a) $$\wp(u) - \wp(v) = -\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}.$$

(b) $$\wp(\boldsymbol{v}\cdot z) - \wp(\boldsymbol{w}\cdot z) = -\frac{\Omega_{\boldsymbol{v}+\boldsymbol{w}}(z)\Omega_{\boldsymbol{v}-\boldsymbol{w}}(z)}{\Omega_{\boldsymbol{v}}(z)^2\Omega_{\boldsymbol{w}}(z)^2}.$$

Proof. Part (a) is well-known; see [Chandrasekharan 1985], for example. Part (b) follows by direct calculation using Definition 3.1. □

Lemma 3.6.

(a) $$\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b) = \frac{\sigma(x+a+b)\sigma(x)\sigma(a-b)}{\sigma(x+a)\sigma(x+b)\sigma(a)\sigma(b)}.$$

(b) $$\zeta(x+a+b) - \zeta(x+a) - \zeta(x+b) + \zeta(x) = \frac{\sigma(2x+a+b)\sigma(a)\sigma(b)}{\sigma(x+a+b)\sigma(x+a)\sigma(x+b)\sigma(x)}.$$

Proof. (a) Denote by f and g the two sides of the equation to be proved. Considered as functions of any one of x, a or b, these are elliptic functions. Suppose that $a, b \notin \Lambda$. Consider f and g as functions of x. The set of poles of f or g is $\{-a, -b\}$. The zeroes of g (the right-hand side) are at $-a-b$ and 0. These are also zeroes of f, since ζ is an odd function. Hence $f = cg$ for some c not depending on x. Now define instead

$$F = (\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b))\,\sigma(x+a)\sigma(x+b),$$
$$G = \sigma(x+a+b)\sigma(x).$$

We have $F = c'G$ for some constant c' independent of x. Taking derivatives and evaluating at $x = 0$, we have

$$(\wp(b) - \wp(a))\,\sigma(a)\sigma(b) = c'\sigma(a+b)\sigma'(0)$$

We have $\sigma'(0) = 1$. By Lemma 3.5, we then have

$$c' = -\frac{\sigma(a-b)}{\sigma(a)\sigma(b)}$$

which concludes the proof of (a). Part (b) is obtained by a change of variables $x \leftarrow a$, $a \leftarrow x+b$, $b \leftarrow x$. □

Forming the elliptic net.

Theorem 3.7. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. Fix $z_1, \ldots, z_n \in \mathbb{C}$. Then the function $W : \mathbb{Z}^n \to \mathbb{C}$ defined by*

$$W(\boldsymbol{v}) = \Omega_{\boldsymbol{v}}(z_1, \ldots, z_n; \Lambda)$$

is an elliptic net.

Proof. For notational simplicity, we drop the arguments z_i, Λ on $\Omega_{\boldsymbol{v}}$ and also write $\sigma(\boldsymbol{v})$, $\wp(\boldsymbol{v})$ and $\zeta(\boldsymbol{v})$ for $\sigma(v_1z_1+\cdots+v_nz_n)$, $\wp(v_1z_1+\cdots+v_nz_n)$ and $\zeta(v_1z_1+\cdots+v_nz_n)$. We observe that $\boldsymbol{v}=\boldsymbol{0}$ if and only if $\Omega_{\boldsymbol{v}}\equiv 0$.

We intend to show that (3) holds for W in $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$ and $\boldsymbol{s}$. If any one of $\boldsymbol{p}$, $\boldsymbol{q}$ or $\boldsymbol{r}$ are zero, then (3) holds trivially (note that σ is an odd function, so that $\Omega_{-\boldsymbol{v}}=-\Omega_{\boldsymbol{v}}$). Hence we may assume that none of $\Omega_{\boldsymbol{p}}$, $\Omega_{\boldsymbol{q}}$, or $\Omega_{\boldsymbol{r}}$ is identically zero. For any quadratic form f defined on $\mathbb{Z}^n$, we have the following relation for all $\boldsymbol{p},\boldsymbol{q},\boldsymbol{s}\in\mathbb{Z}^n$:

$$f(\boldsymbol{p}+\boldsymbol{q}+\boldsymbol{s})+f(\boldsymbol{p}-\boldsymbol{q})+f(\boldsymbol{s})-f(\boldsymbol{p}+\boldsymbol{s})-f(\boldsymbol{p})-f(\boldsymbol{q}+\boldsymbol{s})-f(\boldsymbol{q})=0. \quad (16)$$

First we address the case that $\boldsymbol{s}=\boldsymbol{0}$. By (16) and Lemma 3.5,

$$\frac{\Omega_{\boldsymbol{p}+\boldsymbol{q}}\Omega_{\boldsymbol{p}-\boldsymbol{q}}}{\Omega_{\boldsymbol{p}}^2\Omega_{\boldsymbol{q}}^2}=\frac{\sigma(\boldsymbol{p}+\boldsymbol{q})\sigma(\boldsymbol{p}-\boldsymbol{q})}{\sigma(\boldsymbol{p})^2\sigma(\boldsymbol{q})^2}=\wp(\boldsymbol{q})-\wp(\boldsymbol{p}).$$

Therefore, we have

$$\frac{\Omega_{\boldsymbol{p}+\boldsymbol{q}}\Omega_{\boldsymbol{p}-\boldsymbol{q}}}{\Omega_{\boldsymbol{p}}^2\Omega_{\boldsymbol{q}}^2}+\frac{\Omega_{\boldsymbol{q}+\boldsymbol{r}}\Omega_{\boldsymbol{q}-\boldsymbol{r}}}{\Omega_{\boldsymbol{q}}^2\Omega_{\boldsymbol{r}}^2}+\frac{\Omega_{\boldsymbol{r}+\boldsymbol{p}}\Omega_{\boldsymbol{r}-\boldsymbol{p}}}{\Omega_{\boldsymbol{r}}^2\Omega_{\boldsymbol{p}}^2}=0,$$

which gives the relation (3) for $\boldsymbol{s}=\boldsymbol{0}$, that is,

$$\Omega_{\boldsymbol{p}+\boldsymbol{q}}\Omega_{\boldsymbol{p}-\boldsymbol{q}}\Omega_{\boldsymbol{r}}^2+\Omega_{\boldsymbol{q}+\boldsymbol{r}}\Omega_{\boldsymbol{q}-\boldsymbol{r}}\Omega_{\boldsymbol{p}}^2+\Omega_{\boldsymbol{r}+\boldsymbol{p}}\Omega_{\boldsymbol{r}-\boldsymbol{p}}\Omega_{\boldsymbol{q}}^2=0.$$

Now suppose that $\boldsymbol{s}\neq\boldsymbol{0}$ and so $\Omega_{\boldsymbol{s}}\not\equiv 0$. By (16) and Lemma 3.6,

$$\begin{aligned}\frac{\Omega_{\boldsymbol{p}+\boldsymbol{q}+\boldsymbol{s}}\Omega_{\boldsymbol{p}-\boldsymbol{q}}\Omega_{\boldsymbol{s}}}{\Omega_{\boldsymbol{p}+\boldsymbol{s}}\Omega_{\boldsymbol{p}}\Omega_{\boldsymbol{q}+\boldsymbol{s}}\Omega_{\boldsymbol{q}}}&=\frac{\sigma(\boldsymbol{p}+\boldsymbol{q}+\boldsymbol{s})\sigma(\boldsymbol{p}-\boldsymbol{q})\sigma(\boldsymbol{s})}{\sigma(\boldsymbol{p}+\boldsymbol{s})\sigma(\boldsymbol{p})\sigma(\boldsymbol{q}+\boldsymbol{s})\sigma(\boldsymbol{q})}\\&=\zeta(\boldsymbol{p}+\boldsymbol{s})-\zeta(\boldsymbol{p})-\zeta(\boldsymbol{q}+\boldsymbol{s})+\zeta(\boldsymbol{q}).\end{aligned}$$

Therefore, we have

$$\frac{\Omega_{\boldsymbol{p}+\boldsymbol{q}+\boldsymbol{s}}\Omega_{\boldsymbol{p}-\boldsymbol{q}}\Omega_{\boldsymbol{s}}}{\Omega_{\boldsymbol{p}+\boldsymbol{s}}\Omega_{\boldsymbol{p}}\Omega_{\boldsymbol{q}+\boldsymbol{s}}\Omega_{\boldsymbol{q}}}+\frac{\Omega_{\boldsymbol{q}+\boldsymbol{r}+\boldsymbol{s}}\Omega_{\boldsymbol{q}-\boldsymbol{r}}\Omega_{\boldsymbol{s}}}{\Omega_{\boldsymbol{q}+\boldsymbol{s}}\Omega_{\boldsymbol{q}}\Omega_{\boldsymbol{r}+\boldsymbol{s}}\Omega_{\boldsymbol{r}}}+\frac{\Omega_{\boldsymbol{r}+\boldsymbol{p}+\boldsymbol{s}}\Omega_{\boldsymbol{r}-\boldsymbol{p}}\Omega_{\boldsymbol{s}}}{\Omega_{\boldsymbol{r}+\boldsymbol{s}}\Omega_{\boldsymbol{r}}\Omega_{\boldsymbol{p}+\boldsymbol{s}}\Omega_{\boldsymbol{p}}}=0,$$

or, more simply,

$$\Omega_{\boldsymbol{p}+\boldsymbol{q}+\boldsymbol{s}}\Omega_{\boldsymbol{p}-\boldsymbol{q}}\Omega_{\boldsymbol{r}+\boldsymbol{s}}\Omega_{\boldsymbol{r}}+\Omega_{\boldsymbol{q}+\boldsymbol{r}+\boldsymbol{s}}\Omega_{\boldsymbol{q}-\boldsymbol{r}}\Omega_{\boldsymbol{p}+\boldsymbol{s}}\Omega_{\boldsymbol{p}}+\Omega_{\boldsymbol{r}+\boldsymbol{p}+\boldsymbol{s}}\Omega_{\boldsymbol{r}-\boldsymbol{p}}\Omega_{\boldsymbol{q}+\boldsymbol{s}}\Omega_{\boldsymbol{q}}=0,$$

which is what was required to prove. □

The identity (3) for $\Omega_{\boldsymbol{v}}$ is similar to several identities known in complex function theory [Gasper and Rahman 2004; Wenchang et al. 1996].

Explicit rational functions. Elliptic functions for a lattice Λ of $\mathbb{C}$ give rational functions on the associated elliptic curve (via complex uniformization). If we give a Weierstrass model for the same elliptic curve, we can give explicit expressions for the rational functions as elements of the usual field of rational functions associated to the model. In the following proposition, we do this for $\Omega_{\boldsymbol{v}}$ for some small $\boldsymbol{v} \in \mathbb{Z}^n$, for $n = 1, 2, 3$.

Proposition 3.8. *Consider an elliptic curve E, and a Weierstrass model for E given by*

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

As usual, let

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

To E we can also associate a complex uniformization and elliptic functions $\Omega_{\boldsymbol{v}}$ as above. As rational functions on E, we have the following equalities.

For $n = 1$:

$$\Omega_1 = 1, \qquad \Omega_2 = 2y + a_1x + a_3,$$
$$\Omega_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \; cr\Omega_4 = (2y + a_1x + a_3)$$
$$\left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2\right).$$

For $n = 2$:

$$\Omega_{(1,0)} = \Omega_{(0,1)} = \Omega_{(1,1)} = 1,$$
$$\Omega_{(1,-1)} = x_2 - x_1, \qquad \Omega_{(-1,1)} = x_1 - x_2,$$
$$\Omega_{(2,1)} = 2x_1 + x_2 - \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - a_1\left(\frac{y_2-y_1}{x_2-x_1}\right) + a_2,$$
$$\Omega_{(1,2)} = x_1 + 2x_2 - \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - a_1\left(\frac{y_2-y_1}{x_2-x_1}\right) + a_2.$$

For $n = 3$:

$$\Omega_{(1,0,0)} = \Omega_{(0,1,0)} = \Omega_{(0,0,1)} = \Omega_{(1,1,0)} = \Omega_{(0,1,1)} = \Omega_{(1,0,1)} = 1,$$
$$\Omega_{(1,-1,0)} = x_2 - x_1, \quad \Omega_{(0,1,-1)} = x_3 - x_2, \quad \Omega_{(-1,0,1)} = x_1 - x_3,$$
$$\Omega_{(-1,1,0)} = x_1 - x_2, \quad \Omega_{(0,-1,1)} = x_2 - x_3, \quad \Omega_{(1,0,-1)} = x_3 - x_1,$$
$$\Omega_{(1,1,1)} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)},$$

$$\Omega_{(-1,1,1)} = \frac{y_1(x_2-x_3)-y_2(x_3-x_1)-y_3(x_1-x_2)}{(x_2-x_3)} + a_1x_1 + a_3,$$
$$\Omega_{(1,-1,1)} = \frac{-y_1(x_2-x_3)+y_2(x_3-x_1)-y_3(x_1-x_2)}{(x_3-x_1)} + a_1x_2 + a_3,$$
$$\Omega_{(1,1,-1)} = \frac{-y_1(x_2-x_3)-y_2(x_3-x_1)+y_3(x_1-x_2)}{(x_1-x_2)} + a_1x_3 + a_3.$$

Proof. The division polynomial formulae (the $n = 1$ case) are well-known; see [Chandrasekharan 1985], [Frey and Lange 2006, p. 80], or [Silverman 2009, Exercise 3.7]. The formulae for $n = 2$ and the related first three lines of formulae for $n = 3$ are immediate consequences of Lemma 3.5 and the addition law for elliptic curves [Silverman 2009, Algorithm 2.3]. Only the cases where $n = 3$, $v_i \neq 0$ for all $i = 1, 2, 3$ are not immediate: these formulae are a result of the proof of Lemma 2.6. Note that using Remark 2.7 results in the same formulae. □

4. Net polynomials over arbitrary fields

In the last section, we defined elliptic functions $\Omega_{\boldsymbol{v}}$ in the case of $\mathbb{C}/\Lambda$. In this section we wish to define the same rational functions for any elliptic curve over any field, calling them $\Psi_{\boldsymbol{v}}$, the *net polynomials*. We will start from the results of the last section.

Defining net polynomials. Let $R = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$ be a polynomial ring over $\mathbb{Q}$ in the variables α_i. Define $f(x, y) \in R[x, y]$ by

$$f(x, y) = y^2 + \alpha_1xy + \alpha_3y - x^3 - \alpha_2x^2 - \alpha_4x - \alpha_6.$$

Consider the affine scheme $\mathscr{E} : f(x, y) = 0$ over R. Let $\boldsymbol{a} = (a_i) \in \mathbb{C}^5$. The association $(\alpha_i) \mapsto (a_i)$ gives a map $\phi_{\boldsymbol{a}} : R \to \mathbb{C}$. Consider the affine variety over $\mathbb{C}$ given by

$$C_{\boldsymbol{a}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then $\phi_{\boldsymbol{a}}$ gives rise to a Cartesian diagram

$$\begin{array}{ccc} \mathscr{E}^n & \longleftarrow & C_{\boldsymbol{a}}^n \\ \downarrow & & \downarrow \\ \operatorname{Spec}(R) & \longleftarrow & \operatorname{Spec}(\mathbb{C}) \end{array}$$

where $\mathscr{E}^n = \mathscr{E} \times_{\operatorname{Spec} R} \cdots \times_{\operatorname{Spec} R} \mathscr{E}$ is the n-fold fibre product of $\mathscr{E}$ with itself over R.

The rational functions $\Omega_{\boldsymbol{v}} \in \mathscr{K}(C_{\boldsymbol{a}}^n)$ have rational expressions in x, y and the a_i (in terms of the Weierstrass model, as in for example Proposition 3.8). These expressions have rational coefficients by construction and the general theory of

sigma functions (the divisors are Galois invariant). So these same expressions (with a_i replaced with α_i) give rational functions $\Psi_{\boldsymbol{v}} \in \mathcal{K}(\mathscr{E}^n)$.

Theorem 4.1. *Let $n \geq 1$. Denote by $\mathcal{K}(\mathscr{E}^n)$ the field of rational functions on $\mathscr{E}^n$. There exists a unique system of functions $\Psi_{\boldsymbol{v}} \in \mathcal{K}(\mathscr{E}^n)$ depending on $\boldsymbol{v} \in \mathbb{Z}^n$ such that*

(a) *the map*

$$W : \mathbb{Z}^n \to \mathcal{K}(\mathscr{E}^n), \quad \boldsymbol{v} \mapsto \Psi_{\boldsymbol{v}}$$

is an elliptic net, and

(b) *whenever $C_{\boldsymbol{a}}$ is elliptic, the restriction of $\Psi_{\boldsymbol{v}}$ to a fibre $C_{\boldsymbol{a}}^n$ is the rational function $\Omega_{\boldsymbol{v}}$.on $C_{\boldsymbol{a}}^n$.*

Proof. The union of the $C_{\boldsymbol{a}}^n$ for which $C_{\boldsymbol{a}}$ is an elliptic curve is Zariski dense, and so the $\Psi_{\boldsymbol{v}}$ are determined uniquely by their restrictions to these fibres. □

We call these $\Psi_{\boldsymbol{v}}$ the *net polynomials*; we will discuss shortly the "polynomial" ring $\mathcal{R}_n$ in which they live.

We transfer some useful properties of the $\Omega_{\boldsymbol{v}}$ to properties of the $\Psi_{\boldsymbol{v}}$ on $\mathscr{E}^n$. Again, there are unique rational functions X and Y for $\mathscr{E}$ whose restriction to elliptic $C_{\boldsymbol{a}}$ correspond to the Weierstrass functions $\wp$ and $\frac{1}{2}\wp'$. Each $\boldsymbol{v} \in \mathbb{Z}^n$ gives rise to a map $\boldsymbol{v} : \mathscr{E}^n \to \mathscr{E}$ which is the linear combination associated to the vector $\boldsymbol{v}$ (e.g., $(1, 1)$ is the usual group law). Define rational functions $X_{\boldsymbol{v}} = X \circ \boldsymbol{v}$ and $Y_{\boldsymbol{v}} = Y \circ \boldsymbol{v}$ on $\mathscr{E}^n$.

The next lemma follows immediately from Lemma 3.5.

Lemma 4.2. $$\Psi_{\boldsymbol{v}}^2 \Psi_{\boldsymbol{w}}^2 (X_{\boldsymbol{v}} - X_{\boldsymbol{w}}) = -\Psi_{\boldsymbol{v}+\boldsymbol{w}} \Psi_{\boldsymbol{v}-\boldsymbol{w}}.$$

More generally, there is a map $T : \mathscr{E}^m \to \mathscr{E}^n$ associated to any $T \in M_{n\times m}(\mathbb{Z})$. The next proposition follows from Proposition 3.4.

Proposition 4.3. *Let $\boldsymbol{v} \in \mathbb{Z}^n$. Let T be any $n \times m$ matrix with entries in $\mathbb{Z}$ and transpose T^{tr}. Then*

$$(\Psi_{\boldsymbol{v}} \circ T) \prod_{i=1}^{n} \Psi_{T^{tr}(\boldsymbol{e}_i)}^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \leq i < j \leq n} \Psi_{T^{tr}(\boldsymbol{e}_i + \boldsymbol{e}_j)}^{v_i v_j} = \Psi_{T^{tr}(\boldsymbol{v})}. \tag{17}$$

Net polynomials at primes. In this section we determine a little more about the exact nature of the elliptic net $\Psi_{\boldsymbol{v}}$. In particular, we wish to restrict the possible divisor of $\Psi_{\boldsymbol{v}}$, and show that it has zero valuation for certain primes.

Consider the ring $S = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$. Since $f(x, y)$ is defined over S, we may define $\mathscr{E}_S : f(x, y) = 0$ as a scheme over Spec S whose fibre over Spec R is

$\mathscr{E}$. Then $\mathscr{E}_S^n = \mathscr{E}_S \times_{\operatorname{Spec} S} \cdots \times_{\operatorname{Spec} S} \mathscr{E}_S$ is a scheme over Spec S whose fibre over Spec R is $\mathscr{E}^n$. Define

$$\mathscr{R}_n = S[x_i, y_i]_{1\le i\le n}\left[(x_i - x_j)^{-1}\right]_{1\le i<j\le n} \Big/ \langle f(x_i, y_i)\rangle_{1\le i\le n}.$$

The ring $\mathscr{R}_n$ is the affine coordinate ring of the affine piece of $\mathscr{E}_S^n$ obtained by removing all the diagonals and antidiagonals, in the sense of the elliptic curve group law (in other words, on an elliptic curve fibre, $x_i = x_j$ if and only if the corresponding points satisfy $P_i = \pm P_j$). There is a natural identification of $\mathscr{R}_n$ with a subset of $\mathscr{K}(\mathscr{E}^n)$.

Theorem 4.4. *The functions $\Psi_{\boldsymbol{v}}$ are elements of $\mathscr{R}_n$. Let $\mathfrak{p}$ be any prime of $\mathscr{R}_n$ which is a lift of a prime of S. Then $\Psi_{\boldsymbol{v}} \notin \mathfrak{p}$.*

The lifted ideal $\mathfrak{p} = \mathfrak{q}\mathscr{R}_n$ is prime whenever $\mathfrak{q}$ is a prime of S. The proof of the theorem will involve showing for all valuations v associated to such primes $\mathfrak{p}$ that $v(\Psi_{\boldsymbol{v}})$ (slightly modified) is a quadratic form with certain vanishing. Then the following lemma will establish that this function is identically zero.

Let B and C be abelian groups written additively. The function $f : B \to C$ is a *quadratic form* if for all $x, y, z \in B$,

$$f(x+y+z) - f(x+y) - f(y+z) - f(x+z) + f(x) + f(y) + f(z) = 0.$$

If f is a quadratic form, then for all $x, y \in B$,

$$f(x+y) + f(x-y) - 2f(x) - 2f(y) = 0.$$

The converse holds if C is 2-torsion free.

Lemma 4.5. *Let $M : \mathbb{Z}^n \to \mathbb{Z}$ be a quadratic form. Suppose that $M(\boldsymbol{v}) = 0$ for all $\boldsymbol{v} = \boldsymbol{e}_i$ and $\boldsymbol{v} = \boldsymbol{e}_i + \boldsymbol{e}_j$ (i.e., for standard basis vectors and their two-term sums). Then $M(\boldsymbol{v}) = 0$ for all $\boldsymbol{v}$.*

Proof. It is well-known that any value of a quadratic form can be given in terms of its value at a certain "base" of vectors. In particular,

$$f\left(\sum_{i=1}^n a_i \boldsymbol{e}_i\right) = \sum_{i=1}^n \left(2a_i^2 - \sum_{j=1}^n a_i a_j\right) f(\boldsymbol{e}_i) + \sum_{1\le i<j\le n} a_i a_j f(\boldsymbol{e}_i + \boldsymbol{e}_j). \qquad \square$$

Proof of Theorem 4.4. Each $\Psi_{\boldsymbol{v}} \in \mathscr{K}(\mathscr{E}^n)$ has a corresponding Weil divisor. Suppose a codimension-one subscheme X appears as a summand in this divisor, and let $\widetilde{X} = X \cap C_{\boldsymbol{a}}^n$. If $C_{\boldsymbol{a}}$ is elliptic, $\widetilde{X} \neq \varnothing$, and $\widetilde{X} \neq C_{\boldsymbol{a}}^n$, then $\widetilde{X}$ is of codimension one in $C_{\boldsymbol{a}}^n$ and appears in the divisor of $\Omega_{\boldsymbol{v}}$ to the same order as X appears in the divisor of $\Psi_{\boldsymbol{v}}$. Definition 3.1 determines the divisors of $\Omega_{\boldsymbol{v}}$ and this restricts the possible divisors for $\Psi_{\boldsymbol{v}}$. In particular, it shows that $s\Psi_{\boldsymbol{v}} \in \mathscr{R}_n$, where $s \in S$.

Therefore, taking v to be a valuation of $\mathcal{R}_n$ lifted from a valuation of S associated to a prime $\mathfrak{q}$ of S, it will suffice to show that $v(\Psi_{\boldsymbol{v}}) = 0$ for all $\boldsymbol{v} \in \mathbb{Z}^n$.

Lemma 4.2 implies

$$X_{\boldsymbol{v}} - X_{\boldsymbol{w}} = -\frac{\Psi_{\boldsymbol{v}+\boldsymbol{w}}\Psi_{\boldsymbol{v}-\boldsymbol{w}}}{\Psi_{\boldsymbol{v}}^2\Psi_{\boldsymbol{w}}^2}.$$

We claim that $v(X_{\boldsymbol{v}} - X_{\boldsymbol{w}}) = 0$ whenever $\boldsymbol{v} \neq \pm\boldsymbol{w}$, $\boldsymbol{v} \neq 0$, and $\boldsymbol{w} \neq 0$.

First suppose $v(X_{\boldsymbol{v}} - X_{\boldsymbol{w}}) < 0$; we show that $\boldsymbol{v} = 0$ or $\boldsymbol{w} = 0$. Indeed, we know that $v(X_{\boldsymbol{v}}) < 0$ or $v(X_{\boldsymbol{w}}) < 0$. Suppose $v(X_{\boldsymbol{v}}) < 0$. This implies that $\boldsymbol{v}(\boldsymbol{P}) = \mathbb{O}$ for all $\boldsymbol{P}$ on the nonsingular part of the fibre over $\mathfrak{q}$ of $\mathscr{E}_S$. Since $\boldsymbol{P}$ ranges over all possible values (e.g., $\boldsymbol{P} = (P, \mathbb{O}, \ldots, \mathbb{O})$), we find that this implies that $[v_i] = [0]$ for all i. In turn, this shows that $\boldsymbol{v} = 0$. Similarly, if $v(X_{\boldsymbol{w}}) < 0$, then $\boldsymbol{w} = 0$.

Next suppose $v(X_{\boldsymbol{v}} - X_{\boldsymbol{w}}) > 0$; we show that $\boldsymbol{v} = \pm\boldsymbol{w}$. Suppose the valuation is positive. Then $\boldsymbol{v}(\boldsymbol{P}) = \pm\boldsymbol{w}(\boldsymbol{P})$ for all $\boldsymbol{P}$ on the nonsingular part of the fibre over $\mathfrak{q}$ of $\mathscr{E}_S$. Since $\boldsymbol{P}$ ranges over all possible values (e.g., $\boldsymbol{P} = (P, \mathbb{O}, \ldots, \mathbb{O})$ or $\boldsymbol{P} = (P, P, \mathbb{O}, \ldots, \mathbb{O})$), we find that this implies, in particular, that for all $0 \leq i \leq j \leq n$, we have $[v_i \pm w_i] = [0]$ and $[v_i + v_j \pm (w_i + w_j)] = [0]$ on $\mathscr{E}_S$. In turn, this gives $v_i = \pm w_i$ and $v_i + v_j = \pm(w_i + w_j)$. Together these imply that $\boldsymbol{v} = \pm\boldsymbol{w}$. This demonstrates the claim.

Define a function $M : \mathbb{Z}^n \to \mathbb{Z}$ by

$$M(\boldsymbol{v}) = \begin{cases} v(\Psi_{\boldsymbol{v}}) & \text{if } \boldsymbol{v} \neq 0, \\ 0 & \text{if } \boldsymbol{v} = 0. \end{cases}$$

Note that $M(-\boldsymbol{v}) = M(\boldsymbol{v})$, from which one can deduce that

$$M(\boldsymbol{v}+\boldsymbol{w}) + M(\boldsymbol{v}-\boldsymbol{w}) - 2M(\boldsymbol{v}) - 2M(\boldsymbol{w}) = 0 \tag{18}$$

whenever $\boldsymbol{v} = 0$ or $\boldsymbol{w} = 0$. Our work up until now has shown that (18) holds in all other cases except $\boldsymbol{v} + \boldsymbol{w} = 0$ or $\boldsymbol{v} - \boldsymbol{w} = 0$. These remaining two cases reduce to the statement that for all $\boldsymbol{u}$, $M(2\boldsymbol{u}) = 4M(\boldsymbol{u})$. To obtain this, take the sum of the four instances of (18) with $(\boldsymbol{v}, \boldsymbol{w})$ respectively taking the values $(4\boldsymbol{u}, \boldsymbol{u})$, $(3\boldsymbol{u}, \boldsymbol{u})$, $(3\boldsymbol{u}, \boldsymbol{u})$ and $(2\boldsymbol{u}, \boldsymbol{u})$, and then subtract the instance of (18) with $(\boldsymbol{v}, \boldsymbol{w}) = (3\boldsymbol{u}, 2\boldsymbol{u})$.

We have shown that (18) holds for all $\boldsymbol{v}$ and $\boldsymbol{w}$, and that therefore $M : \mathbb{Z}^n \to \mathbb{Z}$ is a quadratic form (since $\mathbb{Z}$ is 2-torsion free). The other assumptions of Lemma 4.5 are verified by Proposition 3.8. Therefore, M is identically zero, which is what was required to prove. □

Summary. Let $n \geq 1$. For any elliptic curve or scheme C, let $\mathbb{O}$ denote the identity, $[m] : C \to C$ denote multiplication by m, $p_i : C^n \to C$ denote projection onto the i-th component, and $s : C^n \to C$ denote sum of all components. For $\boldsymbol{v} \in \mathbb{Z}^n$, define

the expression

$$D_{C,\boldsymbol{v}} = ([v_1] \times \cdots \times [v_n])^* s^*(\mathbb{O}) - \sum_{1 \le k < j \le n} v_k v_j (p_k^* \times p_j^*) s^*(\mathbb{O}) - \sum_{k=1}^{n} \left(2v_k^2 - \sum_{j=1}^{n} v_k v_j \right) p_k^*(\mathbb{O}),$$

which is a divisor on the n-fold product C^n. Over the complex numbers, the functions $\Omega_{\boldsymbol{v}}$ have these divisors and satisfy the elliptic net recurrence (3) (see Section 3).

We now collect the results of the previous sections in one statement.

Theorem 4.6. *Let $n \ge 1$. There exists a unique collection of rational functions $\Psi_{\boldsymbol{v}} \in \mathcal{K}(\mathcal{E}_S^n)$ for each $\boldsymbol{v} \in \mathbb{Z}^n$ satisfying these conditions*:

(a) *The map $\boldsymbol{v} \mapsto \Psi_{\boldsymbol{v}}$ gives an elliptic net $W : \mathbb{Z}^n \to \mathcal{R}_n$.*

(b) $\Psi_{\boldsymbol{v}} = 1$ *whenever $\boldsymbol{v} = \boldsymbol{e}_i$ for some $1 \le i \le n$ or $\boldsymbol{v} = \boldsymbol{e}_i + \boldsymbol{e}_j$ for some $1 \le i < j \le n$.*

(c) $\mathrm{Div}(\Psi_{\boldsymbol{v}}) = D_{\mathcal{E}_S, \boldsymbol{v}}$.

Proof. Part (a) follows from Theorems 4.1 and 4.4. Part (b) follows from Proposition 3.8 and Theorem 4.1. Part (c) follows from Theorem 4.4. □

5. Elliptic nets from elliptic curves

In light of Theorem 4.6, it is now natural to define an elliptic net associated to any cubic Weierstrass curve over any field.

Definition 5.1. Let K be any field. Let $a_1, a_2, a_3, a_4, a_6 \in K$. To this we associate a map

$$S = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6] \to K, \quad \alpha_i \mapsto a_i.$$

Let

$$f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$$

and let C be a curve defined by $f(x, y) = 0$. Then we have a Cartesian diagram

$$\begin{array}{ccc} \mathcal{E}_S^n & \longleftarrow & C^n \\ \downarrow & & \downarrow \\ \mathrm{Spec}(S) & \longleftarrow & \mathrm{Spec}(K) \end{array}$$

under which we may pullback $\Psi_{\boldsymbol{v}}$ to obtain $\phi_{\boldsymbol{v}} \in \mathcal{K}(C^n)$ (this is possible since the fibre on the right is not contained in the support of the divisor of $\Psi_{\boldsymbol{v}}$, by Theorem 4.6).

The nonsingular points of C defined over K, denoted $C_{\text{ns}}(K)$, form a group. We call a set of points $\{P_1, \ldots, P_n\}$ on the nonsingular part C_{ns} of a cubic curve *appropriate* if

(a) $P_i \neq 0$ for all i, (b) $[2]P_i \neq 0$ for all i,

(c) $P_i \neq \pm P_j$ for any $i \neq j$, and (d) $[3]P_1 \neq 0$ whenever $n = 1$.

If we have an appropriate n-tuple of points $\boldsymbol{P} \in C_{\text{ns}}(K)^n$, we may define a map

$$W_{C,\boldsymbol{P}} : \mathbb{Z}^n \to K$$

by setting $W_{C,\boldsymbol{P}}(\boldsymbol{v}) = \phi_{\boldsymbol{v}}(\boldsymbol{P})$. By Theorem 4.6, this will be an elliptic net. This will be called *the elliptic net associated to C and $\boldsymbol{P}$*.

We have the following additional corollary to Theorem 4.6.

Corollary 5.2. *For an elliptic net $W_{C,\boldsymbol{P}} : \mathbb{Z}^n \to K$ associated to a curve C and nonsingular points $\boldsymbol{P}$, we have $W(\boldsymbol{v}) = 0$ if and only if $\boldsymbol{v}(\boldsymbol{P}) = \mathbb{O}$ on C_{ns}.*

Proof. This follows from the statement that $\Omega_{\boldsymbol{v}}(\boldsymbol{v} \cdot \boldsymbol{z}) = 0$ if and only if $\boldsymbol{v} \cdot \boldsymbol{z} \in \Lambda$ (see Section 3). □

Example 5.3. In (4) (page 201) we displayed an example elliptic net $W_{E,(P,Q)}$ associated to the elliptic curve and points

$$E : y^2 + y = x^3 + x^2 - 2x, \quad P = (0, 0), \quad Q = (1, 0)$$

Some of the smaller terms of this net can be calculated using Proposition 3.8; for example,

$$W(0,0) = 0, \quad W(1,0) = W(0,1) = W(1,1) = 1,$$
$$W(2,0) = 2y_1 + a_1x_1 + a_3 = 1, \qquad W(0,2) = 2y_2 + a_1x_2 + a_3 = 1,$$
$$W(1,-1) = x_2 - x_1 = 1,$$
$$W(2,1) = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2 = 2,$$
$$W(2,-1) = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 = -1.$$

More terms can be calculated using the recurrence relation (3). Since P and Q are independent nontorsion points, there are no zeroes in the array except the zero located at the origin ($W(0,0) = 0$). The row through the term 0 is the elliptic divisibility sequence associated to E and P, which begins

$$1,\ 1,\ -3,\ 11,\ 38,\ 249,\ -2357,\ 8767,\ 496035,\ -3769372,\ -299154043,$$
$$-12064147359,\ 632926474117,\ -65604679199921,\ \ldots$$

The column through 0 is the elliptic divisibility sequence associated to Q.

6. Elliptic curves from elliptic nets

We are now in a position to use the results of Section 2 to determine exactly which elliptic curves (or more generally cubic Weierstrass curves) give rise to any given elliptic net.

Scale equivalence and normalization.

Proposition 6.1. *Let $W : A \to K$ be an elliptic net. Let $f : A \to K^*$ be a quadratic form. Define $W^f : A \to K$ by*

$$W^f(\boldsymbol{v}) = f(\boldsymbol{v})W(\boldsymbol{v}).$$

Then W^f is an elliptic net.

Proof. Let $p, q, r, s \in A$. We use multiplicative notation in K^*, so that f satisfies

$$f(p+q+s)f(p)f(q)f(s)f(p+q)^{-1}f(q+s)^{-1}f(p+s)^{-1} = 1. \tag{19}$$

The parallelogram law for quadratic forms (written multiplicatively) states that

$$f(p-q)f(p+q) = f(p)^2 f(q)^2. \tag{20}$$

Multiplying $f(r)f(r+s)$ and equations (19) and (20) together, we obtain

$$f(p+q+s)f(p-q)f(r+s)f(r) = f(q+s)f(p+s)f(r+s)f(p)f(q)f(r)f(s)^{-1},$$

which is symmetric in p, q, and r, so

$$\begin{aligned} f(p+q+s)f(p-q)f(r+s)f(r) &= f(q+r+s)f(q-r)f(p+s)f(p) \\ &= f(r+p+s)f(r-p)f(q+s)f(q), \end{aligned}$$

which shows that the recurrence (3) holds for W^f if it does for W. □

If two elliptic nets are related in the manner of W and W^f for some quadratic form f, then we call them *scale equivalent*. This is clearly an equivalence relation.

Let $W : \mathbb{Z}^n \to K$ be an elliptic net. We say that W is *normalized* if $W(\boldsymbol{e}_i) = 1$ for all $1 \le i \le n$ and $W(\boldsymbol{e}_i + \boldsymbol{e}_j) = 1$ for all $1 \le i < j \le n$. An elliptic net arising from a curve and points is normalized. It should be stressed that the concept of *normalized* is only defined for elliptic nets with a preferred basis.

If any term of the form $W(\boldsymbol{e}_i)$, $W(2\boldsymbol{e}_i)$, $W(\boldsymbol{e}_i+\boldsymbol{e}_j)$, or $W(\boldsymbol{e}_i-\boldsymbol{e}_j)$ is zero (where $i \ne j$), or if $n = 1$ and any term of the form $W(3\boldsymbol{e}_1)$ is zero, then we say that W is *degenerate*. Compare the definition of *degenerate* to the definition of *appropriate* in Section 5.

Proposition 6.2. *If $W : \mathbb{Z}^n \to K$ is a nondegenerate elliptic net, there is exactly one scaling W^f which is normalized.*

Proof. Define

$$A_{ii} = W(\boldsymbol{e}_i)^{-1}, \quad \text{for } 1 \le i \le n,$$
$$A_{ij} = \frac{W(\boldsymbol{e}_i)W(\boldsymbol{e}_j)}{W(\boldsymbol{e}_i + \boldsymbol{e}_j)}, \quad \text{for } 1 \le i < j \le n,$$
$$f(\boldsymbol{v}) = \prod_{1 \le i \le j \le n} A_{ij}^{v_i v_j}.$$

Then W^f is normalized. Uniqueness follows from the elementary properties of quadratic forms (as in the proof of Lemma 4.5). □

The proof demonstrates that scale equivalence has $\binom{n+1}{2}$ degrees of freedom. If $W : \mathbb{Z}^n \to K$ is an elliptic net, then its *normalization* $\widetilde{W}$ is defined to be the unique normalized elliptic net which is a scaling of W. A *coordinate sublattice* of $\mathbb{Z}^n$ is a sublattice of the form

$$\{\boldsymbol{v} \in \mathbb{Z}^n : v_i = 0 \text{ for } i \notin I\}$$

for some proper nonempty subset $I \subset \{1, 2, \ldots, n\}$. The *rank* of the sublattice is the cardinality of I.

***Curves from nets of ranks* 1 *and* 2.** Define a change of variables of a cubic curve in Weierstrass form to be *unihomothetic* if it is of the form

$$x' = x + r, \quad y' = y + sx + t, \tag{21}$$

for some r, s and t.

The rank-one result in the following form is due to Christine Swart.

Proposition 6.3 [Swart 2003, Theorem 4.5.3]. *Let $W : \mathbb{Z} \to K$ be a normalized nondegenerate elliptic net. Then the family of curve-point pairs (C, P) such that $W = W_{C,P}$ is three dimensional. These are the curve and nonsingular point*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad P = (0, 0),$$

where

$$a_1 = \frac{W(4) + W(2)^5 - 2W(2)W(3)}{W(2)^2W(3)},$$
$$a_2 = \frac{W(2)W(3)^2 + (W(4) + W(2)^5) - W(2)W(3)}{W(2)^3W(3)},$$
$$a_3 = W(2), \qquad a_4 = 1, \qquad a_6 = 0,$$

or any image of these under a unihomothetic change of coordinates.

Proof. A normalized rank 1 nondegenerate elliptic net has $W(2) \neq 0$ and $W(3) \neq 0$. Any singular point $P = (x, y)$ on a cubic Weierstrass curve has vanishing partial derivatives, which implies that $\Psi_2(P) = 2y + a_1x + a_3 = 0$ (see Proposition 3.8). Therefore, if any curve and singular point gives rise to W, then $W(2) = 0$, in contradiction to nondegeneracy. The division polynomials Ψ_1, Ψ_2, Ψ_3 and Ψ_4 are invariant under a change of coordinates of the form (21). Then, it is a simple calculation to check that $W_{C,P}$ agrees with W at the first four terms; hence $W_{C,P} = W$ by Theorem 2.2. Conversely, suppose $W = W_{C',P'}$. After applying a transformation of the form (21) taking P' to $(0, 0)$ and taking a_4 to 1, substitution of the division polynomials into the equations above verifies that $a'_i = a_i$ for all i. □

Proposition 6.4. *Let $W : \mathbb{Z}^2 \to K$ be a normalized nondegenerate elliptic net. Then the family of 3-tuples (C, P_1, P_2) such that $W = W_{C,P_1,P_2}$ is three dimensional. These are the curve and nonsingular points*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
$$P_1 = (0, 0), \quad P_2 = (W(1, 2) - W(2, 1), 0),$$

with

$$a_1 = \frac{W(2, 0) - W(0, 2)}{W(2, 1) - W(1, 2)}, \quad a_2 = 2W(2, 1) - W(1, 2), \quad a_3 = W(2, 0),$$
$$a_4 = (W(2, 1) - W(1, 2))W(2, 1), \qquad a_6 = 0,$$

or any image of these under a unihomothetic change of coordinates.

Proof. In a normalized nondegenerate elliptic net,

$$W(2, 1) - W(1, 2) = W(1, -1) \neq 0, \quad W(2, 0) \neq 0, \quad W(0, 2) \neq 0$$

(see Theorem 2.5). Thus (as in the previous theorem) if a curve and points give rise to W, then the points are nonsingular. The formulae for $W(2, 0)$, $W(0, 2)$, $W(2, 1)$ and $W(1, 2)$ are invariant under a change of coordinates of the form (21). The net W_{C,P_1,P_2} agrees with W at the terms $(2, 0)$, $(0, 2)$, $(2, 1)$ and $(1, 2)$; hence $W_{C,P_1,P_2} = W$ by Theorem 2.5. Conversely, suppose $W = W_{C',P'_1,P'_2}$. After applying a unihomothetic transformation taking P'_1 to $(0, 0)$ and P'_2 to $(W(1, 2) - W(2, 1), 0)$, substitution of the net polynomials into the equations above verifies that $a'_i = a_i$ for all i. □

Example 6.5. Plugging terms from the elliptic net of (4) into the formulae in the statement of Proposition 6.4 we recover the corresponding E, P, and Q.

Remark 6.6. A more symmetric set of equations in the case of characteristic not equal to 2 is as follows:

$$P_1 = (v, 0), \quad P_2 = (-v, 0), \quad 2v = W(2, 1) - W(1, 2),$$

$$a_1 = \frac{W(2,0) - W(0,2)}{W(2,1) - W(1,2)}, \quad 2a_2 = W(2,1) + W(1,2),$$
$$2a_3 = W(2,0) + W(0,2), \quad 4a_4 = -(W(2,1) - W(1,2))^2,$$
$$8a_6 = -(W(2,1) - W(1,2))^2(W(2,1) + W(1,2)).$$

Curves from nets in general rank.

Theorem 6.7. *Let $n \geq 1$. Let $W : \mathbb{Z}^n \to K$ be a normalized nondegenerate elliptic net. Then the set of curves C and $\boldsymbol{P} \in C^n$ such that $W = W_{C,\boldsymbol{P}}$ forms a three-dimensional family of tuples $(C, \boldsymbol{P})$. Further, none of the points $P \in \boldsymbol{P}$ are singular. In particular, the family consists of one such tuple and all its images under unihomothetic changes of coordinates.*

Proof. The proof is by strong induction on n, where the inductive statement has two parts:

(I) The theorem holds for n.

(II) $W(\boldsymbol{v}) \neq 0$ for some $\boldsymbol{v} \in \{\pm 1\}^n$.

The base case consists of ranks $n = 1, 2$. Part (I) is by Propositions 6.3 and 6.4; part (II) is by nondegeneracy, which implies $W(\boldsymbol{e}_1) \neq 0$ and $W(\boldsymbol{e}_1 + \boldsymbol{e}_2) \neq 0$.

Suppose $n \geq 3$ and the inductive statement holds for all $k < n$. Let $W_1, \ldots, W_n$ be the normalized elliptic subnets of W associated to the rank $n-1$ coordinate sublattices $L_i = \{\boldsymbol{v} : v_i = 0\}$. These are defined as nets $W_i : L_i \to K$ but they can be identified with nets $W_i' : \mathbb{Z}^{n-1} \to K$ in the obvious way (by deleting the zero coordinate). They are normalized and nondegenerate (by definition, nondegeneracy at rank n implies nondegeneracy on rank $n-1$ sublattices for $n > 2$). By part (I) the inductive hypothesis, we have $W_i' = W_{C_i,\boldsymbol{P}_i}$ for some curves C_i and nonsingular points $\boldsymbol{P}_i \in C_i^{n-1}$.

We observe a consequence of Proposition 4.3. Suppose $V_1 : \mathbb{Z}^m \to K$ is an elliptic net of rank m associated to C and $\boldsymbol{P}$. Also suppose

$$V_2 : \{\boldsymbol{v} \in \mathbb{Z}^m : v_m = 0\} \to K$$

is the elliptic subnet of V_1 associated to the coordinate sublattice of rank $m-1$ which consists of vectors with last coordinate zero. Suppose $V_2' : \mathbb{Z}^{m-1} \to K$ is naturally identified with V_2 by simply deleting the last coordinate of the domain. Then V_2' is associated to C and $\boldsymbol{P}'$ where $\boldsymbol{P}'$ is simply $\boldsymbol{P}$ with the last coordinate deleted. This statement, appropriately adjusted, holds for any coordinate hyperplane (not just the one with last coordinate zero).

Consider two of the rank $n-1$ subnets, say W_i and W_j. Let $W_{ij} = W_i \cap W_j$ in W. Define $W_{ij}' : \mathbb{Z}^{n-2} \to K$ by the obvious identification. Then, $W_{ij}' = W_{C_{ij},\boldsymbol{P}_{ij}}$ for some curve C_{ij} and $\boldsymbol{P}_{ij} \in C_{ij}^{n-2}$. By the foregoing, $C_i = C_j = C_{ij}$, $\boldsymbol{P}_{ij}$ is just $\boldsymbol{P}_j$

with the i-th coordinate deleted, and $\boldsymbol{P}_{ij}$ is just $\boldsymbol{P}_i$ with the $(j-1)$-th coordinate deleted.

Considering every such pair, we may define a candidate curve C by $C = C_i$ for all i and $\boldsymbol{P} \in C^n$ defined as the unique n-tuple which results in $\boldsymbol{P}_i$ upon deleting the i-th coordinate. By the foregoing, this is well-defined. Now we see that W agrees with $W_{C,\boldsymbol{P}}$ on all coordinate sublattices of rank $n-1$. By part (II) of the inductive hypothesis and Theorem 2.8, we see that W is determined by its sublattices of rank $n-1$. Therefore $W = W_{C,\boldsymbol{P}}$.

To show part (II) of the inductive statement, we observe that if $W(\boldsymbol{v}) = 0$ for all $\boldsymbol{v} \in \{\pm 1\}^n$, then $\boldsymbol{v}(\boldsymbol{P}) = \mathbb{O}$ for all such $\boldsymbol{v}$ (by Corollary 5.2). But this is impossible, since it would imply $[2]P_i = \mathbb{O}$ for $1 \le i \le n$, a contradiction to nondegeneracy (again Corollary 5.2).

A change of coordinates of the form (21) for C does not change the elliptic net, as it is determined by its values on its coordinate hyperplanes, where this is true. Further, if two tuples *not* related by such a change of coordinates generate the same net W, then the same would hold for some coordinate hyperplane, a contradiction. This demonstrates part (I) of the inductive statement. □

7. The curve-net theorem

We set some remaining terminology, and then proceed to the statement and proof of the main theorem.

Homothety and singular elliptic nets. The only changes of coordinates of a Weierstrass equation into another are compositions of unihomothetic changes of coordinates and changes of coordinates of the form $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$, which we refer to as *homotheties* (since they correspond to homotheties of the lattice in the complex uniformization).

Proposition 7.1. *Consider the rank n elliptic net $W_{C,\boldsymbol{P}}$ associated to*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

defined over K and $\boldsymbol{P} \in C(K)^n$. Let λ be a nonzero element of K. Suppose $\phi_\lambda : C \to C_\lambda$ is the isomorphism of curves taking C to

$$C_\lambda : y^2 + \lambda a_1xy + \lambda^3 a_3y = x^3 + \lambda^2 a_2x^2 + \lambda^4 a_4x + \lambda^6 a_6$$

under the change of coordinates $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$. Then

$$\widetilde{W}_{C_\lambda, \phi_\lambda(\boldsymbol{P})} = \lambda \widetilde{W}_{C,\boldsymbol{P}}$$

In particular, let δ_{ij} be the Kronecker delta, and define

$$g(\boldsymbol{v}) = -1 - \sum_{1 \le i < j \le n} (-1)^{\delta_{ij}} v_i v_j.$$

Then

$$W_{C_\lambda, \phi_\lambda(\boldsymbol{P})} = \lambda^{g(\boldsymbol{v})} W_{C,\boldsymbol{P}}.$$

Proof. The first statement is entailed by the second. From the general theory of Weierstrass sigma functions, $\sigma(\lambda z, \lambda\Lambda) = \lambda\sigma(z, \Lambda)$. Thus, by Definition 3.1,

$$\Omega_{\boldsymbol{v}}(\lambda z; \lambda\Lambda) = \lambda^{g(\boldsymbol{v})}\Omega_{\boldsymbol{v}}(z; \Lambda).$$

As in Section 4, this allows us to conclude that the same holds for $\Psi_{\boldsymbol{v}}$, so that

$$\Psi_{\boldsymbol{v}}(\lambda^2 x, \lambda^3 y, \lambda^i \alpha_i) = \lambda^{g(\boldsymbol{v})}\Psi_{\boldsymbol{v}}(x, y, \alpha_i),$$

from which the result follows. □

Definition 7.2. Let $W : \mathbb{Z}^n \to K$ be an elliptic net. With the notation of Proposition 7.1, we define

$$W^\lambda(\boldsymbol{v}) := \lambda^{g(\boldsymbol{v})} W(\boldsymbol{v}).$$

This gives an action of K on elliptic nets $W : \mathbb{Z}^n \to K$ called the *homothety action*. Two elliptic nets are *homothetic* if they are in the same orbit of the action of K.

The following proposition is immediate.

Proposition 7.3. *Let $W : \mathbb{Z}^n \to K$ be an elliptic net. Then for any nonzero $\lambda \in K$, W^λ is normalized if and only if W is.*

Let $W : \mathbb{Z}^n \to K$ be an elliptic net. If the curve C associated to its normalization is a nodal or cuspidal cubic, then W is called *singular*. If, instead, C is an elliptic curve, then W is called *nonsingular*. In either case, the discriminant Δ of W is defined to be the discriminant of the associated Weierstrass equation. Similarly, the j-invariant is the j-invariant of the associated Weierstrass equation. The discriminant of an elliptic net changes by a factor of λ^{12} under homothety, while the j-invariant remains unaltered.

The curve-net theorem. We may put a partial ordering on tuples $(C, P_1, \ldots, P_n)$ where C is a Weierstrass curve and P_i are nonsingular points on the curve. We do this by defining

$$(C, P_1, \ldots, P_n) \leq (D, Q_1, \ldots, Q_m)$$

if and only if $C = D$ and the groups they generate satisfy a containment

$$\langle P_1, \ldots, P_n \rangle \subseteq \langle Q_1, \ldots, Q_n \rangle .$$

The collection of all elliptic nets is partially ordered by the subnet relation. Collecting our work up to this point, we have now shown:

Theorem 7.4. *For each field K, there is an explicit isomorphism of partially ordered sets*

$$\left\{\begin{array}{l}\text{scale equivalence classes of}\\ \text{nondegenerate elliptic nets}\\ W : \mathbb{Z}^n \to K, \text{ for some } n\end{array}\right\}$$

$$\Updownarrow$$

$$\left\{\begin{array}{l}\text{tuples } (C, P_1, \ldots, P_m) \text{ for some } m, \text{ where } C \text{ is a}\\ \text{cubic curve in Weierstrass form over } K, \text{ consid-}\\ \text{ered modulo unihomothetic changes of variables}\\ \text{and such that } \{P_i\} \in C_{\mathrm{ns}}(K)^m \text{ is appropriate}\end{array}\right\}.$$

Nonsingular nets correspond to elliptic curves. The action of K (by homothety) on the sets preserves the order and respects the isomorphism. The bijection takes an elliptic net of rank n to a tuple with n points. The elliptic net W associated to a tuple $(C, P_1, \ldots, P_n)$ satisfies the property that $W(v_1, \ldots, v_n) = 0$ if and only if $v_1 P_1 + \cdots + v_n P_n = 0$ on the curve C.

Proof. In the diagram in the statement of the theorem, call the upper set $\mathcal{N}$ and the lower set $\mathcal{C}$. The first claim is that there is an injective map $\mathcal{N} \to \mathcal{C}$. Proposition 6.2 shows that each scale equivalence classes in $\mathcal{N}$ contains a unique normalized elliptic net, so we can define the map by Theorem 6.7 (which also guarantees injectivity). Corollary 5.2 shows that the result is an element of $\mathcal{C}$. This shows the first claim.

The second claim is that there exists an inverse map $\mathcal{C} \to \mathcal{N}$. The map is given by Definition 5.1, which is well-defined as a result of Theorem 4.6. It is required to check that the resulting elliptic net is normalized (Proposition 3.8) and nondegenerate (Corollary 5.2). Theorem 6.7 says that this map is indeed an inverse to the map of the first claim. This gives the second claim and the bijection of sets.

It is clear that the bijection associates an elliptic net of rank n to a tuple with n points, and that it preserves the partial ordering. The action of homothety is preserved by Proposition 7.1. And the final statement of the theorem is a result of Corollary 5.2. □

Remark 7.5. The degenerate cases present several difficulties. One is that a degenerate elliptic net may not be determined by the usual initial set of terms as given in Section 2. For example, the sequence given by

$$W(n) = \begin{cases} 0 & \text{if } n \neq k, \\ 1 & \text{if } n = k, \end{cases}$$

is an elliptic net for any nonzero integer k. However, some degenerate sequences can be thought of as arising from singular points on a singular cubic. For example, consider a sequence associated to an elliptic curve E and point P both defined over

$\mathbb{Q}$ such that P reduces to a singular point modulo some prime p. Then the sequence regarded modulo p as living in $\mathbb{F}_p$ (which is necessarily a degenerate elliptic net) should be associated to a point on the special fibre of the Néron model. It is likely that Theorem 7.4 can be extended to include these cases (this is future work).

Acknowledgements

I thank my thesis advisor, Joseph Silverman, for many patient hours. I also thank Rafe Jones, Alf van der Poorten, and Jonathan Wise.

References

[Ayad 1993] M. Ayad, "Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques", *Ann. Inst. Fourier* (*Grenoble*) **43**:3 (1993), 585–618. MR 94f:11009

[Chandrasekharan 1985] K. Chandrasekharan, *Elliptic functions*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **281**, Springer, Berlin, 1985. MR 87e:11058 Zbl 0575.33001

[Chudnovsky and Chudnovsky 1986] D. V. Chudnovsky and G. V. Chudnovsky, "Sequences of numbers generated by addition in formal groups and new primality and factorization tests", *Adv. in Appl. Math.* **7**:4 (1986), 385–434. MR 88h:11094 Zbl 0614.10004

[Cornelissen and Zahidi 2007] G. Cornelissen and K. Zahidi, "Elliptic divisibility sequences and undecidable problems about rational points", *J. Reine Angew. Math.* **613** (2007), 1–33. MR2009h:11196 Zbl 1178.11076

[Eisenträger and Everest 2009] K. Eisenträger and G. Everest, "Descent on elliptic curves and Hilbert's tenth problem", *Proc. Amer. Math. Soc.* **137**:6 (2009), 1951–1959. MR 2009k:11201

[Everest et al. 2003] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs **104**, American Mathematical Society, Providence, RI, 2003. MR 2004c:11015 Zbl 1033.11006

[Everest et al. 2004] G. Everest, V. Miller, and N. Stephens, "Primes generated by elliptic curves", *Proc. Amer. Math. Soc.* **132**:4 (2004), 955–963. MR 2005a:11076 Zbl 1043.11051

[Everest et al. 2006] G. Everest, G. Mclaren, and T. Ward, "Primitive divisors of elliptic divisibility sequences", *J. Number Theory* **118**:1 (2006), 71–89. MR 2007a:11074 Zbl 0169.15902

[Fomin and Zelevinsky 2002] S. Fomin and A. Zelevinsky, "The Laurent phenomenon", *Adv. in Appl. Math.* **28**:2 (2002), 119–144. MR 2002m:05013 Zbl 1012.05012

[Frey and Lange 2006] G. Frey and T. Lange, "Background on curves and Jacobians", pp. 45–85 in *Handbook of elliptic and hyperelliptic curve cryptography*, edited by H. Cohen et al., CRC, Boca Raton, FL, 2006. MR 2162720

[Gasper and Rahman 2004] G. Gasper and M. Rahman, *Basic hypergeometric series*, 2nd ed., Encyclopedia of Mathematics and its Applications **96**, Cambridge University Press, Cambridge, 2004. MR 2006d:33028 Zbl 1129.33005

[Hone 2005] A. N. W. Hone, "Elliptic curves and quadratic recurrence sequences", *Bull. London Math. Soc.* **37**:2 (2005), 161–171. MR 2005h:11111 Zbl 1166.11333

[Ingram 2009] P. Ingram, "Multiples of integral points on elliptic curves", *J. Number Theory* **129**:1 (2009), 182–208. MR 2010a:11102 Zbl 05485801

[Mazur and Tate 1991] B. Mazur and J. Tate, "The p-adic sigma function", *Duke Math. J.* **62**:3 (1991), 663–688. MR 93d:11059 Zbl 0735.14020

[Poonen 2003] B. Poonen, "Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$", *J. Amer. Math. Soc.* **16**:4 (2003), 981–990. MR 2004f:11145 Zbl 1028.11077

[van der Poorten 2005] A. J. van der Poorten, "Elliptic curves and continued fractions", *J. Integer Seq.* **8**:2 (2005), [article] 05.2.5. MR 2006h:11083

[van der Poorten and Swart 2006] A. J. van der Poorten and C. S. Swart, "Recurrence relations for elliptic sequences: every Somos 4 is a Somos k", *Bull. London Math. Soc.* **38**:4 (2006), 546–554. MR 2007d:11024 Zbl 1169.11013

[Propp 2001] J. Propp, Robbins forum, various messages from January 2, 2001 through March 6, 2001, available at http://faculty.uml.edu/jpropp/about-robbins.txt.

[Shipsey 2001] R. Shipsey, *Elliptic divibility sequences*, Ph.D. thesis, Goldsmiths, University of London, 2001.

[Silverman 2004] J. H. Silverman, "Common divisors of elliptic divisibility sequences over function fields", *Manuscripta Math.* **114**:4 (2004), 431–446. MR 2005d:11096 Zbl 1128.11015

[Silverman 2005] J. H. Silverman, "p-adic properties of division polynomials and elliptic divisibility sequences", *Math. Ann.* **332**:2 (2005), 443–474. MR 2006f:11063 Zbl 1066.11024

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. MR 2010i:11005 Zbl 1194.11005

[Stange 2007] K. E. Stange, "The Tate pairing via elliptic nets", pp. 329–348 in *Pairing-based cryptography: Pairing 2007* (Tokyo, 2007), edited by T. Takagi et al., Lecture Notes in Comput. Sci. **4575**, Springer, Berlin, 2007. MR 2009e:11233 Zbl 1151.94570

[Stange 2010] K. E. Stange, Scripts in PARI/GP 2.3.4 and SAGE 4.6.1, 2010, available at http://math.katestange.net.

[Streng 2008] M. Streng, "Divisibility sequences for elliptic curves with complex multiplication", *Algebra Number Theory* **2**:2 (2008), 183–208. MR 2009e:11110 Zbl 1158.14029

[Swart 2003] C. Swart, *Elliptic curves and related sequences*, Ph.D. thesis, Royal Holloway and Bedford New College, University of London, 2003.

[Ward 1948] M. Ward, "Memoir on elliptic divisibility sequences", *Amer. J. Math.* **70** (1948), 31–74. MR 9,332j

[Wenchang et al. 1996] C. Wenchang, S. B. Ekhad, and R. J. Chapman, "Problems and Solutions: Solutions: 10226", *Amer. Math. Monthly* **103**:2 (1996), 175–177. MR 1542800

Communicated by John H. Coates
Received 2010-04-28 Revised 2010-09-16 Accepted 2010-10-17

stange@math.stanford.edu *Department of Mathematics, Stanford University, 450 Serra Mall, Building 380, Stanford, CA, 94305, United States*
http://math.katestange.net

ALGEBRA AND NUMBER THEORY 5:2(2011)

msp

The basic geometry of Witt vectors, I
The affine case

James Borger

We give a concrete description of the category of étale algebras over the ring of Witt vectors of a given finite length with entries in an arbitrary ring. We do this not only for the classical p-typical and big Witt vector functors but also for certain analogues over arbitrary local and global fields. The basic theory of these generalized Witt vectors is developed from the point of view of commuting Frobenius lifts and their universal properties, which is a new approach even for classical Witt vectors. Our larger purpose is to provide the affine foundations for the algebraic geometry of generalized Witt schemes and arithmetic jet spaces, so the basics are developed in some detail, with an eye toward future applications.

This work was partly supported by Discovery Project DP0773301, a grant from the Australian Research Council.
MSC2010: 13F35.
Keywords: Witt vector, Witt space, lambda-ring, Frobenius lift, plethory.

Introduction

Witt vector functors are certain functors from the category of (commutative) rings to itself. The most common are the p-typical Witt vector functors W, for each prime number p. Given a ring A, one traditionally defines $W(A)$ as a set to be $A^{\mathbb{N}}$ and then gives it the unique ring structure which is functorial in A and such that the set maps

$$\begin{aligned} W(A) &\xrightarrow{w} A^{\mathbb{N}} \\ (x_0, x_1, \dots) &\longmapsto \langle x_0,\ x_0^p + px_1,\ x_0^{p^2} + px_1^p + p^2x_2,\ \dots \rangle \end{aligned}$$

are ring homomorphisms for all rings A, where the target has the ring structure with componentwise operations. For example, we have

$$\begin{aligned} (x_0, x_1, \dots) + (y_0, y_1, \dots) &= \Big(x_0 + y_0,\ x_1 + y_1 - \sum_{i=1}^{p-1} \tfrac{1}{p}\tbinom{p}{i} x_0^i y_0^{p-i},\ \dots\Big) \\ (x_0, x_1, \dots) \cdot (y_0, y_1, \dots) &= (x_0y_0,\ x_0^p y_1 + x_1 y_0^p + px_1y_1,\ \dots). \end{aligned}$$

Observe that the four polynomials in x_0, y_0, x_1, y_1 displayed on the right-hand side have integer coefficients, as they must if they are to define operations on $W(A)$ for all rings A. Conversely, to prove that the desired functorial ring structure on W exists, it is enough to prove that the polynomials sitting in the higher components have integer coefficients too. This is Witt's theorem.

On the other hand, the polynomials at the component of index n depend only on the variables $x_0, y_0, \dots, x_n, y_n$. This is clear by induction. It follows that the quotient set $A^{[0,n]} = \{(x_0, \dots, x_n)\}$ of $W(A) = A^{\mathbb{N}}$ is a quotient ring, which we denote by $W_n(A)$. (It is traditionally denoted $W_{n+1}(A)$. The shift in indexing is preferable for reasons discussed in 2.5.)

In some cases, the rings $W(A)$ and $W_n(A)$ are isomorphic to familiar rings. For example, $W(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to the ring $\mathbb{Z}_p$ of p-adic integers, and $W_n(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to $\mathbb{Z}/p^{n+1}\mathbb{Z}$. If p is invertible in A, then w is a bijection and so the Witt vector rings become product rings: $W_n(A) \cong A^{[0,n]}$ and $W(A) \cong A^{\mathbb{N}}$. But in most cases, $W(A)$ is not a familiar ring.

While this traditional approach to Witt vectors is adequate for many purposes, it has two shortcomings. The first is that it is not clear how we should think about the affine scheme $\operatorname{Spec} W_n(A)$ geometrically. Indeed, I am not aware of a truly geometric description of $\operatorname{Spec} W_n(A)$ in any nontrivial case in the literature. If we want to fully incorporate Witt vectors into arithmetic algebraic geometry (and we do), it is important to have a thorough understanding of their geometry. The main point here and in the companion paper [Borger 2010] is to set up a framework for that. The geometry in this paper is however limited to the basic results in the affine case needed for the general treatment in [Borger 2010].

The second shortcoming of the traditional approach is that it does not explain what the defining purpose of Witt vectors is. The answer, at least for this paper, is that they control Frobenius lifts—ring endomorphisms which reduce to the Frobenius map modulo p. Here we are following Borger and Wieland [2005, §12.3–4], who in turn followed Joyal [1985a; 1985b]. Motivated by this perspective, we will define Witt vector functors relative to primes in any global or local field. This generality includes not only the p-typical functors above but also the so-called big Witt vector functor and less common variants of the p-typical ones due to Drinfeld [1976, Proposition 1.1] and to Hazewinkel [1978, (18.6.13)]. It also includes many variants unstudied till now. We will work with these generalized functors throughout the paper. In fact, this will take no more effort once we establish some basic reduction results.

Let us now discuss the contents in more detail.

Section 1 introduces our generalized Witt vectors. Given a Dedekind domain R and a set E of maximal ideals of R with finite residue fields, we will define a functor $W_{R,E}$ from the category Ring_R of R-algebras to itself:

$$W_{R,E}\colon \mathsf{Ring}_R \to \mathsf{Ring}_R.$$

(In fact, we will work with slightly more general R and E.) We call $W_{R,E}$ the E-typical Witt vector functor. When $R=\mathbb{Z}$ and E consists of a single maximal ideal $p\mathbb{Z}$, our functor will agree with the p-typical Witt vector functor above; when E consists of all maximal ideals of $\mathbb{Z}$, our functor will agree with the big Witt vector functor. The definition of $W_{R,E}$ is in two steps. First we define a functor

$$W^{\mathrm{fl}}_{R,E}\colon \mathsf{Ring}^{\mathrm{fl}}_R \to \mathsf{Ring}^{\mathrm{fl}}_R,$$

where $\mathsf{Ring}^{\mathrm{fl}}_R$ is the full subcategory of Ring_R consisting of R-algebras which are $\mathfrak{m}$-torsion free for all ideals $\mathfrak{m}\in E$. We call such algebras E-flat. Then we define $W_{R,E}$ to be a certain natural extension of $W^{\mathrm{fl}}_{R,E}$ to all of Ring_R.

Let $\mathbb{N}^{(E)}$ denote the commutative monoid $\bigoplus_E \mathbb{N}$, where $\mathbb{N}$ is $\{0,1,\dots\}$ under addition. Given an action of $\mathbb{N}^{(E)}$ on an R-algebra B, let $\psi_{\mathfrak{m}}$ denote the endomorphism of B given by the $\mathfrak{m}$-th element of the standard basis of $\mathbb{N}^{(E)}$. Let us say that such an action is a $\Lambda_{R,E}$-structure if for each $\mathfrak{m}\in E$, the map $\psi_{\mathfrak{m}}$ reduces to the Frobenius endomorphism $x\mapsto x^{[R:\mathfrak{m}]}$ on $B/\mathfrak{m}B$. Now, for any R-algebra A, the monoid $\mathbb{N}^{(E)}$ acts on $A^{\mathbb{N}^{(E)}}$ through its translation action on itself in the exponent. When A is E-flat, we define $W^{\mathrm{fl}}_{R,E}(A)$ to be the largest of the sub-R-algebras $B\subseteq A^{\mathbb{N}^{(E)}}$ having the properties that B is stable under the action of $\mathbb{N}^{(E)}$ and that the induced action on B is a $\Lambda_{R,E}$-structure. It is elementary to check that a maximal such subalgebra $W^{\mathrm{fl}}_{R,E}(A)$ exists.

This definition can be expressed as a universal property. Let $\mathsf{Ring}^{\mathrm{fl}}_{\Lambda_{R,E}}$ denote the following category: the objects are E-flat R-algebras equipped with a $\Lambda_{R,E}$-structure, and the morphisms are $\mathbb{N}^{(E)}$-equivariant R-algebra maps. Then $W^{\mathrm{fl}}_{R,E}$, viewed as a functor $\mathsf{Ring}^{\mathrm{fl}}_R \to \mathsf{Ring}^{\mathrm{fl}}_{\Lambda_{R,E}}$, is the right adjoint of the evident forgetful functor.

One then defines $W_{R,E}$ to be the left Kan extension of $W^{\mathrm{fl}}_{R,E}$, now viewed as a functor $\mathsf{Ring}^{\mathrm{fl}}_R \to \mathsf{Ring}_R$. This amounts to the following. It is not hard to show that the functor $W^{\mathrm{fl}}_{R,E}$ is representable, that is, there exists an E-flat R-algebra $\Lambda_{R,E}$ and an isomorphism $W^{\mathrm{fl}}_{R,E}(-) = \mathrm{Hom}(\Lambda_{R,E}, -)$, as set-valued functors. Because $W^{\mathrm{fl}}_{R,E}$ takes values in R-algebras, $\Lambda_{R,E}$ carries the structure of a co-R-algebra object in $\mathsf{Ring}^{\mathrm{fl}}_R$. Because such a structure is described using maps between certain coproducts of $\Lambda_{R,E}$ with itself, and because $\mathsf{Ring}^{\mathrm{fl}}_R$ is a full subcategory of Ring_R closed under coproducts, $\Lambda_{R,E}$ continues to be a co-R-algebra object when viewed as an object of Ring_R. Therefore it represents an R-algebra-valued functor, and this functor is what $W_{R,E}$ is defined to be.

Since the definition of $W_{R,E}$ in terms of $W^{\mathrm{fl}}_{R,E}$ is of a purely category-theoretic nature, one should view the E-flat case as the central one. This is in contrast to the common point of view that the purpose of Witt vector functors is to lift rings from positive characteristic to characteristic zero.

As in the E-flat setting, $W_{R,E}$ is the right adjoint of the forgetful functor

$$\mathsf{Ring}_{\Lambda_{R,E}} \to \mathsf{Ring}_R,$$

but to make sense of this, it is necessary to know the what a $\Lambda_{R,E}$-structure on a general R-algebra is. Unfortunately, it is not easy to state the definition, and so we will leave it to the body of the paper. In the E-flat setting, it is equivalent to a commuting family of Frobenius lifts indexed by E, as above; but in general, it is a slightly stronger structure that is better behaved. When R is $\mathbb{Z}$ and E consists of all maximal ideals of $\mathbb{Z}$, a $\Lambda_{R,E}$-structure is equivalent to a λ-ring structure in the sense of Grothendieck's Riemann–Roch theory, but this does not admit a simple definition either.

In addition to the right adjoint $W_{R,E}$, the forgetful functor $\mathsf{Ring}_{\Lambda_{R,E}} \to \mathsf{Ring}_R$ has a left adjoint, which we denote by $A \mapsto \Lambda_{R,E} \odot A$. It has a smaller presence in this paper, but it is very important—even in the p-typical case, as the work of Buium [1996; 2005] makes clear.

Section 2 defines functors $W_{R,E,n}$, which are truncations of $W_{R,E}$ in the same way that the functors W_n above are truncations of W. For any $A \in \mathsf{Ring}^{\mathrm{fl}}_R$ and $n \in \mathbb{N}^{(E)}$, let $W^{\mathrm{fl}}_{R,E,n}(A)$ denote the image of the subring $W^{\mathrm{fl}}_{R,E}(A) \subseteq A^{\mathbb{N}}$ under the canonical projection

$$A^{\mathbb{N}^{(E)}} \to A^{[0,n]},$$

where

$$[0,n] = \{i \in \mathbb{N}^{(E)} \mid i_{\mathfrak{m}} \leqslant n_{\mathfrak{m}} \text{ for all } \mathfrak{m} \in E\}.$$

Then $W^{\mathrm{fl}}_{R,E,n}$ is a functor $\mathsf{Ring}^{\mathrm{fl}}_R \to \mathsf{Ring}^{\mathrm{fl}}_R$. It is representable by an E-flat R-algebra $\Lambda_{R,E,n}$, and we extend it to a functor

$$W_{R,E,n} \colon \mathsf{Ring}_R \to \mathsf{Ring}_R$$

by taking its left Kan extension, as above. These truncated functors are related to the original one by the formula

$$W_{R,E}(A) = \lim_n W_{R,E,n}(A).$$

Even in the p-typical case, this approach to defining the Witt vectors has the advantage over the traditional one that universal properties are emphasized and the particulars of explicit constructions are played down. But this comes at a cost. For instance, it is not obvious that $W_{R,E,n}$ preserves surjectivity of maps. To prove this and other basic facts, it appears necessary to bring back the Witt components $(x_0, x_1, \dots)$ above, at least in some form. To define them, the ideals of E must be principal; the purpose of section 3 is to define them in the minimal case we will need, which is when E consists of a single principal ideal $\mathfrak{m}$. A version of the proof of Witt's theorem then shows there is a unique functorial bijection $A^{\mathbb{N}} \to W_{R,E}(A)$ such that when A is E-flat, the composition $A^{\mathbb{N}} \to W_{R,E}(A) \subseteq A^{\mathbb{N}}$ satisfies

$$(x_0, x_1, x_2, \dots) \mapsto \langle x_0,\ x_0^q + \pi x_1,\ x_0^{q^2} + \pi x_1^q + \pi^2 x_2,\ \dots \rangle$$

where $q = [R : \mathfrak{m}]$ and π is a fixed generator of $\mathfrak{m}$. We can similarly identify $W_{R,E,n}(A)$ with the quotient $A^{[0,n]}$ consisting of vectors $(x_0, \dots, x_n)$. Let me emphasize that the components $(x_0, x_1, \dots)$ depend on the choice of generator $\pi \in \mathfrak{m}$ in a complex, non-multilinear way. But we can use them to define Verschiebung operators

$$\begin{aligned} V^j_{\mathfrak{m}} \colon \mathfrak{m}^j \otimes_R W_{R,E,n}(A) &\to W_{R,E,n+j}(A) \\ \pi^j \otimes (x_0, \dots, x_n) &\mapsto (0, \dots, 0, x_0, \dots, x_n), \end{aligned}$$

which are independent of the choice of the generator π. Making that so is the purpose the tensor factor $\mathfrak{m}^j$.

When E consists of a single ideal $\mathfrak{m}$ (possibly nonprincipal), section 4 describes $W_{R,E,n}$ in terms of the case where $\mathfrak{m}$ is principal, which is covered by section 3. This is done by working Zariski locally on R. Using the same technique, we will show that the Verschiebung maps as above can be defined when $\mathfrak{m}$ is not assumed to be principal. In fact, there is a unique functorial family of such maps agreeing with the maps defined above. The image of $V^j_{\mathfrak{m}}$ is the kernel of the canonical projection $W_{R,E,n+j}(A) \to W_{R,E,j}(A)$.

Similarly, section 5 gives a description of $W_{R,E,n}$ when E is general in terms of the case where E consists of a single ideal, which is covered by section 4: if $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ are the ideals in the support of n, there is a natural isomorphism

$$W_{R,E,n} \xrightarrow{\sim} W_{R,\mathfrak{m}_r,n_{\mathfrak{m}_r}} \circ \cdots \circ W_{R,\mathfrak{m}_1,n_{\mathfrak{m}_1}}. \tag{0-0-1}$$

Such a description also holds for $W_{R,E}$, though some care must be taken when E is infinite. It is also possible to describe the functor $\Lambda_{R,E} \odot -$, as well as its truncated variants $\Lambda_{R,E,n} \odot -$, in terms of the case where E consists of a single ideal.

Section 6 gives several ring-theoretic facts about $W_{R,E,n}$ which we will need later. For example, this is where we prove that $W_{R,E,n}$ preserves surjectivity. Most of the arguments there appear to require the use of Witt components and the reduction techniques of sections 4 and 5.

Sections 7–9 prove the main results, which relate Witt vector functors and étale maps. Suppose E consists of a single ideal $\mathfrak{m}$. For any ring A and any integer $n \geqslant 1$, we have a diagram

$$W_{R,E,n}(A) \xrightarrow{\alpha_n} W_{R,E,n-1}(A) \times A \underset{t\circ \mathrm{pr}_2}{\overset{s\circ \mathrm{pr}_1}{\rightrightarrows}} A/\mathfrak{m}^n A. \tag{0-0-2}$$

When $\mathfrak{m}$ is principal, the maps α_n, s, and t can be defined in terms of the Witt components relative to a fixed generator $\pi \in \mathfrak{m}$ as follows:

$$\begin{aligned} \alpha_n &: (a_0, \dots, a_n) \mapsto \big((a_0, \dots, a_{n-1}), a_0^{q^n} + \pi a_1^{q^{n-1}} \cdots + \pi^n a_n\big) \\ s &: (a_0, \dots, a_{n-1}) \mapsto (a_0^{q^n} + \cdots + \pi^{n-1} a_{n-1}^q) \bmod \mathfrak{m}^n A \\ t &: a \mapsto a \bmod \mathfrak{m}^n A. \end{aligned}$$

If A is $\mathfrak{m}$-torsion free, (0-0-2) is an equalizer diagram. Figure 1 shows the induced diagram of schemes in the p-typical case when $n = 1$.

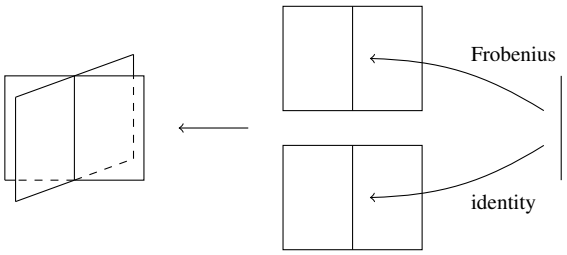
Now let C denote the following category: an object is a pair (B, φ), where B is an étale $(W_{R,E,n-1}(A) \times A)$-algebra and φ is an isomorphism of $A/\mathfrak{m}^n A$-algebras

$$A/\mathfrak{m}^n A \otimes_{t\circ \mathrm{pr}_2} B \xrightarrow{\varphi} A/\mathfrak{m}^n A \otimes_{s\circ \mathrm{pr}_1} B$$

and where a morphism $(B_1, \varphi_1) \to (B_2, \varphi_2)$ is a $(W_{R,E,n-1}(A) \times A)$-algebra map $f : B_1 \to B_2$ such that

$$\varphi_2 \circ (A/\mathfrak{m}^n A \otimes_{t\circ \mathrm{pr}_2} f) = (A/\mathfrak{m}^n A \otimes_{s\circ \mathrm{pr}_1} f) \circ \varphi_1.$$

In other words, C is the category of algebras equipped with gluing data relative to the diagram (0-0-2), or equivalently C is the (weak) fiber product of the category of étale $W_{n-1}(A)$-algebras and the category étale A-algebras over the category of étale $A/\mathfrak{m}^n A$-algebras via the evident functors.



$$\operatorname{Spec} W_1(A) \longleftarrow \operatorname{Spec}(A \times A) \rightleftarrows \operatorname{Spec} A/pA$$

Figure 1. As a topological space, $\operatorname{Spec} W_1(A)$ (traditionally written $W_2(A)$) is two copies of $\operatorname{Spec} A$ glued along $\operatorname{Spec} A/pA$. This is also true as schemes if we assume that A is p-torsion free and we glue transversely and with a Frobenius twist, as indicated. There is a similar description of $\operatorname{Spec} W_n(A)$ as $\operatorname{Spec} W_{n-1}(A)$ glued with $\operatorname{Spec} A$ along $\operatorname{Spec} A/p^n A$. See the diagram (0-0-2).

Theorem A. *The base-change functor from the category of étale $W_{R,E,n}(A)$-algebras to C is an equivalence. If A is $\mathfrak{m}$-torsion free, then a quasi-inverse is given by sending (B, φ) to the equalizer of the two maps*

$$B \underset{\varphi\circ(1\otimes \mathrm{id}_B)}{\overset{1\otimes \mathrm{id}_B}{\rightrightarrows}} A/\mathfrak{m}^n A \otimes_{s\circ \mathrm{pr}_1} B.$$

The first statement can be expressed succinctly in geometric terms; it says that the map α_n satisfies effective descent for étale algebras and that descent data is equivalent to gluing data with respect to the diagram (0-0-2). Using theorem A and induction on n, it is in principle possible to reduce questions about étale $W_n(A)$-algebras to questions about étale A-algebras. This is still true when E consists of more than one ideal, but now by (0-0-1) and induction on r.

Section 9 generalizes van der Kallen's theorem [1986, (2.4)] to any R and E:

Theorem B. *Let $f\colon A \to B$ be an étale morphism of R-algebras. Then the map $W_{R,E,n}(f)\colon W_{R,E,n}(A) \to W_{R,E,n}(B)$ of R-algebras is étale.*

This result is fundamental in extending Witt constructions beyond affine schemes and will be used often in [Borger 2010]. Van der Kallen's argument, which has an infinitesimal flavor, could be extended to our setting with only minor modifications.[1] Instead we deduce theorem B from theorem A, so our argument has a globally geometric flavor.

[1] Until recently, [van der Kallen 1986] had escaped the notice of many workers in de Rham–Witt theory, to whom theorem B was unknown even for the p-typical Witt vectors.

1. Generalized Witt vectors and Λ-rings

The purpose of this section is to define our generalized Witt vectors and Λ-rings. It is largely an expansion in more concrete terms of the portion of [Borger and Wieland 2005] dealing with Witt vectors and Λ-rings. The approach here will allow us to avoid much of the abstract language of operations on rings, as first introduced in [Tall and Wraith 1970].

For the traditional way of defining Λ-rings and Witt vectors, see [Bourbaki 1983, XI, §1] and especially the exercises for that section. One can also see Witt's original paper [1937] on p-typical Witt vectors and his notes on big Witt vectors [Witt 1998, pp. 157–163].

1.1. *Supramaximal ideals.* Let us say that an ideal $\mathfrak{m}$ of a ring R is supramaximal if either

(a) $R/\mathfrak{m}$ is a finite field, $R_{\mathfrak{m}}$ is a discrete valuation ring, and $\mathfrak{m}$ is finitely presented as an R-module, or

(b) $\mathfrak{m}$ is the unit ideal.

By far the most important example is a maximal ideal with finite residue field in a Dedekind domain. (In fact, all phenomena in this paper occur already over $R = \mathbb{Z}$, and this case covers the classical Witt vectors and λ-rings.) The reason we allow the unit ideal is only so that a supramaximal ideal remains supramaximal after any localization.

Note that a supramaximal ideal $\mathfrak{m}$ is invertible as an R-module. Indeed, locally at $\mathfrak{m}$ it is the maximal ideal of a discrete valuation ring, and away from $\mathfrak{m}$ it is the unit ideal.

1.2. *General notation.* Fix a ring R and a family $(\mathfrak{m}_\alpha)_{\alpha\in E}$ of pairwise coprime supramaximal ideals of R indexed by a set E. Note that because the unit ideal is coprime to itself, it can be repeated any number of times; otherwise the ideals $\mathfrak{m}_\alpha$ are distinct. For each $\alpha \in E$, let q_α denote the cardinality of $R/\mathfrak{m}_\alpha$. We will often abusively speak of $\mathfrak{m}_\alpha$ rather than α as being an element of E, especially when $\mathfrak{m}_\alpha$ is maximal, in which case it comes from a unique $\alpha \in E$.

Let $R[1/E]$ denote the R-algebra whose spectrum is the complement of E in $\operatorname{Spec} R$. It is the universal R-algebra in which every $\mathfrak{m}_\alpha$ becomes the unit ideal. It also has the more concrete description

$$R[1/E] = \bigotimes_{\alpha\in E} R[1/\mathfrak{m}_\alpha],$$

where the tensor product is over R and $R[1/\mathfrak{m}_\alpha]$ is defined to be the coequalizer of the maps

$$\operatorname{Sym}(R) \rightrightarrows \operatorname{Sym}(\mathfrak{m}_\alpha^{-1})$$

of symmetric algebras, where $\mathfrak{m}_\alpha^{-1}$ is the dual of $\mathfrak{m}_\alpha$, one of the maps is Sym applied to the canonical map $R \to \mathfrak{m}_\alpha^{-1}$, and the other is the map induced by the R-module map $R \to \mathrm{Sym}(\mathfrak{m}_\alpha^{-1})$ that sends $1 \in R$ to the element $1 \in \mathrm{Sym}(\mathfrak{m}_\alpha^{-1})$ in degree zero.

Finally, we write $\mathbb{N}$ for the monoid $\{0, 1, 2, \dots\}$ under addition and write Ring_R for the category of R-algebras.

1.3. *E-flat R-modules.* Let us say that an R-module M is *E-flat* if for all maximal ideals $\mathfrak{m}$ in E, the following equivalent conditions are satisfied:

(a) $R_\mathfrak{m} \otimes_R M$ is a flat $R_\mathfrak{m}$-module,

(b) the map $\mathfrak{m} \otimes_R M \to M$ is injective.

The equivalence of these two can be seen as follows. Condition (b) is equivalent to the statement $\mathrm{Tor}_1^R(R/\mathfrak{m}, M) = 0$, which is equivalent to

$$\mathrm{Tor}_1^{R_\mathfrak{m}}(R/\mathfrak{m}, R_\mathfrak{m} \otimes_R M) = 0.$$

Since $R_\mathfrak{m}$ is a discrete valuation ring, this is equivalent to the $R_\mathfrak{m}$-module $R_m \otimes_R M$ being torsion free and hence flat.

We say an R-algebra is E-flat if its underlying R-module is. Let $\mathsf{Ring}_R^{\mathsf{fl}}$ denote the full subcategory of Ring_R consisting of the E-flat R-algebras.

1.4. Proposition. *Any product of E-flat R-modules is E-flat, and any sub-R-module of an E-flat R-module is E-flat.*

Proof. We will use condition (b) above. Let $(M_i)_{i \in I}$ be a family of E-flat R-modules. We want to show that for each maximal ideal $\mathfrak{m}$ in E, the composition

$$\mathfrak{m} \otimes \textstyle\prod_i M_i \longrightarrow \prod_i \mathfrak{m} \otimes M_i \longrightarrow \prod_i M_i$$

is injective. Because each M_i is E-flat, the right-hand map is injective, and so it is enough to show the left-hand map is injective.

Since $\mathfrak{m}$ is assumed to be finitely presented as an R-module, we can express it as a cokernel of a map $N' \to N$ of finite free R-modules. Then we have the following diagram with exact rows:

$$\begin{array}{ccccccc}
N' \otimes_R \prod_i M_i & \longrightarrow & N \otimes_R \prod_i M_i & \longrightarrow & \mathfrak{m} \otimes_R \prod_i M_i & \longrightarrow & 0 \\
\downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} & & \downarrow & & \\
\prod_i N' \otimes_R M_i & \longrightarrow & \prod_i N \otimes_R M_i & \longrightarrow & \prod_i \mathfrak{m} \otimes_R M_i & \longrightarrow & 0.
\end{array}$$

The left two vertical maps are isomorphisms because N' and N are finite free. Therefore the rightmost vertical map is an injection (and even an isomorphism).

Now suppose M' is a sub-R-module of an E-flat R-module M. Since $\mathfrak{m}$ is an invertible R-module, $\mathfrak{m} \otimes_R M'$ maps injectively to $\mathfrak{m} \otimes_R M$. Since M is E-flat, $\mathfrak{m} \otimes_R M'$ further maps injectively to M, and hence to M'. □

1.5. *Ψ-rings.* Let A be an R-algebra. Let us define a $\Psi_{R,E}$-action, or a $\Psi_{R,E}$-ring structure, on A to be a commuting family of R-algebra endomorphisms ψ_α indexed by $\alpha \in E$. This is the same as an action of the monoid $\mathbb{N}^{(E)} = \bigoplus_E \mathbb{N}$ on A. For any element $n \in \mathbb{N}^{(E)}$, we will also write ψ_n for the endomorphism of A induced by n. A morphism of $\Psi_{R,E}$-rings is defined to be an $\mathbb{N}^{(E)}$-equivariant morphism of rings.

The free $\Psi_{R,E}$-ring on one generator e is $\Psi_{R,E} = R[e]^{\otimes_R \mathbb{N}^{(E)}}$, where $\mathbb{N}^{(E)}$ acts on $\Psi_{R,E}$ through its action on itself in the exponent. In particular, $\Psi_{R,E}$ is freely generated as an R-algebra by the elements $\psi_n(e)$, where $n \in \mathbb{N}^{(E)}$. Then it is natural to write $\psi_n = \psi_n(e) \in \Psi_{R,E}$ and $\psi_\alpha = \psi_{b_\alpha} \in \Psi_{R,E}$, where $b_\alpha \in \mathbb{N}^{(E)}$ denotes the α-th standard basis vector, and $e = \psi_0 \in \Psi_{R,E}$ for the identity operator.

For any $\Psi_{R,E}$-ring A, there is a unique set map

$$\Psi_{R,E} \times A \xrightarrow{\circ} A \tag{1-5-1}$$

with the property that for all $\alpha \in E$, $r \in R$, $f_1, f_2 \in \Psi_{R,E}$, $a \in A$ we have

$$\psi_\alpha \circ a = \psi_\alpha(a) \tag{1-5-2}$$

and

$$r \circ a = r, \quad (f_1 + f_2) \circ a = (f_1 \circ a) + (f_2 \circ a), \quad (f_1 f_2) \circ a = (f_1 \circ a)(f_2 \circ a). \tag{1-5-3}$$

Taking $A = \Psi_{R,E}$, we get a binary operation $\circ$ on $\Psi_{R,E}$ called *composition* or *plethysm*. One can check that this makes $\Psi_{R,E}$ a monoid (noncommutative unless $R = 0$) with identity e and that (1-5-1) is a monoid action.

In the language of plethystic algebra [Borger and Wieland 2005], we can interpret $\Psi_{R,E}$ as the free R-plethory $R\langle \psi_\alpha | \alpha \in E \rangle$ on the R-algebra endomorphisms ψ_α. Then a $\Psi_{R,E}$-action in the sense above is the same as a $\Psi_{R,E}$-action in the sense of abstract plethystic algebra. In particular, $\Psi_{R,E}$ can be viewed as the ring of natural unary operations on $\Psi_{R,E}$-rings, and the composition operation $\circ$ above agrees with the usual composition of unary operations. (Compare with 1.18 below.)

1.6. *E-flat Λ-rings.* Let A be an R-algebra which is E-flat. Define a $\Lambda_{R,E}$-action, or a $\Lambda_{R,E}$-ring structure, on A to be a $\Psi_{R,E}$-action with the following *Frobenius lift* property: for all $\alpha \in E$, the endomorphism $\mathrm{id} \otimes \psi_\alpha$ of $R/\mathfrak{m}_\alpha \otimes_R A$ agrees with the Frobenius map $x \mapsto x^{q_\alpha}$. A morphism of E-flat $\Lambda_{R,E}$-rings is simply defined to be a morphism of the underlying $\Psi_{R,E}$-rings. Let us denote this category by $\mathsf{Ring}^{\mathsf{fl}}_{\Lambda_{R,E}}$.

1.7. *The ghost ring.* Since an action of $\Psi_{R,E}$ on an R-algebra A is the same as an action (in the category of R-algebras) of the monoid $\mathbb{N}^{(E)}$, the forgetful functor from the category of $\Psi_{R,E}$-rings to that of R-algebras has a right adjoint given by

$$A \mapsto \prod_{\mathbb{N}^{(E)}} A = A^{\mathbb{N}^{(E)}},$$

where $\mathbb{N}^{(E)}$ acts on $A^{\mathbb{N}^{(E)}}$ through its action on itself in the exponent. (This is a general fact about monoid actions in any category with products.) For $a \in A^{\mathbb{N}^{(E)}}$ and $n, n' \in \mathbb{N}^{(E)}$, the n-th component of $\psi_{n'}(a)$ is the $(n+n')$-th component of a.

One might call $A^{\mathbb{N}^{(E)}}$ the cofree $\Psi_{R,E}$-ring on the R-algebra A. It has traditionally been called the ring of *ghost components* or *ghost vectors*. By 1.4, it is E-flat if A is.

When $|E| = 1$, there is the possibility of confusing the ghost ring $A^{\mathbb{N}}$, which has the product ring structure, with the usual ring $A^{\mathbb{N}}$ of Witt components (see 3.5), which has an exotic ring structure. To prevent this, we will use angle brackets $\langle a_0, a_1, \dots \rangle$ for elements of the ghost ring.

1.8. *Witt vectors of E-flat rings.* Let us now construct the functor $W^{\mathrm{fl}}_{R,E}$. We will show in 1.9 that it is the right adjoint of the forgetful functor from the category of E-flat $\Lambda_{R,E}$-rings to that of E-flat R-algebras. (Further, the flatness will be removed in 1.12.)

Let A be a E-flat R-algebra. Let $U_0(A)$ denote the cofree $\Psi_{R,E}$-ring $A^{\mathbb{N}^{(E)}}$. For any $i \geqslant 0$, let

$$U_{i+1}(A) = \{b \in U_i(A) \mid \psi_\alpha(b) - b^{q_\alpha} \in \mathfrak{m}_\alpha U_i(A) \text{ for all } \alpha \in E\}.$$

This is a sub-R-algebra of $A^{\mathbb{N}^{(E)}}$. Indeed, it is the intersection over $\alpha \in E$ of the equalizers of pairs of R-algebra maps

$$U_i(A) \rightrightarrows R/\mathfrak{m}_\alpha \otimes_R U_i(A)$$

given by $x \mapsto 1 \otimes \psi_\alpha(x)$ and by $x \mapsto (1 \otimes x)^{q_\alpha}$.

Now define

$$W^{\mathrm{fl}}_{R,E}(A) = \bigcap_{i \geqslant 0} U_i(A). \tag{1-8-1}$$

This is the ring of *E-typical Witt vectors* with entries in A. It is a sub-R-algebra of $A^{\mathbb{N}^{(E)}}$. Observe that $W^{\mathrm{fl}}_{R,E}(A) = A^{\mathbb{N}^{(E)}}$ if A is an $R[1/E]$-algebra.

1.9. Proposition. (a) *$W^{\mathrm{fl}}_{R,E}(A)$ is a sub-$\Psi_{R,E}$-ring of $A^{\mathbb{N}^{(E)}}$.*

(b) *This $\Psi_{R,E}$-ring structure on $W^{\mathrm{fl}}_{R,E}(A)$ is a $\Lambda_{R,E}$-ring structure.*

(c) *The induced functor $A \mapsto W^{\mathrm{fl}}_{R,E}(A)$ from E-flat R-algebras to E-flat $\Lambda_{R,E}$-rings is the right adjoint of the forgetful functor.*

Proof. (a) Let us first show by induction that each $U_i(A)$ is a sub-$\Psi_{R,E}$-ring of $A^{\mathbb{N}^{(E)}}$. For $i = 0$, we have $U_0(A) = A^{\mathbb{N}^{(E)}}$, and so it is clear. For $i \geqslant 1$, we use the description of $U_{i+1}(A)$ as the intersection of the equalizers of the pairs of ring maps

$$U_i(A) \rightrightarrows R/\mathfrak{m}_\alpha \otimes_R U_i(A)$$

given in 1.8. Observe that both these ring maps become $\Psi_{R,E}$-ring maps if we give $R/\mathfrak{m}_\alpha \otimes_R U_i(A)$ a $\Psi_{R,E}$-action by defining $\psi_\beta \colon a \otimes x \mapsto a \otimes \psi_\beta(x)$, for all $\beta \in E$. Since limits of $\Psi_{R,E}$-rings exist and their underlying rings agree with the limits taken in the category of rings, $U_{i+1}(A)$ is a sub-$\Psi_{R,E}$-ring of $A^{\mathbb{N}^{(E)}}$. Therefore $W^{\mathrm{fl}}_{R,E}(A)$, the intersection of the $U_i(A)$, is also a sub-$\Psi_{R,E}$-ring of $A^{\mathbb{N}^{(E)}}$.

(b) It is enough to verify

$$\psi_\alpha(x) - x^{q_\alpha} \in \mathfrak{m}_\alpha W^{\mathrm{fl}}_{R,E}(A) = \mathfrak{m}_\alpha \bigcap_{i \geqslant 0} U_i(A),$$

for all $\alpha \in E$ and $x \in W^{\mathrm{fl}}_{R,E}(A)$. For any $i \geqslant 0$, we know

$$\psi_\alpha(x) - x^{q_\alpha} \in \mathfrak{m}_\alpha U_i(A),$$

because $x \in W^{\mathrm{fl}}_{R,E}(A) \subseteq U_{i+1}(A)$. Therefore we know

$$\psi_\alpha(x) - x^{q_\alpha} \in \bigcap_{i \geqslant 0} \mathfrak{m}_\alpha U_i(A).$$

So, it is enough to show

$$\mathfrak{m}_\alpha \bigcap_{i \geqslant 0} U_i(A) = \bigcap_{i \geqslant 0} \mathfrak{m}_\alpha U_i(A). \tag{1-9-1}$$

Since $\mathfrak{m}_\alpha$ is finitely generated, it is a quotient of a finite free R-module N. Consider the induced diagram

$$\begin{array}{ccc} \mathfrak{m}_\alpha \otimes_R \lim_i U_i(A) & \xrightarrow{h} & \lim_i \mathfrak{m}_\alpha \otimes_R U_i(A) \\ \uparrow & & \uparrow{\scriptstyle g} \\ N \otimes_R \lim_i U_i(A) & \xrightarrow{f} & \lim_i N \otimes_R U_i(A) \end{array}$$

Since N is finite free, f is an isomorphism; since $\mathfrak{m}_\alpha$ is projective, the map $N \to \mathfrak{m}_\alpha$ has a section and hence so does g. Therefore $g \circ f$ is surjective and hence so is h, which implies (1-9-1).

(c) Let A be an E-flat R-algebra, let B be an E-flat $\Lambda_{R,E}$-ring, and let $\bar{\gamma} \colon B \to A$ be an R-algebra map. By the cofree property of $A^{\mathbb{N}^{(E)}}$, there is a unique $\Psi_{R,E}$-ring map $\gamma \colon B \to A^{\mathbb{N}^{(E)}}$ lifting $\bar{\gamma}$. We now only need to show that the image of γ is

contained in $W^{\mathrm{fl}}_{R,E}(A)$. By induction, it is enough to show that if $\mathrm{im}(\gamma) \subseteq U_i(A)$, then $\mathrm{im}(\gamma) \subseteq U_{i+1}(A)$.

Let b be an element of B. Then for each $\alpha \in E$, we have

$$\psi_\alpha\big(\gamma(b)\big) - \gamma(b)^{q_\alpha} = \gamma\big(\psi_\alpha(b) - b^{q_\alpha}\big) \in \gamma(\mathfrak{m}_\alpha B) \subseteq \mathfrak{m}_\alpha\, \mathrm{im}(\gamma) \subseteq \mathfrak{m}_\alpha U_i(A).$$

Therefore, by definition of $U_{i+1}(A)$, the element $\gamma(b)$ lies in $U_{i+1}(A)$. □

1.10. *Exercises.* Let $R = \mathbb{Z}$. If E consists of the single ideal $p\mathbb{Z}$, then $W^{\mathrm{fl}}(\mathbb{Z})$ agrees with the subring of the ghost ring $\mathbb{Z}^{\mathbb{N}}$ consisting of vectors $a = \langle a_0, a_1, \dots \rangle$ that satisfy

$$a_n \equiv a_{n+1} \bmod p^{n+1}$$

for all $n \geqslant 0$. In particular, the elements are p-adic Cauchy sequences and the rule $a \mapsto \lim_{n\to\infty} a_n$ defines a surjective ring map $W^{\mathrm{fl}}(\mathbb{Z}) \to \mathbb{Z}_p$.

We can go a step further with $W^{\mathrm{fl}}(\mathbb{Z}_p)$. Let I denote the ideal $p\mathbb{Z}_p \times p^2\mathbb{Z}_p \times \cdots$ in $\mathbb{Z}_p^{\mathbb{N}}$. Then $W^{\mathrm{fl}}(\mathbb{Z}_p)$ is isomorphic to the ring $\mathbb{Z}_p \oplus I$ with multiplication defined by the formula $(x, y)(x', y') = (xx', xy' + yx' + yy')$.

Now suppose that E consists of all the maximal ideals of $\mathbb{Z}$, and identify $\mathbb{N}^{(E)}$ with the set of positive integers, by unique factorization. Then $W^{\mathrm{fl}}(\mathbb{Z})$ consists of the ghost vectors $\langle a_1, a_2, \dots \rangle$ that satisfy

$$a_j \equiv a_{pj} \bmod p^{1+\mathrm{ord}_p(j)}$$

for all $j \geqslant 1$ and all primes p.

1.11. *Representing W^{fl}.* Let us construct a flat R-algebra $\Lambda_{R,E}$ representing the functor $W^{\mathrm{fl}}_{R,E}$. First we will construct objects $\Lambda^i_{R,E}$ representing the functors U_i. For $i = 0$, it is clear: U_0 is represented by $\Lambda^0_{R,E} = \Psi_{R,E}$. Now assume $\Lambda^i_{R,E}$ has been constructed and that it is a sub-R-algebra of $R[1/E] \otimes_R \Psi_{R,E}$ satisfying

$$R[1/E] \otimes_R \Lambda^i_{R,E} = R[1/E] \otimes_R \Psi_{R,E}.$$

Then let $\Lambda^{i+1}_{R,E}$ denote the sub-$\Lambda^i_{R,E}$-algebra of $R[1/E] \otimes_R \Psi_{R,E}$ generated by all elements $\pi^* \otimes (\psi_\alpha(f) - f^{q_\alpha})$, where $\pi^* \in \mathfrak{m}_\alpha^{-1} \subseteq R[1/E]$, $f \in \Lambda^i_{R,E}$, and $\alpha \in E$. Then $\Lambda^i_{R,E}$ is flat over R. Indeed, it is E-flat because it is a sub-R-algebra of $R[1/E] \otimes_R \Psi_{R,E}$, and it is flat away from E because $R[1/E] \otimes_R \Lambda_{R,E}$ agrees with the free $R[1/E]$-algebra $R[1/E] \otimes_R \Psi_{R,E}$. It also clearly represents U_i.

Finally, we set

$$\Lambda_{R,E} = \bigcup_{i \geqslant 0} \Lambda^i_{R,E} \subseteq R[1/E] \otimes_R \Psi_{R,E}. \tag{1-11-1}$$

It is flat over R because it is a colimit of flat R-algebras, and it represents $W^{\mathrm{fl}}_{R,E}$ because each $\Lambda^i_{R,E}$ represents U_i. As an example, if $E = E' \amalg E''$, where E''

consists of only copies of the unit ideal, then $\Lambda_{R,E}$ agrees with the monoid algebra $\Lambda_{R,E'}[\mathbb{N}^{(E'')}]$. We will often use the shortened forms Λ_E or, when $E = \{\mathfrak{m}\}$, $\Lambda_{\mathfrak{m}}$.

Since $\Lambda_{R,E}$ represents W^{fl}, which takes values in R-algebras, $\Lambda_{R,E}$ carries the structure of a co-R-algebra object in $\mathsf{Ring}_R^{\mathrm{fl}}$. Because $\mathsf{Ring}_R^{\mathrm{fl}}$ is closed under coproducts (the tensor product of flat modules being flat), a co-ring structure consists in morphisms

$$\Delta^+, \Delta^\times \colon \Lambda_{R,E} \longrightarrow \Lambda_{R,E} \otimes_R \Lambda_{R,E}, \quad \varepsilon^+, \varepsilon^\times \colon \Lambda_{R,E} \longrightarrow R \tag{1-11-2}$$

corresponding to addition, multiplication, the additive identity, and the multiplicative identity on the functor $W_{R,E}^{\mathrm{fl}}$. The R-linear structure on $W_{R,E}^{\mathrm{fl}}$ corresponds to a morphism

$$\beta \colon \Lambda_{R,E} \to R^R = \prod_R R. \tag{1-11-3}$$

All these structure maps satisfy the opposite of the R-algebra axioms. (In the language of schemes, one would say this makes $\operatorname{Spec} \Lambda_{R,E}$ an R-algebra scheme over R; or in the language of [Borger and Wieland 2005], it makes $\Lambda_{R,E}$ an R-R-biring.)

1.12. *Definition of W in general.* We can view $\Lambda_{R,E}$ as an object of Ring_R, instead of $\mathsf{Ring}_R^{\mathrm{fl}}$. Then define $W_{R,E}$ as a set-valued functor on Ring_R by

$$W_{R,E}(A) = \operatorname{Hom}_{\mathsf{Ring}_R}(\Lambda_{R,E}, A). \tag{1-12-1}$$

The structure maps (1-11-2)–(1-11-3) give $W_{R,E}$ the structure of a functor with values in R-algebras:

$$W_{R,E} \colon \mathsf{Ring}_R \longrightarrow \mathsf{Ring}_R. \tag{1-12-2}$$

(Note that here we really use the fact that the coproduct in $\mathsf{Ring}_R^{\mathrm{fl}}$ agrees with that in Ring_R. In 1.11, it was used only to justify the symbol $\otimes$ for the coproduct.)

For any $A \in \mathsf{Ring}_R$, let us call the $W_{R,E}(A)$ the R-algebra of *E-typical Witt vectors with entries in A*. Its restriction to $\mathsf{Ring}_R^{\mathrm{fl}}$ agrees with $W_{R,E}^{\mathrm{fl}}$ because $\mathsf{Ring}_R^{\mathrm{fl}}$ is a full subcategory of Ring_R.

We will often write W_E or W for $W_{R,E}$ when there is no risk of confusion. When E consists of a single ideal $\mathfrak{m}$, we will also write $W_{R,\mathfrak{m}}$ or $W_{\mathfrak{m}}$.

1.13. *Remark: Kan extensions.* In categorical terms, $W_{R,E}$ is the left Kan extension of $i \circ W_{R,E}^{\mathrm{fl}}$ along the inclusion functor i:

$$\begin{array}{ccc} \mathsf{Ring}_R^{\mathrm{fl}} & \xrightarrow{\ i\ } & \mathsf{Ring}_R \\ {\scriptstyle W_{R,E}^{\mathrm{fl}}}\uparrow & & \uparrow{\scriptstyle W_{R,E}} \\ \mathsf{Ring}_R^{\mathrm{fl}} & \xrightarrow{\ i\ } & \mathsf{Ring}_R. \end{array} \tag{1-13-1}$$

(See [Borceux 1994a, 3.7], for example, for the general theory of Kan extensions.) I mention this only to emphasize that the passage from the E-flat case to the general case is by a purely category-theoretic process, and hence the heart of the theory lies in the E-flat case. This is in contrast to the common point of view that the purpose of Witt vector functors is to lift rings from positive characteristic to characteristic zero.

1.14. *Ghost map w.* The ghost map

$$w\colon W_{R,E}(A) \longrightarrow \prod_{\mathbb{N}^{(E)}} A$$

is the natural map induced by the universal property of Kan extensions applied to the inclusion maps $W^{\mathrm{fl}}_{R,E}(A) \to \prod_{\mathbb{N}^{(E)}} A$, which are functorial in A. Equivalently, it is the morphism of functors induced by the map

$$\Psi_{R,E} = \Lambda^0_{R,E} \longrightarrow \Lambda_{R,E}$$

of representing objects. When A is E-flat, it is harmless to identify w with the inclusion map.

1.15. *Example: p-typical and big Witt vectors.* Suppose R is $\mathbb{Z}$. If E consists of the single ideal $p\mathbb{Z}$, then W agrees with the classical p-typical Witt vector functor [Witt 1937]. Indeed, for p-torsion free rings A, this follows from Cartier's lemma, which says that the traditionally defined p-typical Witt vector functor restricted to the category of p-torsion-free rings has the same universal property as W^{fl}. (See [Bourbaki 1983, IX.44, exercice 14] or [Lazard 1975, VII§4].) Therefore, they are isomorphic functors. For A general, one just observes that the traditional functor is represented by the ring $\mathbb{Z}[x_0, x_1, \dots]$, which is p-torsion free, and so it is the left Kan extension of its restriction to the category of p-torsion-free rings. Therefore it agrees with W as defined here.

Another proof of this is given in 3.5. It makes a direct connection with the traditional Witt components, rather than going through the universal property.

Suppose instead that E is the family of all maximal ideals of $\mathbb{Z}$. Then W agrees with the classical big Witt vector functor. As above, this can be shown by reducing to the torsion-free case and then citing the analogue of Cartier's lemma. (Which version of Cartier's lemma depends on how we define the classical big Witt vector functor. If we use generalized Witt polynomials, we need [Bourbaki 1983, IX.55, exercise 41b]. If it is defined as the cofree λ-ring functor, as in [Grothendieck 1958], then we need Wilkerson's theorem [1982, Proposition 1.2].)

Finally, we will see in 3.5 that when R is a complete discrete valuation ring and E consists of the maximal ideal of R, then W agrees with Hazewinkel's ramified Witt vector functor [Hazewinkel 1978, (18.6.13)].

1.16. *Comonad structure on W.* The functor $W^{\mathrm{fl}}\colon \mathsf{Ring}_R^{\mathrm{fl}} \to \mathsf{Ring}_R^{\mathrm{fl}}$ is naturally a comonad, being the composition of a functor (the forgetful one) with its right adjoint, and this comonad structure prolongs naturally to $W_{R,E}$. The reason for this can be expressed in two ways—in terms of Kan extensions or in terms of representing objects.

The first way is to invoke the general fact that $W_{R,E}$, as the Kan extension of the comonad $W^{\mathrm{fl}}_{R,E}$, has a natural comonad structure. This uses the commutativity of (1-13-1) and the fullness and faithfulness of i. The other way is to translate the structure on W^{fl} of being a comonad into a structure on its representing object $\Lambda_{R,E}$. One then observes that this is exactly the structure for the underlying R-algebra $i(\Lambda_{R,E})$ to represent a comonad on Ring_R. (This is called an R-plethory structure in [Borger and Wieland 2005].)

1.17. *Λ-rings.* The category $\mathsf{Ring}_{\Lambda_{R,E}}$ of $\Lambda_{R,E}$-rings is by definition the category of coalgebras for the comonad $W_{R,E}$, that is, the category of R-algebras equipped with a coaction of the comonad $W_{R,E}$. Since $W_{R,E}$ extends $W^{\mathrm{fl}}_{R,E}$, a $\Lambda_{R,E}$-ring structure on an E-flat R-algebra A is the same as a commuting family of Frobenius lifts ψ_α.

When $R = \mathbb{Z}$ and E is the family of all maximal ideals of $\mathbb{Z}$, then a Λ-ring is the same as a λ-ring in the sense of [Grothendieck 1958] (and originally called a "special λ-ring"). In the E-flat case, this is Wilkerson's theorem [1982, Proposition 1.2]. The proof is an exercise in symmetric functions, but the deeper meaning eludes me. The general case follows from the E-flat case by category theory, as in 1.15.

1.18. *Free Λ-rings and $\Lambda \odot -$.* Since $W_{R,E}$ is a representable comonad on Ring_R, the forgetful functor from the category of $\Lambda_{R,E}$-rings to the category of R-algebras has a left adjoint denoted $\Lambda_{R,E} \odot -$. This follows either from the adjoint functor theorem in category theory [Borceux 1994a, 3.3.3], or by simply writing down the adjoint in terms of generators and relations, as in [Borger and Wieland 2005, 1.3]. The second approach involves the R-plethory structure on $\Lambda_{R,E}$, and is similar to the description of tensor products, free differential rings, and so on in terms of generators and relations.

The functor $\Lambda_{R,E} \odot -$, viewed as an endofunctor on the category of R-algebras, is naturally a monad, simply because it is the left adjoint of the comonad $W_{R,E}$. Further, the category of algebras for this monad is naturally equivalent to $\mathsf{Ring}_{\Lambda_{R,E}}$. This can be proved using Beck's theorem [Borceux 1994b, 4.4.4], and is the same as the fact that the category of K-modules, for any ring K, can be defined as the category of algebras for the monad $K \otimes -$ or coalgebras for the comonad $\mathrm{Hom}(K, -)$.

We can interpret elements of $\Lambda_{R,E}$ as natural operations on $\Lambda_{R,E}$-rings. Indeed, a $\Lambda_{R,E}$-ring structure on a ring A is by definition a (type of) map $A \to W_{R,E}(A)$. It therefore induces a set map

$$\Lambda_{R,E} \times A \longrightarrow \Lambda_{R,E} \times W_{R,E}(A) = \Lambda_{R,E} \times \mathrm{Hom}_R(\Lambda_{R,E}, A) \longrightarrow A,$$

which is functorial in A. In particular, if we take $A = \Lambda_{R,E}$, we get a set map

$$\Lambda_{R,E} \times \Lambda_{R,E} \xrightarrow{\circ} \Lambda_{R,E}. \tag{1-18-1}$$

It agrees with the restriction of the composition map $\circ$ on $\Psi_{R[1/E],E} = R[1/E] \otimes_R \Psi_{R,E}$ given in 1.5. In particular, it is associative with identity e.

In fact, all natural operations on $\Lambda_{R,E}$-rings come from $\Lambda_{R,E}$ in this way. See [Borger and Wieland 2005] for an abstract account from this point of view.

1.19. *Remark: identity-based approaches.* It is possible to set up the theory of $\Lambda_{R,E}$-rings more concretely using universal identities rather than category theory. (See [Buium 1996; Buium and Simanca 2009; Joyal 1985a; 1985b], for example.) In this subsection, I will say something about that point of view and its relation to the category-theoretic one, but it will not be used elsewhere in this paper.

First suppose that for each $\alpha \in E$, the ideal $\mathfrak{m}_\alpha$ is generated by a single element π_α. For any $\Lambda_{R,E}$-ring A and any element $a \in A$, there exists an element $\delta_\alpha(a) \in A$ such that

$$\psi_\alpha(a) = a^{q_\alpha} + \pi_\alpha \delta_\alpha(a).$$

If we now assume that A is E-flat, the element $\delta_\alpha(a)$ is uniquely determined by this equation, and therefore δ_α defines an operator on A:

$$\delta_\alpha(a) = \frac{\psi_\alpha(a) - a^{q_\alpha}}{\pi_\alpha}.$$

Observe that if the integer q_α maps to 0 in R, for example when R is a ring of integers in a function field, then δ_α is additive; but otherwise it essentially never is. (Also note that δ_α is the same as the operator $\theta_{\pi_\alpha,1}$ defined in 3.1 below.)

Conversely, if A is an E-flat R-algebra, equipped with operators δ_α, there is at most one $\Lambda_{R,E}$-ring structure on A whose δ_α-operators are the given ones. To say when such a $\Lambda_{R,E}$-ring structure exists, we only need to express in terms of the operators δ_α the condition that the operators ψ_α be commuting R-algebra homomorphisms. After dividing by any accumulated factors of π_α, this gives the identities of Buium–Simanca [2009, Definition 2.1]:

$$\delta_\alpha(r) = \frac{r - r^{q_\alpha}}{\pi_\alpha}, \quad \text{for } r \in R, \tag{1-19-1}$$

$$\delta_\alpha(a+b) = \delta_\alpha(a) + \delta_\alpha(b) + C_\alpha(a,b), \tag{1-19-2}$$

$$\delta_\alpha(ab) = \delta_\alpha(a) b^{q_\alpha} + a^{q_\alpha} \delta_\alpha(b) + \pi_\alpha \delta_\alpha(a) \delta_\alpha(b), \tag{1-19-3}$$

$$\delta_\alpha \circ \delta_{\alpha'}(a) = \delta_{\alpha'} \circ \delta_\alpha(a) + C_{\alpha,\alpha'}\big(a, \delta_\alpha(a), \delta_{\alpha'}(a)\big), \tag{1-19-4}$$

where

$$C_\alpha(x, y) = \frac{x^{q_\alpha} + y^{q_\alpha} - (x+y)^{q_\alpha}}{\pi_\alpha} = -\sum_{i=1}^{q_\alpha - 1} \frac{1}{\pi_\alpha} \binom{q_\alpha}{i} x^{q_\alpha - i} y^i \tag{1-19-5}$$

and

$$C_{\alpha,\alpha'}(x, y, z) = \frac{C_{\alpha'}(x^{q_\alpha}, \pi_\alpha y)}{\pi_\alpha} - \frac{C_\alpha(x^{q_{\alpha'}}, \pi_{\alpha'} z)}{\pi_{\alpha'}} - \frac{\delta_\alpha(\pi_{\alpha'})}{\pi_{\alpha'}} z^{q_\alpha} + \frac{\delta_{\alpha'}(\pi_\alpha)}{\pi_\alpha} y^{q_{\alpha'}}. \tag{1-19-6}$$

One can easily check that the coefficients of these polynomials are elements of R.

For any R-algebra A, let us define a $\delta_{R,E}$-structure on A to be a family of operators δ_α satisfying the axioms above. Thus, if A is an E-flat R-algebra, then a $\Lambda_{R,E}$-structure—by definition a commuting family of Frobenius lifts indexed by E—is equivalent to a $\delta_{R,E}$-structure. The point of all this, then, is that if we no longer require A to be E-flat, a $\delta_{R,E}$-structure is generally stronger than having a commuting family of Frobenius lifts, but it is still equivalent to having a $\Lambda_{R,E}$-structure. This offers another point of view on the difference between a $\Lambda_{R,E}$-structure and a commuting family of Frobenius lifts: A $\delta_{R,E}$-structure is well behaved from the point of view of universal algebra (and hence so is a $\Lambda_{R,E}$-structure) because it is given by operators δ_α whose effect on the ring structure is described by universal identities, as above; but the structure of a commuting family of Frobenius lifts does not have this property because of the existential quantifier hidden in the word *lift*.

The equivalence between $\delta_{R,E}$-structures and $\Lambda_{R,E}$-structures can be seen as follows. For E-flat R-algebras A, it was explained above. For general A, the equivalence can be shown by checking that the cofree $\delta_{R,E}$-ring functor is represented by an E-flat R-algebra (in fact, a free one). It therefore agrees with the left Kan extension of its restriction to the category of E-flat algebras, and hence agrees with $W_{R,E}$.

We could extend the identity-based approach to the case where the ideals $\mathfrak{m}_\alpha$ are not principal, but then we would need operators

$$\delta_{\alpha,\pi_\alpha^*}(x) = \pi_\alpha^*(\psi_\alpha(x) - x^{q_\alpha}) \tag{1-19-7}$$

for every element $\pi_\alpha^* \in \mathfrak{m}_\alpha^{-1}$, or at least for those in a chosen generating set of $\mathfrak{m}_\alpha^{-1}$, and we would need additional axioms relating them. A particularly convenient generating set of $\mathfrak{m}_\alpha^{-1}$ is one of the form $\{1, \pi_\alpha^*\}$, which always exists. Further, for each $\alpha \in E$, it is enough to use the operators ψ_α and $\delta_{\alpha,\pi_\alpha^*}$ instead of $\delta_{\alpha,1}$ and $\delta_{\alpha,\pi_\alpha^*}$,

because $\delta_{\alpha,1}$ can be expressed in terms of ψ_α, by (1-19-7). Therefore if we fix elements $\pi_\alpha^* \in \mathfrak{m}_\alpha^{-1}$ which are R-module generators modulo 1, the relations needed for the generating set $\bigcup_{\alpha\in E}\{\psi_\alpha, \delta_{\alpha,\pi_\alpha^*}\}$ of operators are those in (1-19-1)–(1-19-6) but one needs to make the following changes: for each $\alpha \in E$, replace each occurrence of π_α^{-1} with π_α^*, and add axioms that ψ_α is an R-algebra homomorphism, that ψ_α commutes with all $\psi_{\alpha'}$ and all $\delta_{\alpha',\pi_{\alpha'}^*}$, and that (1-19-7) holds.

When R is an $\mathbb{F}_p$-algebra for some prime number p, the polynomials $C_\alpha(x, y)$ are zero and the axioms above simplify considerably. In particular, the operators δ_α are additive, and so it is possible to describe a $\Lambda_{R,E}$-structure using a cocommutative twisted bialgebra, the additive bialgebra of the plethory $\Lambda_{R,E}$. See [Borger and Wieland 2005, sections 2 and 10].

1.20. *Localization of the ring R of scalars.* Let R' be an E-flat R-algebra such that the structure map $R \to R'$ is an epimorphism of rings. (For example, the map $\operatorname{Spec} R' \to \operatorname{Spec} R$ could be an open immersion.) Then the family $(\mathfrak{m}_\alpha)_{\alpha\in E}$ induces a family $(\mathfrak{m}'_\alpha)_{\alpha\in E}$ of ideals of R', where $\mathfrak{m}'_\alpha = \mathfrak{m}_\alpha R'$. By the assumptions on R', each $\mathfrak{m}'_\alpha$ is supramaximal. Let us write $E' = E$ and use the notation E' for the index set of the $\mathfrak{m}'_\alpha$.

Let us construct an isomorphism:

$$R' \otimes_R \Lambda_{R,E} \xrightarrow{\sim} \Lambda_{R',E'}. \tag{1-20-1}$$

The category $\mathsf{Ring}^{\mathsf{fl}}_{\Lambda_{R',E'}}$ (see 1.6) is a subcategory of the category of $\mathsf{Ring}^{\mathsf{fl}}_{\Lambda_{R,E}}$. Indeed, any object $A' \in \mathsf{Ring}^{\mathsf{fl}}_{\Lambda_{R',E'}}$ is an R-algebra with endomorphisms $\psi_{\mathfrak{m}_\alpha}$, for each $\alpha \in E$. These endomorphisms are again commuting Frobenius lifts, simply because $A'/\mathfrak{m}'_\alpha A' = A'/\mathfrak{m}_\alpha A'$. Since A' is E'-flat (and by the assumptions on R'), A' is E-flat. Therefore, it can be viewed as a $\Lambda_{R,E}$-ring.

Further, $\mathsf{Ring}^{\mathsf{fl}}_{\Lambda_{R',E'}}$ agrees with the subcategory of $\mathsf{Ring}^{\mathsf{fl}}_{\Lambda_{R,E}}$ consisting of objects A whose structure map $R \to A$ factors through R', necessarily uniquely. Now consider the underlying-set functor on this category. From the definition of $\mathsf{Ring}^{\mathsf{fl}}_{\Lambda_{R',E'}}$, this functor is represented by the right-hand side of (1-20-1), and from the second description, it is represented by the left-hand side. Let (1-20-1) be the induced isomorphism on representing objects. It sends an element $r' \otimes f$ to $r'f$.

The isomorphism of represented functors which is induced by (1-20-1) gives natural maps

$$W_{R',E'}(A') \xrightarrow{\sim} W_{R,E}(A'), \tag{1-20-2}$$

for R'-algebras A'.

Finally, let us show that for any R'-algebra B', the canonical map

$$\Lambda_{R,E} \odot B' \xrightarrow{\sim} \Lambda_{R',E'} \odot B' \tag{1-20-3}$$

is an isomorphism. It is enough to show that for any R'-algebra A', the induced map

$$\mathrm{Hom}_{R'}(\Lambda_{R',E'} \odot B', A') \longrightarrow \mathrm{Hom}_{R'}(\Lambda_{R,E} \odot B', A')$$

is a bijection. Since $\mathsf{Ring}_{R'}$ is a full subcategory of Ring_R, the right-hand side agrees with $\mathrm{Hom}_R(\Lambda_{R,E} \odot B', A')$, and so the map above is an isomorphism by (1-20-2).

1.21. *Teichmüller lifts.* Let A be an R-algebra, let A° denote the commutative monoid of all elements of A under multiplication, and let $R[A^\circ]$ denote the monoid algebra on A°. Then for each $\alpha \in E$, the monoid endomorphism $a \mapsto a^{q_\alpha}$ of A° induces an R-algebra endomorphism ψ_α of $R[A^\circ]$ which reduces to the q_α-th power map modulo $\mathfrak{m}_\alpha$. Since $R[A^\circ]$ is free as an R-module, it is flat. And since the various ψ_α commute with each other, they provide $R[A^\circ]$ with a $\Lambda_{R,E}$-structure. Combined with the R-algebra map $R[A^\circ] \to A$ given by the counit of the evident adjunction, this gives, by the right-adjoint property of $W_{R,E}$, a $\Lambda_{R,E}$-ring map $t\colon R[A^\circ] \to W_{R,E}(A)$. We write the composite monoid map

$$A^\circ \xrightarrow{\text{unit}} R[A^\circ]^\circ \xrightarrow{t^\circ} W_{R,E}(A)^\circ$$

as simply $a \mapsto [a]$. It is a section of the R-algebra map $w_0\colon W_{R,E}(A) \to A$ and is easily seen to be functorial in A. The element $[a]$ is called the *Teichmüller lift* of a.

2. Grading and truncations

2.1. *Ordering on $\mathbb{Z}^{(E)}$.* For two elements $n', n \in \mathbb{Z}^{(E)} = \bigoplus_E \mathbb{Z}$, write $n' \leqslant n$ if we have $n'_\alpha \leqslant n_\alpha$ for all $\alpha \in E$. Also put

$$[0, n] = \{n' \in \mathbb{N}^{(E)} \mid n' \leqslant n\}.$$

2.2. *Truncations.* We have the following decomposition of $\Psi_{R,E}$:

$$\Psi_{R,E} = \bigotimes_{\alpha\in E} \bigotimes_{i\in\mathbb{N}} R[\psi_\alpha^{\circ i}] = \bigotimes_{n\in\mathbb{N}^{(E)}} R[\psi_n] = R[\psi_n | n \in \mathbb{N}^{(E)}].$$

(Thus, $\Psi_{R,E}$ is an $\mathbb{N}^{(E)}$-indexed coproduct in the category of R-algebras, much like graded rings are monoid-indexed coproducts in the category of modules. One might say that $\Psi_{R,E}$ is an $\mathbb{N}^{(E)}$-graded plethory. This point of view will not be used below.) For each $n \in \mathbb{Z}^{(E)}$, put

$$\Psi_{R,E,n} = \bigotimes_{\alpha\in E} \bigotimes_{0\leqslant i\leqslant n_\alpha} R[\psi_\alpha^{\circ i}] = \bigotimes_{n'\in[0,n]} R[\psi_{n'}] = R\big[\psi_{n'} | n' \in [0, n]\big].$$

Then $\Psi_{R,E,n}$ represents the Ring_R-valued functor that sends A to the product ring $A^{[0,n]}$, which is naturally a quotient of $A^{\mathbb{N}^{(E)}}$.

Define a similar filtration on $\Lambda_{R,E}$ by

$$\Lambda_{R,E,n} = \Lambda_{R,E} \cap \big(R[1/E] \otimes_R \Psi_{R,E,n}\big). \tag{2-2-1}$$

We will often use the shortened forms $\Lambda_{E,n}$, $\Psi_{E,n}$, $\Lambda_{\mathfrak{m},n}$, $\Psi_{\mathfrak{m},n}$, and so on.

2.3. Proposition. (a) *For each $n \in \mathbb{N}^{(E)}$, the R-scheme* $\operatorname{Spec} \Lambda_{R,E,n}$ *admits a unique structure of an R-algebra object in the category of R-schemes such that the map* $\operatorname{Spec} \Lambda_{R,E} \to \operatorname{Spec} \Lambda_{R,E,n}$ *induced by the inclusion $\Lambda_{R,E,n} \subseteq \Lambda_{R,E}$ is a homomorphism of R-algebra schemes over R.*

(b) *For each $m, n \in \mathbb{N}^{(E)}$, we have*

$$\Lambda_{R,E,m} \circ \Lambda_{R,E,n} \subseteq \Lambda_{R,E,m+n}, \tag{2-3-1}$$

where $\circ$ denotes the composition map of (1-18-1).

Proof. (a) Write $\Lambda = \Lambda_{R,E}$, $\Lambda_n = \Lambda_{R,E,n}$, and so on. First observe that, for any integer $i \geqslant 0$, all the maps in the diagram

$$\begin{array}{ccc} R[1/E] \otimes_R \Psi_n^{\otimes_R i} & \xrightarrow{a_i} & R[1/E] \otimes_R \Psi^{\otimes_R i} \\ \uparrow & & \uparrow{\scriptstyle c_i} \\ \Lambda_n^{\otimes_R i} & \xrightarrow{b_i} & \Lambda^{\otimes_R i} \end{array}$$

are injective. Indeed, a_i clearly is; the vertical maps are because they become isomorphisms after base change to $R[1/E]$ and because Λ_n and Λ are E-flat; and it follows formally that b_i is injective. Then the uniqueness of the desired R-algebra scheme structure on $\operatorname{Spec} \Lambda_n$, follows from the injectivity of b_2.

Now consider existence. Let

$$\Delta\colon R[1/E] \otimes_R \Psi \longrightarrow R[1/E] \otimes_R \Psi \otimes_R \Psi$$

denote the ring map that induces the addition (resp. multiplication) map on the ring scheme $\operatorname{Spec} R[1/E] \otimes_R \Psi_R$. To show that the desired addition and multiplication maps on $\operatorname{Spec} \Lambda_n$ exist, it is enough to show

$$\Delta(\Lambda_n) \subseteq \Lambda_n \otimes_R \Lambda_n. \tag{2-3-2}$$

In fact, once we do this, we will be done: because each $c_i \circ b_i$ is injective, the ring axioms (associativity, distributivity, and so on) will follow from those on $\operatorname{Spec} R[1/E] \otimes_R \Psi$.

The map Δ sends ψ_α to $\psi_\alpha \otimes 1 + 1 \otimes \psi_\alpha$ (resp. $\psi_\alpha \otimes \psi_\alpha$). Therefore we have

$$\Delta(R[1/E] \otimes_R \Psi_n) \subseteq R[1/E] \otimes_R \Psi_n \otimes_R \Psi_n,$$

and hence

$$\Delta(\Lambda_n) \subseteq \Lambda^{\otimes_R 2} \cap \big(R[1/E] \otimes_R \Psi_n^{\otimes_R 2}\big) = \Lambda_n^{\otimes_R 2}.$$

This establishes (2-3-2) and hence completes the proof of (a).

(b) Combine the definition (2-2-1) with the inclusion

$$(R[1/E] \otimes_R \Psi_m) \circ (R[1/E] \otimes_R \Psi_n) \subseteq (R[1/E] \otimes_R \Psi_{m+n})$$

and the inclusion $\Lambda_m \circ \Lambda_n \subseteq \Lambda$. □

2.4. *Witt vectors of finite length.* Let $W_{R,E,n}$ denote the functor $\mathsf{Ring}_R \to \mathsf{Ring}_R$ represented by $\Lambda_{R,E,n}$:

$$W_{R,E,n}(A) = \mathrm{Hom}_R(\Lambda_{R,E,n}, A). \tag{2-4-1}$$

We call $W_{R,E,n}$ the *E-typical Witt vector functor of length n*. As in 1.12, we will often write $W_{E,n}$ or W_n; when $E = \{\mathfrak{m}\}$, we will also write $W_{R,\mathfrak{m},n}$ or $W_{\mathfrak{m},n}$. We then have

$$W_{R,E}(A) = \lim_n W_{R,E,n}(A). \tag{2-4-2}$$

(Note that it is often better to view $W_{R,E}(A)$ as a pro-ring than to actually take the limit. If we preferred topological rings to pro-rings, we could take the limit and endow it with the natural pro-discrete topology.) It follows from 4.4 and (5-4-2) below that the maps in this projective system are surjective.

The (truncated) ghost map

$$w_{\leqslant n} \colon W_{R,E,n}(A) \longrightarrow A^{[0,n]}, \tag{2-4-3}$$

is the one induced by the inclusion $\Psi_{R,E,n} \subseteq \Lambda_{R,E,n}$ of representing objects. For any $i \in [0,n]$, the composition $w_{\leqslant n}$ with the projection onto the i-th factor gives another natural map

$$w_i \colon W_{R,E,n}(A) \longrightarrow A. \tag{2-4-4}$$

Also the containment (2-3-1) induces an R-algebra map

$$W_{R,E,m+n}(A) \longrightarrow W_{R,E,n}\big(W_{R,E,m}(A)\big) \tag{2-4-5}$$

which sends an element $a \colon \Lambda_{R,E,m+n} \to A$ of $W_{R,E,m+n}(A)$ to the map $\gamma \mapsto [\beta \mapsto a(\beta \circ \gamma)]$, for variables $\gamma \in \Lambda_{R,E,n}$ and $\beta \in \Lambda_{R,E,m}$. We will call (2-4-5) *co-plethysm*. It agrees with the map of functors induced by the map

$$\Lambda_{R,E,m} \odot \Lambda_{R,E,n} \longrightarrow \Lambda_{R,E,m+n}, \quad \beta \odot \gamma \mapsto \beta \circ \gamma \tag{2-4-6}$$

on representing objects, where $\beta \odot \gamma$ is defined as in [Borger and Wieland 2005].

Finally, observe that for any element $f \in \Lambda_{R,E,n}$ the natural $\Lambda_{R,E}$-ring operation

$$f \colon W_{R,E}(A) \to W_{R,E}(A)$$

(a map of sets) descends to a map

$$f\colon W_{R,E,m+n}(A) \to W_{R,E,m}(A).$$

Indeed, it is the composition

$$W_{R,E,m+n}(A) \overset{(2\text{-}4\text{-}5)}{\longrightarrow} W_{R,E,n}\big(W_{R,E,m}(A)\big) = \mathrm{Hom}(\Lambda_{R,E,n}, W_{R,E,m}(A)) \overset{-(f)}{\longrightarrow} W_{R,E,m}(A), \quad (2\text{-}4\text{-}7)$$

where $-(f)$ denotes the map that evaluates at f. Particularly important is the example $f = \psi_n$, where the induced map

$$\psi_n\colon W_{R,E,m+n}(A) \to W_{R,E,m}(A) \quad (2\text{-}4\text{-}8)$$

is a ring homomorphism.

2.5. *Remark: traditional versus normalized indexing.* Consider the p-typical Witt vectors, where R is $\mathbb{Z}$ and E consists of the single ideal $p\mathbb{Z}$. Let W'_n denote Witt's functor, as defined in [Witt 1937]. So, for example,

$$W'_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}.$$

In 3.5, we will construct an isomorphism $W'_{n+1} \cong W_n$. Thus, up to a normalization of indices, our truncated Witt functors agree with Witt's.

The reason for this normalization is to make the indexing behave well under plethysm. By (2-3-1) and (2-4-5), the index set has the structure of a commutative monoid, and so it is preferable to use an index set with a familiar monoid structure. If we were to insist on agreement with Witt's indexing, we would have to replace the sum $m+n$ in (2-3-1) and (2-4-5) with $m+n-(1,1,\dots)$, where this would be computed in the product group $\mathbb{Z}^E$. The reason why this has not come up in earlier work is that the plethysm structure has traditionally been used only through the Frobenius maps ψ_α. In other words, only the shift operator on the indexing set was used. Thus the distinction between $\mathbb{N}$ and $\mathbb{Z}_{\geqslant 1}$ was not so important because the shift operator $n \mapsto n+1$ is written the same way on both. But making the identification of $\mathbb{N}$ and $\mathbb{Z}_{\geqslant 1}$ a monoid isomorphism would involve the unwelcome addition law $m+n-1$ on $\mathbb{Z}_{\geqslant 1}$.

It is different with the big Witt vectors, where R is $\mathbb{Z}$ and E consists of all maximal ideals 1.15. They are also traditionally indexed by the positive integers [Hazewinkel 1978, (17.4.4)], but here the positive integers are used multiplicatively rather than additively. In particular, the monoid structure that is required is the obvious one; so the traditional indexing is in agreement with the normalized one: the big Witt ring $W_{p^n}(A)$ (using traditional multiplicative indexing) is naturally isomorphic to our p-typical ring $W_n(A)$ and to Witt's $W'_{n+1}(A)$.

2.6. *Localization of the ring R of scalars.* Let R' be an E-flat R-algebra such that the structure map $R \to R'$ is an epimorphism of rings, as in 1.20.

Then for each $n \in \mathbb{N}^{(E)}$, we have

$$\begin{aligned} R' \otimes_R \Lambda_{R,E,n} &= R' \otimes_R \big(\Lambda_{R,E} \cap (R[1/E] \otimes_R \Psi_{R,E,n})\big) \\ &\xrightarrow{\sim} \big(R' \otimes_R \Lambda_{R,E}\big) \cap (R'[1/E] \otimes_{R'} \Psi_{R',E',n}). \end{aligned}$$

(We only need to check that the displayed map is an isomorphism along E, in which case it is true because R' is E-flat over R.) By (1-20-1), this gives an isomorphism of R'-algebras

$$R' \otimes_R \Lambda_{R,E,n} \xrightarrow{\sim} \Lambda_{R',E',n}. \tag{2-6-1}$$

The induced isomorphism of represented functors gives natural maps

$$W_{R',E',n}(A') \xrightarrow{\sim} W_{R,E,n}(A'), \tag{2-6-2}$$

for R'-algebras A'. If A is an R-algebra, the inverse of this map induces a map

$$R' \otimes_R W_{R,E,n}(A) \longrightarrow W_{R',E',n}(R' \otimes_R A) \tag{2-6-3}$$

We will see in 6.1 that this is an isomorphism.

As with (1-20-3), the map (2-6-2) induces an isomorphism

$$\Lambda_{R,E,n} \odot B' \xrightarrow{\sim} \Lambda_{R',E',n} \odot B', \tag{2-6-4}$$

for any R'-algebra B',

2.7. Proposition. *Let A be an E-flat R-algebra. Then the ghost map*

$$w_{\leqslant n} \colon W_{R,E,n}(A) \longrightarrow A^{[0,n]}$$

is injective. If A is an $R[1/E]$-algebra, it is an isomorphism.

Recall that the analogous facts for infinite-length Witt vectors are also true, either by construction 1.8 or by the universal property 1.9.

Proof. If every ideal in E is the unit ideal, then $\Lambda_{R,E} = \Psi_{R,E}$, and hence we have $\Lambda_{R,E,n} = \Psi_{R,E,n}$. The statement about $R[1/E]$-algebras then follows from (2-6-1). The statement about E-flat R-algebras follows by considering the injection

$$A \to R[1/E] \otimes_R A$$

and applying the previous case to $R[1/E] \otimes_R A$. □

3. Principal single-prime case

For this section, we will restrict to the case where E consists of one ideal $\mathfrak{m}$ generated by an element π. Our purpose is to extend the classical components of Witt vectors from the p-typical context (where R is $\mathbb{Z}$ and E consists of the single ideal $p\mathbb{Z}$) to this slightly more general one. The reason for this is that the Witt components are well-suited to calculation. In the following sections, we will see how to use them, together with 4.1, 5.4, and 6.1, to draw conclusions when E is general.

In fact, the usual arguments and definitions in the classical theory of Witt vectors carry over as long as one modifies the usual Witt polynomials by replacing every p in an exponent with $q_{\mathfrak{m}}$, and every p in a coefficient with π. Some things, such as the Verschiebung operator, depend on the choice of π, and others do not, such as the Verschiebung filtration.

Let n denote an element of $\mathbb{N}$. Let us abbreviate

$$\Lambda_{\mathfrak{m}} = \Lambda_{R,E}, \quad \Lambda_{\mathfrak{m},n} = \Lambda_{R,E,n}, \quad W_{\mathfrak{m}} = W_{R,E}, \quad q = q_{\mathfrak{m}}, \quad \psi = \psi_{\mathfrak{m}},$$

and so on.

3.1. *θ operators.* Define elements $\theta_{\pi,0}, \theta_{\pi,1}, \ldots$ of

$$R[1/\pi] \otimes_R \Lambda_{\mathfrak{m}} = R[1/\pi] \otimes_R \Psi_{\mathfrak{m}}$$

recursively by the generalized Witt polynomials

$$\psi^{\circ n} = \theta_{\pi,0}^{q^n} + \pi\theta_{\pi,1}^{q^{n-1}} + \cdots + \pi^n\theta_{\pi,n}. \tag{3-1-1}$$

(Note that the exponent on the left side means iterated composition, while the exponents on the right mean usual exponentiation, iterated multiplication.) As in 1.5, we can view the elements $\theta_{\pi,i}$ as natural operators on $\Psi_{R[1/\pi],\mathfrak{m}}$-rings. We will often write $\theta_i = \theta_{\pi,i}$ when π is clear.

3.2. Lemma. *We have*

$$\psi \circ \theta_{\pi,n} = \theta_{\pi,n}^q + \pi\theta_{\pi,n+1} + \pi P(\theta_{\pi,0}, \ldots, \theta_{\pi,n-1}), \tag{3-2-1}$$

for some polynomial $P(\theta_{\pi,0}, \ldots, \theta_{\pi,n-1})$ with coefficients in R.

Proof. It is clear for $n = 0$. For $n \geqslant 1$, we will use induction. Recall the general implication

$$x \equiv y \bmod \mathfrak{m} \quad \Longrightarrow \quad x^{q^j} \equiv y^{q^j} \bmod \mathfrak{m}^{j+1},$$

for $j \geqslant 1$, which itself is easily proved by induction. Together with the formula (3-2-1) for $\psi \circ \theta_{\pi,i}$ with $i < n$, this implies

$$\begin{aligned}\psi \circ \psi^{\circ n} &= \sum_{i=0}^{n} \pi^i (\psi \circ \theta_i)^{q^{n-i}} \\ &\equiv \pi^n \psi \circ \theta_n + \sum_{i=0}^{n-1} \pi^i (\theta_i^q)^{q^{n-i}} \mod \mathfrak{m}^{n+1} R[\theta_0, \dots, \theta_{n-1}]\end{aligned}$$

When this is combined with the defining formula (3-1-1) for $\psi^{\circ(n+1)}$, we have

$$\pi^n \psi \circ \theta_n \equiv \pi^n \theta_n^q + \pi^{n+1} \theta_{n+1} \bmod \mathfrak{m}^{n+1} R[\theta_0, \dots, \theta_{n-1}].$$

Dividing by π^n completes the proof. □

3.3. Proposition. *The elements $\theta_{\pi,0}, \theta_{\pi,1}, \dots$ of $R[1/\pi] \otimes_R \Lambda_{\mathfrak{m}}$ lie in $\Lambda_{\mathfrak{m}}$, and they generate $\Lambda_{\mathfrak{m}}$ freely as an R-algebra. Further, the elements $\theta_{\pi,0}, \dots, \theta_{\pi,n}$ lie in $\Lambda_{\mathfrak{m},n}$, and they generate $\Lambda_{\mathfrak{m},n}$ freely as an R-algebra.*

This is essentially [Witt 1937, Theorem 1].

Proof. By induction, the elements $\theta_0, \dots, \theta_n$ generate the same sub-$R[1/\pi]$-algebra of $R[1/\pi] \otimes_R \Lambda_{\mathfrak{m}}$ as $\psi^{\circ 0}, \dots, \psi^{\circ n}$, and are hence algebraically independent over $R[1/\pi]$. Since $R \subseteq R[1/\pi]$, they are also algebraically independent over R.

Let B_n be the sub-R-algebra of $R[1/\pi] \otimes_R \Lambda_{\mathfrak{m}}$ generated by $\theta_0, \dots, \theta_n$, and let $B = \bigcup_n B_n$. To show $\Lambda_{\mathfrak{m}} \supseteq B$, we may assume by induction that $\Lambda_{\mathfrak{m}} \supseteq B_n$ and then show $\Lambda_{\mathfrak{m}} \supseteq B_{n+1}$. By 3.2 and because $\Lambda_{\mathfrak{m}}$ is a $\Lambda_{\mathfrak{m}}$-ring, we have

$$\pi\theta_{n+1} \in \left(\psi \circ \theta_n - \theta_n^q\right) + \mathfrak{m}\Lambda_{\mathfrak{m},n} \subseteq \mathfrak{m}\Lambda_{\mathfrak{m}}.$$

Dividing by π, we have $\theta_{n+1} \in \Lambda_{\mathfrak{m}}$, and hence $\Lambda_{\mathfrak{m}} \supseteq B_n[\theta_{n+1}] = B_{n+1}$.

On the other hand, by 3.2 again, we have

$$\psi \circ \theta_n \equiv \theta_n^q \bmod \mathfrak{m}B_{n+1}$$

for all n. Hence B, being generated by the θ_n, is a sub-$\Lambda_{\mathfrak{m}}$-ring of $R[1/\pi] \otimes_R \Lambda_{\mathfrak{m}}$. It follows that $B \supseteq \Lambda_{\mathfrak{m}} \circ e = \Lambda_{\mathfrak{m}}$, and therefore $B = \Lambda_{\mathfrak{m}}$.

Last, the equality $\Lambda_{\mathfrak{m},n} = B_n$ follows immediately from the above:

$$\begin{aligned}\Lambda_{\mathfrak{m},n} &= \Lambda_{\mathfrak{m}} \cap \left(R[1/\pi] \otimes_R \Psi_{\mathfrak{m},n}\right) = B \cap \left(R[1/\pi] \otimes_R \Psi_{\mathfrak{m},n}\right) \\ &= R[\theta_0, \dots] \cap R[1/\pi][\theta_0, \dots, \theta_n] \\ &= R[\theta_0, \dots, \theta_n] = B_n.\end{aligned}$$

□

3.4. *Example: Presentations of* $\Lambda_{\mathfrak{m},n} \odot A$. Using 3.3, we can turn a presentation of an R-algebra A into a presentation of $\Lambda_{\mathfrak{m},n} \odot A$. We have

$$\Lambda_{\mathfrak{m},n} \odot R[x] \cong \Lambda_{\mathfrak{m},n} = R[\theta_0, \dots, \theta_n],$$

where θ_k is short for $\theta_{\pi,k}$, which corresponds to the element $\theta_{\pi,k}(x) = \theta_{\pi,k} \odot x$.

Because the functor $\Lambda_{\mathfrak{m},n} \odot -$ preserves coproducts and coequalizers, we have

$$\Lambda_{\mathfrak{m},n} \odot \big(R[x_1, \dots, x_r]/(f_1, \dots, f_s)\big) = R[\theta_i(x_j)]/(\theta_i(f_k)), \tag{3-4-1}$$

where $0 \leqslant i \leqslant n$, $1 \leqslant j \leqslant r$, and $1 \leqslant k \leqslant s$. Here each expression $\theta_i(x_j)$ is a single free variable, and $\theta_i(f_k)$ is understood to be the polynomial in the variables $\theta_i(x_j)$ that results from expanding $\theta_i(f_k)$ using the sum and product laws for θ_i. Because $\Lambda_{\mathfrak{m},n} \odot -$ preserves filtered colimits, we can give a similar presentation of $\Lambda_{\mathfrak{m},n} \odot A$ for any R-algebra A. Similarly, we can take the colimit over n to get a presentation for $\Lambda_{\mathfrak{m}} \odot A$.

In the E-typical case, where E is finite, one can write down a presentation of $\Lambda_{R,E} \odot A$ by iterating (3-4-1), according to 5.3 below. We can pass from the case where E is finite to the case where it is arbitrary by taking colimits, as in 5.1.

The method above is not particular to the θ operators—it works for any subset of $\Lambda_{\mathfrak{m},n}$ that generates it freely as an R-algebra. For example, we can use the δ operators of 1.19. Let $\delta^i \in \Lambda_{\mathfrak{m}}$ denote the i-th iterate of δ_π. Then the elements $\delta^0, \dots, \delta^n$ lie in $\Lambda_{\mathfrak{m},n}$ and freely generate it as an R-algebra. (As in 3.3, this follows by induction, but in this case, there are no subtle congruences to check.) Therefore we have

$$\Lambda_{\mathfrak{m},n} \odot \big(R[x_1, \dots, x_r]/(f_1, \dots, f_s)\big) = R[\delta^i(x_j)]/(\delta^i(f_k)), \tag{3-4-2}$$

where $0 \leqslant i \leqslant n$, $1 \leqslant j \leqslant r$, and $1 \leqslant k \leqslant s$. We interpret the expressions $\delta^i(x_j)$ and $\delta^i(f_k)$ as above. The general E-typical case can be handled as above. (See [Buium and Simanca 2009, proof of Proposition 2.12].)

3.5. *Witt components.* It follows from 3.3 that, given π, we have a bijection

$$W_{\mathfrak{m}}(A) \xrightarrow{\sim} A \times A \times \cdots, \tag{3-5-1}$$

which sends a map $f\colon \Lambda_{\mathfrak{m}} \to A$ to the sequence $(f(\theta_{\pi,0}), f(\theta_{\pi,1}), \dots)$. To make the dependence on π explicit, we will often write $(x_0, x_1, \dots)_\pi$ for the image of $(x_0, x_1, \dots)$ under the inverse of this map. If $R = \mathbb{Z}$ and $\pi = p$, then this identifies $W_{\mathfrak{m}}(A)$ with the ring of p-typical Witt vectors as defined traditionally. Similarly, when R is a complete discrete valuation ring, we get an identification of $W_{\mathfrak{m}}(A)$ with Hazewinkel's ring of ramified Witt vectors $W^R_{q,\infty}(A)$. (See [Hazewinkel 1978, (18.6.13), (25.3.17), and (25.3.26)(i)].) We call the x_i the *Witt components* (relative to π) of the element $(x_0, \dots)_\pi \in W(A)$.

Similarly, using the free generating set $\theta_{\pi,0}, \dots, \theta_{\pi,n}$ of $\Lambda_{\mathfrak{m},n}$, we have a bijection

$$W_{\mathfrak{m},n}(A) \xrightarrow{\sim} A^{[0,n]}. \tag{3-5-2}$$

As above, we will write $(x_0, \dots, x_n)_\pi$ for the image of $(x_0, \dots, x_n)$ under the inverse of this map. This identifies $W_{\mathfrak{m},n}(A)$ with the traditionally defined ring of p-typical Witt vectors of length $n+1$. (For remarks on the $+1$ shift, see 2.5.)

Note that the Witt components do not depend on the choice of π in a simple, multilinear way. For example, if u is an invertible element of R and we have

$$(x_0, x_1, \dots)_\pi = (y_0, y_1, \dots)_{u\pi},$$

then we have

$$x_0 = y_0, \qquad x_1 = uy_1, \qquad x_2 = u^2 y_2 + \pi^{-1}(u - u^q) y_1^q, \quad \dots.$$

As in 3.4, we could use the free generating set $\delta^0, \delta^1, \dots$ of $\Lambda_{\mathfrak{m}}$ instead of $\theta_0, \theta_1, \dots$. This would give a different bijection between $W_{\mathfrak{m}}(A)$ and the set $A^{\mathbb{N}}$, and hence an R-algebra structure on the set $A^{\mathbb{N}}$ which is isomorphic to Witt's but not equal to it. The truncated versions agree up to $A \times A$, but differ after that. This is simply because $\delta^0 = \theta_0$ and $\delta^1 = \theta_1$, but $\delta^2 \neq \theta_2$. (See [Joyal 1985b, p. 179].)

3.6. *The ghost principle.* It follows from the descriptions (3-5-1) and (3-5-2) that $W_{\mathfrak{m}}$ and $W_{\mathfrak{m},n}$ preserve surjectivity. On the other hand, every R-algebra is a quotient of an $\mathfrak{m}$-flat R-algebra (even a free one). Therefore to prove any functorial identity involving rings of Witt vectors when $\mathfrak{m}$ is principal, it is enough to restrict to the $\mathfrak{m}$-flat case. Further, any $\mathfrak{m}$-flat R-algebra A is contained in an $R[1/\mathfrak{m}]$-algebra, such as $R[1/\mathfrak{m}] \otimes_R A$. Since $W_{\mathfrak{m}}$ and $W_{\mathfrak{m},n}$, being representable functors, preserve injectivity, it is even enough to check functorial identities on $R[1/\mathfrak{m}]$-algebras A, in which case rings of Witt vectors agree with the much more tractable rings of ghost components. An example with details is given in 3.7.

3.7. *Verschiebung.* For any R-algebra A define an operator V_π, called the Verschiebung (relative to π), on $W_{\mathfrak{m}}(A)$ by

$$V_\pi\big((y_0, y_1, \dots)_\pi\big) = (0, y_0, y_1, \dots)_\pi. \tag{3-7-1}$$

This is clearly functorial in A. Define another, identically denoted operator on the ghost ring $A^{\mathbb{N}}$ by the formula

$$V_\pi\big(\langle z_0, z_1, \dots \rangle\big) = \langle 0, \pi z_0, \pi z_1, \dots \rangle. \tag{3-7-2}$$

These operators are compatible in that we have $w(V_\pi(y)) = V_\pi(w(y))$ for all $y \in W_{\mathfrak{m}}(A)$, and the operator V_π on the ghost ring is clearly R-linear. It follows by

the ghost principle that the operator V_π on $W_\mathfrak{m}(A)$ is R-linear. Here is the argument in some detail.

We need to check the identities $rV_\pi(y) = V_\pi(ry)$ and $V_\pi(x+y) = V_\pi(x)+V_\pi(y)$, for $r \in R$, $x, y \in W_\mathfrak{m}(A)$. Write $x = (x_0, x_1, \dots)_\pi$ and $y = (y_0, y_1, \dots)_\pi$. If A is a E-flat, the ghost map $w\colon W_\mathfrak{m}(A) \to A^\mathbb{N}$ is injective. Therefore V_π is R-linear on $W_\mathfrak{m}(A)$, by the R-linearity of V_π on the ghost ring.

The general case then follows from E-flat case. Fix an E-flat R-algebra $\tilde{A}$ with a surjective R-algebra map $\tilde{A} \to A$. For each i, let $\tilde{y}_i$ be a pre-image of y_i, and set $\tilde{y} = (\tilde{y}_0, \dots)_\pi \in W_\mathfrak{m}(A)$. The induced map $f\colon W_\mathfrak{m}(\tilde{A}) \to W_\mathfrak{m}(A)$ then satisfies $f(\tilde{y}) = y$. Therefore we have

$$\begin{aligned} V_\pi(ry) &= V_\pi(rf(\tilde{y})) = V_\pi(f(r\tilde{y})) = f(V_\pi(r\tilde{y})) \\ &= f(rV_\pi(\tilde{y})) = rf(V_\pi(\tilde{y})) = rV_\pi(f(\tilde{y})) = rV_\pi(y). \end{aligned}$$

The additivity axiom follows similarly.

3.8. *Example.* $W_{R,\mathfrak{m},n}(R)$ has a presentation

$$R[x_1, \dots, x_n]/(x_i x_j - \pi^i x_j \mid 1 \leqslant i \leqslant j \leqslant n),$$

where the element x_i corresponds to $V_\pi^i(1)$.

3.9. *Teichmüller lifts.* Under the composition

$$A \xrightarrow{a \mapsto [a]} W(A) \xrightarrow{w} A \times A \times \cdots$$

(see 1.21), the image of a is $\langle a, a^q, a^{q^2}, \dots \rangle$. It follows from the ghost principle that

$$[a] = (a, 0, 0, \dots)_\pi \in W(A).$$

Multiplication by Teichmüller lifts also has a simple description in terms of Witt components:

$$[a](\dots, b_i, \dots)_\pi = (\dots, a^{q^i} b_i, \dots)_\pi. \tag{3-9-1}$$

Again, this follows from the ghost principle.

4. General single-prime case

Assume E consists of a single ideal $\mathfrak{m}$, possibly not principal. Let n be an element of $\mathbb{N}$. Let us write $W_{R,\mathfrak{m},n} = W_{R,E,n}$ and so on.

Let $K_\mathfrak{m}$ denote $R_\mathfrak{m}[1/\mathfrak{m}]$. If $\mathfrak{m}$ is the unit ideal, we understand $R_\mathfrak{m}$, and hence $K_\mathfrak{m}$, to be the zero ring. Otherwise, $R_\mathfrak{m}$ is a discrete valuation ring and $K_\mathfrak{m}$ is its fraction field. In particular, $\mathfrak{m}$ becomes principal in $R[1/\mathfrak{m}]$, $R_\mathfrak{m}$, and $K_\mathfrak{m}$. The following proposition then allows us to describe $W_{R,\mathfrak{m},n}(A)$ in terms of the case where $\mathfrak{m}$ is principal, and hence in terms of Witt components.

4.1. Proposition. *For $R' = R[1/\mathfrak{m}]$, $R_{\mathfrak{m}}$, $K_{\mathfrak{m}}$, write $W_{R',\mathfrak{m},n} = W_{R',\mathfrak{m}R',n}$. Then for any R-algebra A, the ring $W_{R,\mathfrak{m},n}(A)$ is the equalizer of the two maps*

$$W_{R[1/\mathfrak{m}],\mathfrak{m},n}\big(R[1/\mathfrak{m}] \otimes_R A\big) \times W_{R_{\mathfrak{m}},\mathfrak{m},n}\big(R_{\mathfrak{m}} \otimes_R A\big) \rightrightarrows W_{K_{\mathfrak{m}},\mathfrak{m},n}(K_{\mathfrak{m}} \otimes_R A)$$

induced by projection onto the two factors and the bifunctoriality of $W_{-,\mathfrak{m},n}(-)$.

Proof. The diagram

$$R \longrightarrow R[1/\mathfrak{m}] \times R_{\mathfrak{m}} \underset{\mathrm{pr}_2}{\overset{\mathrm{pr}_1}{\rightrightarrows}} K_{\mathfrak{m}}$$

is an equalizer diagram. Since $K_{\mathfrak{m}}$ is $\mathfrak{m}$-flat, so is any sub-R-module of $K_{\mathfrak{m}}$. It follows that for any R-algebra A, the induced diagram

$$A \longrightarrow \Big(R[1/\mathfrak{m}] \times R_{\mathfrak{m}}\Big) \otimes_R A \rightrightarrows K_{\mathfrak{m}} \otimes_R A$$

is an equalizer diagram. Since $W_{R,\mathfrak{m},n}$ is representable, it preserves equalizers, and so the induced diagram (writing $W_n = W_{R,\mathfrak{m},n}$)

$$W_n(A) \longrightarrow W_n\big(R[1/\mathfrak{m}] \otimes_R A\big) \times W_n\big(R_{\mathfrak{m}} \otimes_R A\big) \rightrightarrows W_n(K_{\mathfrak{m}} \otimes_R A)$$

is also an equalizer diagram. Then (2-6-2) completes the proof. □

4.2. *Verschiebung in general.* We can define Verschiebung maps

$$V^j \colon \mathfrak{m}^j \otimes_R W_{R,\mathfrak{m}}(A) \longrightarrow W_{R,\mathfrak{m}}(A). \tag{4-2-1}$$

To do this, it is enough, by 4.1, to restrict to the case where $\mathfrak{m}$ is principal, as long as our construction is functorial in A and R. So, choose a generator $\pi \in \mathfrak{m}$ and define

$$V^j(\pi^j \otimes y) = V_\pi^j(y), \tag{4-2-2}$$

for all $y \in W_{R,\mathfrak{m}}(A)$. On ghost components it satisfies

$$V^j(x \otimes \langle z_0, z_1, \dots\rangle) = \langle 0, \dots, 0, xz_0, xz_1, \dots\rangle,$$

where the number of leading zeros is j. In particular, it is independent of the choice of π, by the ghost principle.

If we write $W_{R,\mathfrak{m}}(A)_{(j)}$ for $W_{R,\mathfrak{m}}(A)$, viewed as a $W_{R,\mathfrak{m}}(A)$-algebra by way of the map $\psi_j \colon W_{R,\mathfrak{m}}(A) \to W_{R,\mathfrak{m}}(A)$, then the map

$$V^j \colon \mathfrak{m}^j \otimes_R W_{R,\mathfrak{m}}(A)_{(j)} \longrightarrow W_{R,\mathfrak{m}}(A), \tag{4-2-3}$$

is $W_{R,\mathfrak{m}}(A)$-linear, as is easily checked using the ghost principle. Expressed as a formula, it says

$$V^j(x \otimes y\psi_j(z)) = V^j(x \otimes y)z. \tag{4-2-4}$$

In particular, the image $V^j W_{R,\mathfrak{m}}(A)$ of V^j is an ideal of $W_{R,\mathfrak{m}}(A)$.

Let us also record the identities

$$\psi_j\big(V^j(x \otimes y)\big) = xy \tag{4-2-5}$$

and

$$V^j(x \otimes y)V^j(x' \otimes y') = xV^j(x' \otimes yy') \in \mathfrak{m}^j V^j W_{R,\mathfrak{m}}(A). \tag{4-2-6}$$

Again, one checks these using the ghost principle.

Finally, for any $n \in \mathbb{N}$, the map V^j descends to a map

$$V^j \colon \mathfrak{m}^j \otimes_R W_{R,\mathfrak{m},n}(A)_{(j)} \longrightarrow W_{R,\mathfrak{m},n+j}(A), \tag{4-2-7}$$

and the obvious analogues of the identities above hold here.

4.3. *Remark.* We can define Verschiebung maps even if we no longer assume there is only one ideal in E. For any $j \in \mathbb{N}^{(E)}$, let J denote the ideal $\prod_\alpha \mathfrak{m}_\alpha^{j_\alpha}$ of R. Then V^j would be a map $J \otimes_R W_{R,E}(A) \to W_{R,E}(A)$. The identities above, suitably interpreted, continue to hold. We will not need this multiple-prime version.

4.4. Proposition. *The sequence*

$$0 \longrightarrow \mathfrak{m}^j \otimes_R W_{R,\mathfrak{m},n}(A)_{(j)} \xrightarrow{V^j} W_{R,\mathfrak{m},n+j}(A) \longrightarrow W_{R,\mathfrak{m},j}(A) \longrightarrow 0 \tag{4-4-1}$$

is exact.

Proof. Write $W_{R',n} = W_{R',\mathfrak{m}R',n}$ when R' is an R-algebra such that the ideal $\mathfrak{m}R'$ is supramaximal.

First consider the case where $\mathfrak{m}$ is principal. Let $\pi \in \mathfrak{m}$ be a generator. Using (3-7-1), it is clear that V^j is injective and that its image is the set of Witt vectors whose Witt components (relative π) are 0 in positions 0 to $j-1$. By 3.5, the preimage of 0 under the map $W_{R,n+j}(A) \to W_{R,j}(A)$ is the same subset, and the map $W_{R,n+j}(A) \to W_{R,j}(A)$ is surjective.

Now consider the general case. Augment the diagram (4-4-1) by expressing each term of (4-4-1) as an equalizer as in 4.1. Here we use that $\mathfrak{m}$ is R-flat. It then follows from the principal case and the snake lemma that (4-4-1) is left exact.

It remains to prove that the map $W_{R,n+j}(A) \to W_{R,j}(A)$ is surjective. By induction, we can assume $n = 1$. By 4.1, for any $i \in \mathbb{N}$ we have

$$W_{R,i}(A) = W_{R_\mathfrak{m},i}(R_\mathfrak{m} \otimes_R A) \times_{W_{K_\mathfrak{m},i}(K_\mathfrak{m} \otimes_R A)} W_{R[1/\mathfrak{m}],i}(R[1/\mathfrak{m}] \otimes_R A).$$

Now let π denote a generator of the maximal ideal of $R_\mathfrak{m}$, and suppose two elements

$$y = (y_0, \ldots, y_j)_\pi \in W_{R_\mathfrak{m},j}(R_\mathfrak{m} \otimes_R A),$$
$$z = \langle z_0, \ldots, z_j \rangle \in (R[1/\mathfrak{m}] \otimes_R A)^{j+1} = W_{R[1/\mathfrak{m}],j}(R[1/\mathfrak{m}] \otimes_R A)$$

have the same image in $W_{K_\mathfrak{m},j}(K_\mathfrak{m} \otimes_R A)$. To lift the corresponding element of $W_j(A)$ to $W_{j+1}(A)$, we need to find elements

$$y_{j+1} \in R_\mathfrak{m} \otimes_R A \quad \text{and} \quad z_{j+1} \in R[1/\mathfrak{m}] \otimes_R A$$

such that in $K_\mathfrak{m} \otimes_R A$, we have

$$y_0^{q^{j+1}} + \cdots + \pi^{j+1} y_{j+1} = z_{j+1}. \tag{4-4-2}$$

So, choose an element $z_{j+1} \in A$ whose image under the surjection

$$A \longrightarrow A/(\mathfrak{m}A)^{j+1} = R_\mathfrak{m}/(\mathfrak{m}R_\mathfrak{m})^{j+1} \otimes_R A$$

agrees with the image of $y_0^{q^{j+1}} + \cdots + \pi^j y_j$. It follows that the element

$$y_0^{q^{j+1}} + \cdots + \pi^j y_j^q - 1 \otimes z_{j+1} \in R_\mathfrak{m} \otimes_R A$$

lies in $\pi^{j+1}(R_\mathfrak{m} \otimes_R A)$. It thus equals $\pi^{j+1} y_{j+1}$ for some element $y_{j+1} \in R_\mathfrak{m} \otimes_R A$. And so y_{j+1} and z_{j+1} satisfy (4-4-2). □

4.5. Corollary. *For any R-algebra A, we have*

$$\bigoplus_{i \in [0,n]} \mathfrak{m}^i \otimes_R A_{(i)} \xrightarrow{\sim} \mathrm{gr}_V W_{R,\mathfrak{m},n}(A), \tag{4-5-1}$$

where $A_{(i)}$ denotes A viewed as a $W_n(A)$-module via the ring map $w_i \colon W_n(A) \to A$.

4.6. *Reduced ghost components.* We can define infinitely many ghost components for Witt vectors of finite length n if we are willing to settle for answers modulo $\mathfrak{m}^{n+1}$.

First assume $\mathfrak{m}$ is generated by some element π. By examining the Witt polynomials (3-1-1), we can see that for any $i \geqslant 0$, the composition

$$W_{R,\mathfrak{m}}(A) \xrightarrow{w_i} A \longrightarrow A/\mathfrak{m}^{n+1}A$$

vanishes on $V^{n+1} W_{R,\mathfrak{m}}(A)$. It therefore factors through $W_{R,\mathfrak{m},n}(A)$, giving a map $\bar{w}_i$ from $W_{R,\mathfrak{m},n}(A)$ to $A/\mathfrak{m}^{n+1}A$.

When $\mathfrak{m}$ is not assumed to be principal, we define $\bar{w}_i$ by localizing at $\mathfrak{m}$:

$$W_{R,\mathfrak{m},n}(A) \to W_{R_\mathfrak{m},\mathfrak{m}R_\mathfrak{m},n}(R_\mathfrak{m} \otimes_R A) \xrightarrow{\bar{w}_i} (R_\mathfrak{m} \otimes_R A)/\mathfrak{m}^{n+1}(R_\mathfrak{m} \otimes_R A) = A/\mathfrak{m}^{n+1}A,$$

where the middle map is $\bar{w}_i$ as constructed above in the principal case. We call the composition

$$W_{R,\mathfrak{m},n}(A) \xrightarrow{\bar{w}_i} A/\mathfrak{m}^{n+1}A \tag{4-6-1}$$

the i-th *reduced ghost component* map.

5. Multiple-prime case

The purpose of this section is to give some results on reducing the family E (of 1.2) to simpler families. The first reduces from the case where E is arbitrary to the case where it is finite, and the second reduces from the case where it is finite to the case where it has a single element. We will often write $W_E = W_{R,E}$, $\Lambda_E = \Lambda_{R,E}$, and so on, for short.

5.1. Proposition. *The canonical maps*

$$\operatorname{colim}_{E'} \Lambda_{R,E'} \longrightarrow \Lambda_{R,E}, \tag{5-1-1}$$

$$\operatorname{colim}_{E'} \Lambda_{R,E',n'} \longrightarrow \Lambda_{R,E,n} \tag{5-1-2}$$

are isomorphisms. Here E' runs over the finite subfamilies of E, and n' is the restriction to E' of a given element $n \in \mathbb{N}^{(E)}$.

Proof. Consider (5-1-1) first. Since each map $\Lambda_{E'} \to \Lambda_E$ is an injection, (5-1-1) is an injection. Therefore, since Λ_E is freely generated as a Λ_E-ring by the element $e = \psi_0$, it is enough to show the sub-Ψ_E-ring $\operatorname{colim}_{E'} \Lambda_{E'}$ of Λ_E is a sub-Λ_E-ring. Since it is flat, we only need to check the Frobenius lift property. So, suppose $\mathfrak{m} \in E$. For any element x of the colimit, there is a finite family E'' such that $x \in \Lambda_{E''}$ and $\mathfrak{m} \in E''$. But $\Lambda_{E''}$ is a $\Lambda_{E''}$-ring. So we have $\psi_{\mathfrak{m}}(x) \equiv x^{q_{\mathfrak{m}}}$ modulo $\mathfrak{m}\Lambda_{E''}$, and hence modulo $\mathfrak{m}(\operatorname{colim}_{E'} \Lambda_{E'})$. Therefore the Frobenius lift property holds for the colimit ring.

Then (5-1-2) follows:

$$\begin{aligned}\Lambda_{E,n} &= (R[1/E] \otimes_R \Psi_{E,n}) \cap \Lambda_E = (\operatorname{colim}_{E'} R[1/E] \otimes_R \Psi_{E',n'}) \cap \operatorname{colim}_{E'} \Lambda_{E'} \\ &= \operatorname{colim}_{E'} \left((R[1/E] \otimes_R \Psi_{E',n'}) \cap \Lambda_{E'} \right) = \operatorname{colim}_{E'} \Lambda_{E',n'}. \qquad \square\end{aligned}$$

5.2. Corollary. *For any R-algebra A, the canonical maps*

$$W_{R,E}(A) \longrightarrow \lim_{E'} W_{R,E'}(A), \tag{5-2-1}$$

$$W_{R,E,n}(A) \longrightarrow \lim_{E'} W_{R,E',n'}(A) \tag{5-2-2}$$

are isomorphisms, where E', n, and n' are as in 5.1.

5.3. Proposition. *Let $E' \sqcup E''$ be a partition of E. Then the canonical maps*

$$\Lambda_{R,E'} \odot_R \Lambda_{R,E''} \longrightarrow \Lambda_{R,E}, \tag{5-3-1}$$

$$\Lambda_{R,E',n'} \odot_R \Lambda_{R,E'',n''} \longrightarrow \Lambda_{R,E,n} \tag{5-3-2}$$

are isomorphisms, where n' and n'' denote the restrictions to E' and E'' of a given element $n \in \mathbb{N}^{(E)}$.

Proof. It is enough to show each map becomes an isomorphism after base change to $R[1/E']$ and $R[1/E'']$. So, by (1-20-1), we can assume every element in either E' or E'' is the unit ideal.

In the second case, we have

$$\Lambda_{E'} \odot_R \Lambda_{E''} = \Lambda_{E'} \odot_R R[\mathbb{N}^{(E'')}] = \Lambda_{E'}[\mathbb{N}^{(E'')}] = \Lambda_E$$

The argument for (5-3-2) is the same, but we replace the generating set $\mathbb{N}^{(E'')}$ with $[0, n'']$.

Now suppose every element in E' is the unit ideal. Then a $\Lambda_{E'}$-ring is the same as a $\Psi_{E'}$-ring. So we have

$$\Lambda_{E'} \odot_R \Lambda_{E''} = \Lambda_{E''}[\mathbb{N}^{(E')}] = \Lambda_E.$$

For (5-3-2), replace $\mathbb{N}^{(E')}$ with $[0, n']$, as above. □

5.4. Corollary. *Let $E' \sqcup E''$ be a partition of E. Then for any R-algebra A, the canonical maps*

$$W_{R,E}(A) \longrightarrow W_{R,E''}\big(W_{R,E'}(A)\big), \tag{5-4-1}$$

$$W_{R,E,n}(A) \longrightarrow W_{R,E'',n''}\big(W_{R,E',n'}(A)\big) \tag{5-4-2}$$

are isomorphisms, where n, n', n'' are as in 5.3.

5.5. *Remark.* By the results above, it is safe to say that expressions such as

$$\Lambda_{\mathfrak{m}_1} \odot_R \cdots \odot_R \Lambda_{\mathfrak{m}_r} \quad \text{and} \quad W_{\mathfrak{m}_r} \circ \cdots \circ W_{\mathfrak{m}_1}(A) \tag{5-5-1}$$

are independent of the ordering of the $\mathfrak{m}_i$, assuming the $\mathfrak{m}_i$ are pairwise coprime. (Note that it is not generally true that $P \odot P' \cong P' \odot P$ for plethories P and P'. See [Borger and Wieland 2005, 2.8].)

If we ask that the expressions in (5-5-1) be independent only up to isomorphism, then it is not even necessary that the $\mathfrak{m}_\alpha \in E$ be pairwise coprime 1.2. But invariance up to isomorphism is not a such a useful property, and most of the time coprimality really is necessary. For example, we could look at rings with more than one Frobenius lift at a single maximal ideal, but we would not be able to reduce to the case of a single Frobenius lift. Indeed, if E consists of a single maximal ideal $\mathfrak{m}$, the two endomorphisms $\psi_{WW(A)}$ and $W(\psi_{W(A)})$ of $WW(A)$ commute, and the first is clearly a Frobenius lift, but the second is generally not. Therefore $WW(A)$ cannot be the cofree ring with two commuting Frobenius lifts at $\mathfrak{m}$.

In fact, I believe this is the only place where we use the coprimality assumption directly. The rest of our results depend on it only through 5.3. Although I know of no applications, it would be interesting to know whether the abstract setup of this paper, and then the main results, hold when we allow more than one Frobenius lift at each maximal ideal.

6. Basic affine properties

This section provides some basic results about the commutative algebra of Witt vectors. They are just the ones needed to be able to prove the main theorems in sections 8 and 9 and to set up the global theory in the companion paper [Borger 2010]. There are other basic results that could have been included here, but which I have put off to the other paper, where they will be proved for all algebraic spaces.

We continue with the notation of 1.2. Fix an element $n \in \mathbb{N}^{(E)}$. We will often write $W_n = W_{E,n} = W_{R,E,n}$ and so on, for short. By 5.2, we may assume that E agrees with the support of n, and in particular that it is finite.

6.1. Proposition. *Let R' be an E-flat R-algebra such that the structure map $R \to R'$ is a ring epimorphism (as in 1.20). Then the composition*

$$R' \otimes_R W_{R,E,n}(A) \xrightarrow{(2\text{-}6\text{-}3)} W_{R,E,n}(R' \otimes_R A) \xrightarrow[\sim]{(2\text{-}6\text{-}2)^{-1}} W_{R',E',n}(R' \otimes_R A)$$

is an isomorphism, where E' is as in 1.20.

Proof. We may assume by 5.4 that E consists of a single ideal $\mathfrak{m}$. Using 4.1 and the flatness of R' over R, we are reduced to showing that the functors $W_{R[1/\mathfrak{m}],\mathfrak{m},n}$, $W_{R_\mathfrak{m},\mathfrak{m},n}$, and $W_{K_\mathfrak{m},\mathfrak{m},n}$ commute with the functor $R' \otimes_R -$. Therefore we may assume that the ideal $\mathfrak{m}$ is principal.

Write $W_n = W_{R,\mathfrak{m},n}$. The result is clear for $n = 0$, because W_0 is the identity functor. So assume $n \geqslant 1$. By 4.4, we have the map of exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R' \otimes_R \mathfrak{m} \otimes_R W_{n-1}(A) & \xrightarrow{\mathrm{id}_{R'} \otimes V^1} & R' \otimes_R W_n(A) & \longrightarrow & R' \otimes_R A & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & \mathfrak{m} \otimes_R W_{n-1}(R' \otimes_R A) & \xrightarrow{V^1} & W_n(R' \otimes_R A) & \longrightarrow & R' \otimes_R A & \longrightarrow & 0
\end{array}$$

where the vertical maps are given by (2-6-3). By induction the leftmost vertical arrow is an isomorphism. Therefore the inner one is, too. □

6.2. Proposition. *For any ideal I in an R-algebra A, let $W_{R,E,n}(I)$ denote the kernel of the canonical map $W_{R,E,n}(A) \to W_{R,E,n}(A/I)$. Then we have*

$$W_{R,E,n}(I) W_{R,E,n}(J) \subseteq W_{R,E,n}(IJ)$$

for any ideals I, J in A.

Proof. We first show that we may assume E consists of a single ideal $\mathfrak{m}$. In doing this, it will be convenient to prove an equivalent form of the statement: if $IJ \subseteq K$, where K is an ideal in A, then $W_n(I)W_n(J) \subseteq W_n(K)$. Suppose $E = E' \sqcup \{\mathfrak{m}\}$. Let n' be the restriction of n to E. Let $I' = W_{E',n'}(I)$, $J' = W_{E',n'}(J)$, and $K' = W_{E',n'}(K)$. By 5.4, we have $W_{E,n} = W_{\mathfrak{m},n_\mathfrak{m}} \circ W_{E',n'}$, and

hence $W_{E,n}(I) = W_{\mathfrak{m},n_{\mathfrak{m}}}(I')$ and so on. By induction, we have $I'J' \subseteq K'$, and then applying the result in the single-ideal case gives

$$W_{E,n}(I)W_{E,n}(J) = W_{\mathfrak{m},n_{\mathfrak{m}}}(I')W_{\mathfrak{m},n_{\mathfrak{m}}}(J') = W_{\mathfrak{m},n_{\mathfrak{m}}}(K') = W_{E,n}(K).$$

So we will assume $E = \{\mathfrak{m}\}$ and drop E from the notation.

By 6.1, the statement is Zariski local on R, and so we may assume the ideal $\mathfrak{m}$ is generated by some element π. We will work with Witt components relative to π.

We need to show that for any elements $x = (x_0, \dots, x_n)_\pi \in W_n(I)$ and $y = (y_0, \dots, y_n)_\pi \in W_n(J)$, the product xy is in $W_n(IJ)$. So it is sufficient to show this in the universal case, where A is the free polynomial algebra $R[x_0, y_0, \dots, x_n, y_n]$, I is the ideal $(x_0, \dots, x_n)$, and J is the ideal $(y_0, \dots, y_n)$.

Consider the commutative diagram

$$\begin{array}{ccc} W_n(A) & \xrightarrow{w_{\leqslant n}} & A^{[0,n]} \\ \downarrow & & \downarrow \\ W_n(A/IJ) & \xrightarrow{w_{\leqslant n}} & (A/IJ)^{[0,n]}. \end{array}$$

We want to show that the image of xy in $W_n(A/IJ)$ is zero. Since A/IJ is flat (even free) over R, the lower map $w_{\leqslant n}$ is injective, and so it is enough to show the image of xy in $(A/IJ)^{[0,n]}$ is zero. But by the naturality of the ghost map, we have $w_{\leqslant n}(x) \in I^{[0,n]}$ and $w_{\leqslant n}(y) \in J^{[0,n]}$. Therefore $w_{\leqslant n}(xy)$ lies in $(IJ)^{[0,n]}$, which maps to zero in $(A/IJ)^{[0,n]}$. □

6.3. *Remark.* Although the proof of 6.2 given above uses some properties specific to Witt vector functors, the result is true for any representable ring-valued functor. See [Borger and Wieland 2005, 5.5].

6.4. Corollary. *If I is an ideal in an R-algebra A and $I^m = 0$, then $W_{R,E,n}(I)^m = 0$.*

6.5. Proposition. *Let $\varphi\colon A \to B$ be a map of R-algebras. If it is surjective, then so is the map $W_{R,E,n}(\varphi)\colon W_{R,E,n}(A) \to W_{R,E,n}(B)$.*

Proof. By 5.4, we may assume E consists of one ideal $\mathfrak{m}$. Since surjectivity can be checked Zariski locally on R, it is enough by 6.1 to assume $\mathfrak{m}$ is principal. Then using the Witt components, we can identify the set map underlying $W_{R,E,n}(\varphi)$ with the map $\varphi^{[0,n]}\colon A^{[0,n]} \to B^{[0,n]}$, which is clearly surjective. □

6.6. Corollary. *If $\varphi\colon A \to B$ is surjective, then*

$$W_{R,E,n}(A \times_B A) \underset{W_n(\mathrm{pr}_2)}{\overset{W_n(\mathrm{pr}_1)}{\rightrightarrows}} W_{R,E,n}(A) \xrightarrow{W_n(\varphi)} W_{R,E,n}(B)$$

is a coequalizer diagram.

Proof. The functor W_n is representable, and hence commutes with limits. (See 2.4.) Therefore $W_n(A \times_B A)$ agrees with $W_n(A) \times_{W_n(B)} W_n(A)$, which is an equivalence relation on $W_n(A)$, the quotient by which is the image of $W_n(\varphi)$. By 6.5, this is all of $W_n(B)$. □

6.7. *Remark.* This result is particularly appealing when A is E-flat and B is not. Then we can describe $W_n(B)$ in terms of $W_n(A)$ and $W_n(A \times_B A)$, which are directly accessible because A and $A \times_B A$ are E-flat.

6.8. Proposition. *Suppose E consists of one ideal $\mathfrak{m}$, and let A be an R-algebra. For any $i \geqslant 0$, the map* $\operatorname{Spec}(\mathrm{id} \otimes \bar{w}_i)$ *of schemes induced by the ring map*

$$\mathrm{id} \otimes \bar{w}_i \colon R/\mathfrak{m} \otimes_R W_{R,E,n}(A) \longrightarrow R/\mathfrak{m} \otimes_R A/\mathfrak{m}^{n+1}$$

is a universal homeomorphism. For $i = 0$, it is a closed immersion defined by a square-zero ideal.

Proof. Write $W_n = W_{R,E,n}$ and so on. Consider the diagram

$$\begin{array}{ccc} R/\mathfrak{m} \otimes_R W_n(A) & \xrightarrow{\mathrm{id}\otimes \bar{w}_i} & R/\mathfrak{m} \otimes_R A/\mathfrak{m}^{n+1}A \\ \Big\downarrow{\scriptstyle \mathrm{id}\otimes w_0} & & {\scriptstyle r\otimes a \mapsto ra}\Big\downarrow{\scriptstyle \sim} \\ A/\mathfrak{m}A & \xrightarrow{x \mapsto x^{q^i}} & A/\mathfrak{m}A. \end{array}$$

To show it commutes, it is enough to assume $\mathfrak{m}$ is principal, generated by π. Then commutativity follows from the obvious congruence

$$w_i(a) = a_0^{q^i} + \pi a_1^{q^{i-1}} + \cdots + \pi^i a_i \equiv a_0^{q^i} \bmod \mathfrak{m}A,$$

for any element $a = (a_0, a_1, \dots)_\pi \in W(A)$.

Therefore, $\mathrm{id} \otimes \bar{w}_i$ is the composition of a map whose kernel is a nil ideal and a power of the Frobenius map. The scheme maps induced by both of these are universal homeomorphisms.

Now let us show that $\mathrm{id} \otimes w_0$ (which equals $\mathrm{id} \otimes \bar{w}_0$) is a surjection with square-zero kernel. The map $\mathrm{id} \otimes w_0$ is surjective by 1.21 (or 4.4). So let us show the square of its kernel is zero. By 4.4, the kernel of the map $W_n(A) \to R/\mathfrak{m} \otimes_R A$ is the ideal $V^1 W_n(A) + \mathfrak{m} W_n(A)$. Hence it is enough to show $\left(V^1 W_n(A)\right)^2 \subseteq \mathfrak{m} W_n(A)$. This follows from (4-2-6). □

6.9. Proposition. *Let $(B_i)_{i \in I}$ be a family of A-algebras such that the induced map $\coprod_i \operatorname{Spec} B_i \to \operatorname{Spec} A$ is surjective. Then the induced map*

$$\coprod_i \operatorname{Spec} W_{R,E,n}(B_i) \to \operatorname{Spec} W_{R,E,n}(A)$$

is surjective.

Proof. By 5.4, it is enough to assume E consists of one ideal $\mathfrak{m}$. Further, it is enough to show surjectivity after base change to $R[1/\mathfrak{m}]$ and to $R/\mathfrak{m}$. For $R[1/\mathfrak{m}]$, it follows from 6.1 and the equality $W_n(C) = C^{[0,n]}$, when $\mathfrak{m}$ is the unit ideal. Now consider base change to $R/\mathfrak{m}$. By 6.8, the ring $W_n(A)/\mathfrak{m}W_n(A)$ is a nilpotent extension of $A/\mathfrak{m}A$, and likewise for each B_i, and so we are reduced to showing that

$$\coprod_i \operatorname{Spec} B_i/\mathfrak{m}B_i \to \operatorname{Spec} A/\mathfrak{m}A$$

is surjective. This is true since base change distributes over disjoint unions and preserves surjectivity. □

6.10. Proposition. *The R-algebra $\Lambda_{R,E,n}$ is finitely presented, and the functor $W_{R,E,n}$ preserves filtered colimits of R-algebras.*

Proof. Since $W_{R,E,n}$ is represented by $\Lambda_{R,E,n}$, the two statements to be proved are equivalent. By 5.4, we may assume E consists of a single ideal $\mathfrak{m}$. By [EGA 6, 2.7.1], the first statement can be verified fpqc locally on R, and in particular after base change to $R[1/\mathfrak{m}]$ and to $R_{\mathfrak{m}}$. Therefore by (2-6-1), we can assume $\mathfrak{m}$ is generated by a single element π. But by 3.3, the R-algebra $\Lambda_{R,E,n}$ is generated by the finite set $\theta_{\pi,0}, \ldots, \theta_{\pi,n}$. □

7. Some general descent

The purpose of this section is to record some facts about descent of étale algebras which we will use to prove our main result, Theorem 9.2. The results mention nothing about Witt vectors or anything else in this paper. So it would be reasonable to skip this section and refer back to it only as needed.

More precisely, we do the following. First, we set up some language and notation for descent, essentially repeating parts of Grothendieck's TDTE I [1966]. (It could not be otherwise.) Second, we prove an abstract result (7.10) relating gluing data and descent data for certain simple gluing constructions. Third, we recall Grothendieck's theorem (7.11) on integral descent of étale maps. Finally, we prove 7.12, which provides the plan of the proof of 9.2. Aside from the language of descent, only these three results will be used outside this section.

Language

7.1. *Fibered categories.* Let C be a category with fibered products. Let E be a category fibered over C. (See [Grothendieck 1966, A.1.1] or [SGA 1, VI.6.1].) For any object S of C, let E_S denote the fiber of E over S. Let us say that a map $q\colon T \to S$ in C is an E-equivalence if $q^*\colon \mathsf{E}_S \to \mathsf{E}_T$ is an equivalence of categories, and let us say that q is a *universal* E-*equivalence* if for any map $S' \to S$ in C, the base change $q'\colon S' \times_S T \to S'$ is an E-equivalence.

For the applications in the next section, the reader can take

$$\begin{aligned} &\mathsf{C} = \text{the category of affine schemes,}\\ &\mathsf{E} = \text{the fibered category over } \mathsf{C} \text{ where } \mathsf{E}_S \text{ is the category of affine}\\ &\qquad \text{étale } S\text{-schemes and the functors } q^* \text{ are given by base change.} \end{aligned} \tag{7-1-1}$$

Then any closed immersion defined by a nil ideal is a universal E-equivalence [EGA 8, 18.1.2].

7.2. *Composition notation.* Let S be an object of C, and let $\mathsf{C}_{S\times S}$ denote the category of objects over $S \times S$. That is, an object of $\mathsf{C}_{S\times S}$ is a pair (T, π_T), where T is an object of C and π_T is a map $T \to S \times S$, called its structure map; a morphism is a morphism in C commuting with the maps to $S \times S$. For such an object, let $\pi_{T,1}, \pi_{T,2}$ denote the composition of the structure map $T \to S \times S$ with the projections $\mathrm{pr}_1, \mathrm{pr}_2 \colon S \times S \to S$. ($\pi_{T,1}$ is the "source" and $\pi_{T,2}$ is the "target".) We will often abusively leave π_T implicit and say that T is an object of C.

Let 1_S denote the object (S, Δ) of $\mathsf{C}_{S\times S}$, where $\Delta : S \to S \times S$ is the diagonal map.

Given two objects $T, U \in \mathsf{C}_{S\times S}$, define $TU \in \mathsf{C}_{S\times S}$ as follows. As an object of C, it is the fibered product

$$\begin{array}{ccc} TU & \xrightarrow{\mathrm{pr}_1} & T \\ {\scriptstyle \mathrm{pr}_2}\downarrow & & \downarrow{\scriptstyle \pi_{T,2}} \\ U & \xrightarrow{\pi_{T,1}} & S. \end{array} \tag{7-2-1}$$

We give TU the structure of an object of $\mathsf{C}_{S\times S}$ with the map

$$TU = T \times_S U \xrightarrow{(\pi_{T,1}\circ \mathrm{pr}_1, \pi_{U,2}\circ \mathrm{pr}_2)} S \times S. \tag{7-2-2}$$

7.3. *Category objects and equivalence relations.* A category object over S is an object $R \in \mathsf{C}_{S\times S}$ together with maps

$$\begin{aligned} e_R &\colon 1_S \to R,\\ c_R &\colon RR \to R \end{aligned} \tag{7-3-1}$$

in $\mathsf{C}_{S\times S}$ (called identity and composition) satisfying the usual identity and associativity axioms in the definition of a category. A morphism $f \colon R \to R'$ of such category objects is defined to be a morphism in $\mathsf{C}_{S\times S}$ satisfying the functor axioms, that is, such that

$$f \circ e_R = e_R \circ f \quad \text{and} \quad c_{R'} \circ ff = f \circ c_R,$$

where ff denotes the map $RR \to R'R'$ induced by f.

A category-object structure on a subobject $R \subseteq S \times S$ is a property of R in that when it exists, it is unique. One might say that R is a reflexive transitive relation on S. We say R is an equivalence relation on S if, in addition, the endomorphism $(\mathrm{pr}_2, \mathrm{pr}_1)$ of $S \times S$ that switches the two factors restricts to a map

$$s\colon R \to R$$

(which is of course unique when it exists).

7.4. *Pre-actions (gluing data).* Let T be an object of $\mathsf{C}_{S\times S}$. A *pre-action* of T on an object $X \in \mathsf{E}_S$ is defined to be an isomorphism

$$\varphi\colon \pi_{T,2}^*(X) \xrightarrow{\sim} \pi_{T,1}^*(X) \tag{7-4-1}$$

in E_T. A pre-action is also called a gluing datum on X relative to the pair of maps $(\pi_{T,1}, \pi_{T,2})$. (Actually, Grothendieck [1966, A.1.4] calls φ^{-1} the gluing datum.) Let

$$\mathrm{PreAct}(T, X)$$

denote the set of pre-actions of T on X. Any map $T \to T'$ in $\mathsf{C}_{S\times S}$ naturally induces a map

$$\mathrm{PreAct}(T', X) \to \mathrm{PreAct}(T, X).$$

If $f\colon X \to X'$ is a morphism in E_S between objects X, X' with pre-actions φ, φ', then we say f is *T-equivariant* if the diagram

$$\begin{array}{ccc} \pi_{T,2}^*(X) & \xrightarrow{\pi_{T,2}^*(f)} & \pi_{T,2}^*(X') \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi'} \\ \pi_{T,1}^*(X) & \xrightarrow{\pi_{T,1}^*(f)} & \pi_{T,1}^*(X') \end{array}$$

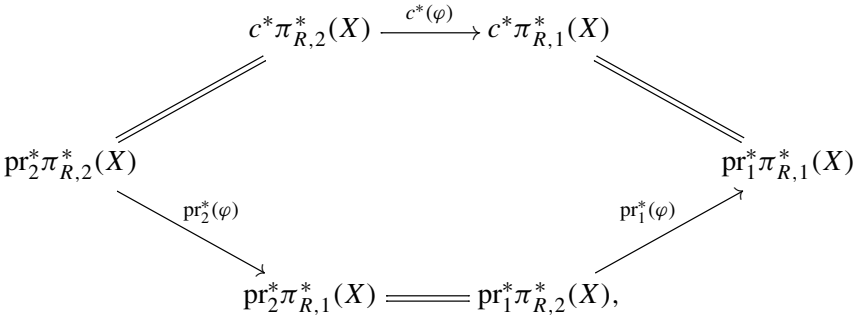
commutes.

In this way, the objects of E_S equipped with a pre-action of T form a category.

7.5. *Actions.* Now let R be a category object over S. An *action* of R on X is defined to be a pre-action φ of R on X such that the diagram

$$\begin{array}{ccc} e^*\pi_{R,2}^*(X) & \xrightarrow{e^*(\varphi)} & e^*\pi_{R,1}^*(X) \\ & \searrow \quad \swarrow & \\ & \mathrm{id}_S^*(X) & \end{array}$$

and the diagram



commute. Here, pr_1 and pr_2 denote the projections $RR \to R$ onto the first and second factors, and the morphisms represented by equality signs are the isomorphisms induced by the canonical structure maps $(g \circ f)^* \xrightarrow{\sim} f^* \circ g^*$ (denoted by $c_{f,g}$ in [Grothendieck 1966, A.1.1(ii)]) of the fibered category E corresponding to the equalities

$$\pi_{R,2} \circ e = \mathrm{id}_S = \pi_{R,1} \circ e$$

and

$$\pi_{R,2} \circ c = \pi_{R,2} \circ \mathrm{pr}_2,$$
$$\pi_{R,1} \circ \mathrm{pr}_2 = \pi_{R,2} \circ \mathrm{pr}_1,$$
$$\pi_{R,1} \circ c = \pi_{R,1} \circ \mathrm{pr}_1.$$

We will often use the following more succinct, if slightly abusive, expressions of the commutativity of the diagrams above:

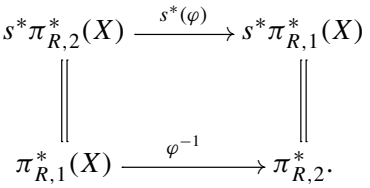
$$e^*(\varphi) = \mathrm{id}_X, \quad c^*(\varphi) = (\mathrm{pr}_1^*\varphi) \circ (\mathrm{pr}_2^*\varphi). \tag{7-5-1}$$

Let $\mathrm{Act}(R, X)$ denote the set of actions of R on X. A morphism $R \to R'$ of category objects induces a map

$$\mathrm{Act}(R', X) \longrightarrow \mathrm{Act}(R, X)$$

in the obvious way.

Last, note that if R is an equivalence relation, the diagram



commutes. This follows immediately from (7-5-1). The abbreviated version is

$$s^*(\varphi) = \varphi^{-1}. \tag{7-5-2}$$

7.6. *Descent data.* Let $q\colon S' \to S$ be a map in C, and put

$$R(S'/S) = S' \times_S S'.$$

View $R(S'/S)$ as an object in $\mathsf{C}_{S'\times S'}$ by taking $\pi_{R(S'/S)}$ to be the evident monomorphism

$$R(S'/S) = S' \times_S S' \longrightarrow S' \times S'$$

Then $R(S'/S)$ is an equivalence relation on S'. An action φ of $R(S'/S)$ on an object X' of $\mathsf{E}_{S'}$ is also called a descent datum on X' from S' to S. (Again, it is actually φ^{-1} that is called the descent datum in [Grothendieck 1966].) We might call $R(S'/S)$ the descent, or Galois, groupoid of the map $q\colon S' \to S$.

Because the two compositions $R(S'/S) = S' \times_S S' \rightrightarrows S' \to S$ are equal, for any object $X \in \mathsf{E}_S$, the object $q^*(X)$ of $\mathsf{E}_{S'}$ has a canonical pre-action of $R(S'/S)$, and it is easy to check that this is an action. We say that q is a *descent map* for the fibered category E if the functor from E_S to the category of objects of $\mathsf{E}_{S'}$ with an R-action is fully faithful. We say it is an *effective descent map* if it is an equivalence.

7.7. *When gluing data is descent data.* Now suppose we have a diagram

$$S'' \rightrightarrows S' \longrightarrow S \tag{7-7-1}$$

in C such that the two compositions $S'' \rightrightarrows S$ are equal. The universal property of products gives a map

$$S'' \longrightarrow S' \times_S S' = R(S'/S).$$

For any object $X' \in \mathsf{E}_{S'}$, this map induces a function

$$\mathrm{Act}(R(S'/S), X') \longrightarrow \mathrm{PreAct}(S'', X').$$

Let us say that *gluing data on X' is descent data* relative to the diagram (7-7-1) when this map is a bijection.

Gluing two objects

Here we spell out in (perhaps excessive) detail some basic facts about equivalence relations on disjoint unions that are E-trivial, but not necessarily trivial, on each factor.

From now on, let C denote the category of affine schemes, schemes, or algebraic spaces. (We only need some weak hypotheses on coproducts in C, but let us not bother to determine which ones we need.)

7.8. *Equivalence relations on a disjoint union.* Suppose S is a coproduct $S_a + S_b$ of two objects $S_a, S_b \in \mathsf{C}$. (We use the symbols a, b to index the summands only to emphasize their distinction from the symbols $1, 2$ that index the factors in the

product $S \times S$.) Let R be an equivalence relation on S, and let R_{ij} denote $R \times_{S\times S} (S_i \times S_j)$, for any $i, j \in \{a, b\}$. Let $\pi_{R_{ij},1}$ denote the evident composition

$$R_{ij} = R \times_{S\times S} (S_i \times S_j) \xrightarrow{\mathrm{pr}_1} S_i$$

and $\pi_{R_{ij},2}$ the analogous map $R_{ij} \to S_j$. We will sometimes view R_{ij} as an object of $\mathsf{C}_{S\times S}$ using the induced map $R_{ij} \to S_i \times S_j \to S \times S$.

Let $e_i \colon S_i \to R_{ii}$ and $c_{ijk} \colon R_{ij}R_{jk} \to R_{ik}$ and $s_{ij} \colon R_{ij} \to R_{ji}$ denote the evident restrictions of e and c and s.

7.9. *Actions over a disjoint union.* For any object X over S, write $X_a = S_a \times_S X$ and $X_b = S_b \times_S X$.

For any pre-action

$$\varphi \colon \pi_{R,2}^* X \longrightarrow \pi_{R,1}^* X, \tag{7-9-1}$$

of R on X, let us write φ_{ij} for the restriction of φ to R_{ij}. In order for this pre-action to be an action, it is necessary and sufficient that for all $i, j, k \in \{a, b\}$ we have

$$e_i^*(\varphi_{ii}) = \mathrm{id}_{X_i}, \tag{7-9-2}$$

$$c_{ijk}^*(\varphi_{ik}) = \mathrm{pr}_1^*(\varphi_{ij}) \circ \mathrm{pr}_2^*(\varphi_{jk}). \tag{7-9-3}$$

This is just a restatement of (7-5-1), summand by summand. In that case, (7-5-2) becomes

$$s_{ij}^*(\varphi_{ji}) = \varphi_{ij}^{-1}. \tag{7-9-4}$$

7.10. Proposition. *Let R be an equivalence relation on $S = S_a + S_b$ such that for $i = a, b$, the map $e_i \colon S_i \to R_{ii}$ is a universal* E*-equivalence. Then for any object $X \in \mathsf{E}_S$, the map*

$$\mathrm{Act}(R, X) \xrightarrow{\varphi \mapsto \varphi_{ba}} \mathrm{PreAct}(R_{ba}, X)$$

is a bijection.

Proof. Let us first show injectivity. Let φ and φ' be actions of R on X such that $\varphi_{ba} = \varphi'_{ba}$. We need to show that this implies $\varphi_{ij} = \varphi'_{ij}$ for all $i, j \in \{a, b\}$. Consider each case separately. For $ij = ba$, it is true by assumption. When $ij = ab$, (7-9-4) and the given equality $\varphi_{ba} = \varphi'_{ba}$ imply

$$\varphi_{ab} = s_{ba}^*(\varphi_{ab})^{-1} = s_{ba}^*(\varphi'_{ab})^{-1} = \varphi'_{ab}.$$

When $i = j$, since e_i is an E-equivalence, it is enough to show $e_i^*(\varphi_{ii}) = e_i^*(\varphi'_{ii})$. But by (7-9-2), we have

$$e_i^*(\varphi_{ii}) = \mathrm{id}_{X_i} = e_i^*(\varphi'_{ii}).$$

Therefore $\varphi = \varphi'$, which proves injectivity.

Now consider surjectivity. Let φ_{ba} be a pre-action of R_{ba} on X. Define

$$\varphi_{ab} = s_{ab}^*(\varphi_{ba})^{-1} \tag{7-10-1}$$

and for $i = a, b$ define φ_{ii} to be the map such that

$$e_i^*(\varphi_{ii}) = \mathrm{id}_{X_i}, \tag{7-10-2}$$

which exists and is unique because e_i is an E-equivalence. We need to check that the pre-action $\varphi = \varphi_{aa} + \varphi_{ab} + \varphi_{ba} + \varphi_{bb}$ of R on X is actually an action. To do this, we will verify the relations (7-9-2) and (7-9-3).

The identity axiom (7-9-2) holds because it is the defining property (7-10-2) of φ_{ii}.

Now consider the associativity axiom (7-9-3) for the various possibilities for ijk. Since $i, j, k \in \{a, b\}$, two of i, j, k must be equal.

If $i = j$, the composition f

$$R_{jk} \xrightarrow[\sim]{\mathrm{pr}_2^{-1}} S_{jj}R_{jk} \xrightarrow{e_j \times \mathrm{id}} R_{jj}R_{jk}$$

is an E-equivalence, because it is a base change of the universal E-equivalence e_j. Therefore it is enough to show

$$f^*c_{jjk}^*(\varphi_{jk}) = f^*\mathrm{pr}_1^*(\varphi_{jj}) \circ f^*\mathrm{pr}_2^*(\varphi_{jk}). \tag{7-10-3}$$

By the equality $\mathrm{pr}_1 \circ f = e_j \circ \pi_{R_{jk},1}$ and (7-10-2), we have

$$f^*\mathrm{pr}_1^*(\varphi_{jj}) = \pi_{R_{jk},1}^* e_j^*(\varphi_{jj}) = \pi_{R_{jk},1}^*(\mathrm{id}_{X_j}) = \mathrm{id}.$$

On the other hand, by $c_{jjk} \circ f = \mathrm{id}_{R_{jk}} = \mathrm{pr}_2 \circ f$, we have $f^*c_{jjk}^*(\varphi_{jk}) = f^*\mathrm{pr}_2^*(\varphi_{jk})$. Equation (7-10-3) then follows.

The case $j = k$ is similar to the case $i = j$. (Or apply s to the case $i = j$.)

Last, suppose $i = k$. The following diagram is easily checked to be cartesian:

$$\begin{array}{ccc} R_{ij} & \xrightarrow{(\mathrm{id}_{R_{ij}}, s_{ij})} & R_{ij}R_{ji} \\ {\scriptstyle \pi_{R_{ij},1}}\downarrow & & \downarrow{\scriptstyle c_{iji}} \\ S_i & \xrightarrow{e_i} & R_{ii}. \end{array} \tag{7-10-4}$$

(This is just another expression of the existence and uniqueness of inverses in a groupoid.) Since e_i is a universal E-equivalence, $(\mathrm{id}_{R_{ij}}, s_{ij})$ is an E-equivalence. So it is enough to show axiom (7-9-3) after applying $(\mathrm{id}_{R_{ij}}, s_{ij})^*$, that is, to show

$$(\mathrm{id}_{R_{ij}}, s_{ij})^*c_{iji}^*(\varphi_{ii}) = (\mathrm{id}_{R_{ij}}, s_{ij})^*\mathrm{pr}_1^*(\varphi_{ij}) \circ (\mathrm{id}_{R_{ij}}, s_{ij})^*\mathrm{pr}_2^*(\varphi_{ji}). \tag{7-10-5}$$

By the commutativity of (7-10-4) and (7-10-2), we have

$$(\mathrm{id}_{R_{ij}}, s_{ij})^* c_{iji}^*(\varphi_{ii}) = \pi_{R_{ij},1}^* e_i^*(\varphi_{ii}) = \pi_{R_{ij},1}^*(\mathrm{id}_{X_i}) = \mathrm{id}.$$

Combining this with the equation $\varphi_{ji} = s_{ji}^*(\varphi_{ij})^{-1}$, (7-10-5) reduces to

$$(\mathrm{id}_{R_{ij}}, s_{ij})^* \mathrm{pr}_1^*(\varphi_{ij}) = (\mathrm{id}_{R_{ij}}, s_{ij})^* \mathrm{pr}_2^* s_{ji}^*(\varphi_{ij}).$$

But this holds because we have

$$\mathrm{pr}_1 \circ (\mathrm{id}_{R_{ij}}, s_{ij}) = \mathrm{id}_{R_{ij}} = s_{ji} \circ s_{ij} = s_{ji} \circ \mathrm{pr}_2 \circ (\mathrm{id}_{R_{ij}}, s_{ij}).$$

Therefore the equations in (7-9-3) hold for all i, j, k, and so the pre-action is an action. □

Grothendieck's theorem

Recall that a map $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ of affine schemes is said to be integral if the corresponding ring map $A \to B$ is integral (and not necessarily injective).

7.11. Theorem. *Every surjective integral map $Y \to X$ of affine schemes is an effective descent map for the fibered category* E *over* C *of* (7-1-1).

This theorem is proven in [SGA 1, IX 4.7] up to two details. First, the argument given there covers only morphisms $Y \to X$ which are finite and of finite presentation; and second, the statement there has no affineness in the assumptions or in the conclusion. The first point can be handled by a standard limiting argument (or one can apply [Rydh 2010, Theorem 5.17 plus Remark 2.5(1b)]). The second point can be handled with Chevalley's theorem; the form most convenient here would the final one [Rydh 2009, Theorem 8.1], which is free of noetherianness, separatedness, finiteness, and scheme-theoretic assumptions.

Gluing and descent of étale algebras

7.12. Proposition. *Consider a diagram of rings*

$$\begin{array}{ccccc} B & \xrightarrow{d} & B' & \overset{h_1}{\underset{h_2}{\rightrightarrows}} & B'' \\ {\scriptstyle e}\uparrow & & {\scriptstyle e'}\uparrow & & \uparrow{\scriptstyle e''} \\ A & \xrightarrow[f]{} & A' & \overset{g_1}{\underset{g_2}{\rightrightarrows}} & A'' \end{array} \tag{7-12-1}$$

such that $h_i \circ e' = e'' \circ g_i$, for $i = 1, 2$. Also assume that

(a) *the two parallel right-hand squares are cocartesian*,

(b) *both rows are equalizer diagrams*,

(c) *relative to the lower row, gluing data on any étale A'-algebra is descent data*,

(d) *f satisfies effective descent for the fibered category of étale algebras, and*

(e) *e' is étale.*

Then e is étale and the left-hand square is cocartesian.

Note that when we use the language of descent in the category of rings (as in (c) and (d)), we understand that it refers to the corresponding statements in the opposite category.

Proof. Property (a) equips the étale A'-algebra B' with gluing data φ relative to (g_1, g_2). Indeed, take φ to be the composition

$$A'' \otimes_{g_1, A'} B' \xrightarrow{\sim} B'' \xrightarrow{\sim} A'' \otimes_{g_2, A'} B'.$$

By property (c), this gluing data comes from unique descent data relative to f. Therefore by (d) and (e), the A'-algebra B' descends to an étale A-algebra C.

Now apply the functor $C \otimes_A -$ to the lower row of diagram (7-12-1). By (a) and the definition of descent, the result can be identified with the sequence

$$C \longrightarrow B' \underset{h_2}{\overset{h_1}{\rightrightarrows}} B''.$$

This sequence is also an equalizer diagram, because the lower row of (7-12-1) is an equalizer diagram, by (b), and because C is étale over A and hence flat. Again by (b), the upper row of (7-12-1) is an equalizer diagram, and so we have $C = B$. Therefore, B is an étale A-algebra and the left-hand square is cocartesian. □

8. Ghost descent in the single-prime case

We return to the notation of 1.2. Suppose E consists of a single maximal ideal $\mathfrak{m}$, and fix an integer $n \geqslant 1$. Write $W_n = W_{R,\mathfrak{m},n}$, and so on. Let A be an R-algebra, and let α_n denote the map

$$W_n(A) \xrightarrow{\alpha_n} W_{n-1}(A) \times A \tag{8-0-2}$$

given by the canonical projection on the factor $W_{n-1}(A)$ and the n-th ghost component w_n on the factor A. Let $I_n(A)$ denote the kernel of α_n. For example, if $\mathfrak{m}$ is generated by π, then in terms of the Witt components, we have

$$I_n(A) = \{(0, \dots, 0, a)_\pi \in A^{[0,n]} \mid \pi^n a = 0\}. \tag{8-0-3}$$

8.1. Proposition. (a) *α_n is an integral ring homomorphism.*

(b) *The kernel $I_n(A)$ of α_n is a square-zero ideal.*

(c) *If A is $\mathfrak{m}$-flat, then α_n is injective.*

(d) *The diagram*

$$\begin{array}{ccc} W_{n-1}(A) & \xrightarrow{\bar{w}_n} & A/\mathfrak{m}^n A \\ \uparrow\uparrow & & \uparrow\uparrow \\ W_n(A) & \xrightarrow{w_n} & A, \end{array}$$

where the vertical maps are the canonical ones, is cocartesian.

(e) *View A as a $W_n(A)$-algebra by the map $w_n\colon W_n(A) \to A$. Then every element in the kernel of the multiplication map $A \otimes_{W_n(A)} A \longrightarrow A$ is nilpotent.*

(f) *In the diagram*

$$W_n(A) \xrightarrow{\alpha_n} W_{n-1}(A) \times A \underset{\overline{\mathrm{pr}}_2}{\overset{\bar{w}_n \circ \mathrm{pr}_1}{\rightrightarrows}} A/\mathfrak{m}^n A, \tag{8-1-1}$$

where $\overline{\mathrm{pr}}_2$ denotes the reduction of pr_2 modulo $\mathfrak{m}^n$, the image of α_n agrees with the equalizer of $\bar{w}_n \circ \mathrm{pr}_1$ and $\overline{\mathrm{pr}}_2$.

Proof. (a): It is enough to show that each factor of $W_{n-1}(A) \times A$ is integral over $W_n(A)$. The first factor is a quotient ring, and hence integral. Now consider an element $a \in A$. Then a^{q^n} is the image in A of the Teichmüller lift $[a] \in W_n(A)$. (See 1.21.) Therefore the second factor is also integral over $W_n(A)$.

(b) It suffices to show this after base change to $R[1/\mathfrak{m}] \times R_{\mathfrak{m}}$. Therefore, by 6.1, we may assume $\mathfrak{m}$ is generated by a single element π. Then an element of the kernel of α_n will be of the form $V_\pi^n[a] = (0, \ldots, 0, a)_\pi$, where $\pi^n a = 0$. On the other hand, by (4-2-6) we have

$$(V_\pi^n[a])(V_\pi^n[b]) = \pi^n V_\pi^n[ab] = (0, \ldots, 0, \pi^n ab)_\pi = 0.$$

(c) We have $(w_{\leqslant n-1} \times \mathrm{id}_A) \circ \alpha_n = w_{\leqslant n}$. Since A is $\mathfrak{m}$-flat, the map $w_{\leqslant n}$ is injective 2.7, and hence so is α_n.

(d) As above, it is enough by 6.1 to assume $\mathfrak{m}$ is generated by a single element π. Then we have

$$A \otimes_{W_n(A)} W_{n-1}(A) = A \otimes_{W_n(A)} W_n(A)/V^n W_n(A) = A/w_n(V^n W_n(A))A.$$

Examining the Witt polynomials (3-1-1) shows $w_n(V^n W_n(A)) = \pi^n A$.

(e) Again, by 6.1 we may assume $\mathfrak{m}$ is generated by a single element π. To show every element $x \in I$ is nilpotent, it is enough to restrict x to a set of generators. Therefore it is enough to show $(1 \otimes a - a \otimes 1)^{q^n} = 0$ for every element $a \in A$.

Now suppose that, for $j = 0, \ldots, q^n$, we could show

$$\binom{q^n}{j} a^j \in \mathrm{im}(w_n). \tag{8-1-2}$$

Then we would have

$$(1\otimes a - a\otimes 1)^{q^n} = \sum_j (-1)^j \binom{q^n}{j} a^j \otimes a^{q^n-j} = \sum_j (-1)^j \otimes \binom{q^n}{j} a^j a^{q^n-j}$$
$$= (1\otimes a - 1\otimes a)^{q^n} = 0,$$

which would complete the proof. So let us show (8-1-2).

Let $f = \operatorname{ord}_p(q)$ and $i = \operatorname{ord}_p(j)$. Then we have

$$\operatorname{ord}_p\binom{q^n}{j} = \operatorname{ord}_p(q^n j^{-1}) + \operatorname{ord}_p\binom{q^n-1}{j-1} \geqslant nf - i.$$

It follows that $\binom{q^n}{j} a^j$ is an R-linear multiple of $\pi^{nf-i}a^j$. Since w_n is an R-algebra map, it is therefore enough to show

$$\pi^{nf-i}a^j \in \operatorname{im}(w_n). \tag{8-1-3}$$

Now, for $b\in A$ and $s=0,\dots,n$, we have $\pi^{n-s}b^{q^s} = w_n(V_\pi^{n-s}[b])$, and therefore $\pi^{n-s}b^{q^s}$ is in the image of w_n. So to show (8-1-3), it is enough to find an integer s and an element $b\in A$ such that $\pi^{n-s}b^{q^s}$ is an R-linear divisor of $\pi^{nf-i}a^j$. In particular, it is sufficient for b and s to satisfy $b^{q^s} = a^j$ and $n-s \leqslant nf-i$.

Take s to be the greatest integer at most if^{-1}. Then we have $q^s \mid j$; so if we set $b = a^{j/q^s}\in A$, we have $b^{q^s} = a^j$. It remains to show $n-s\leqslant nf-i$. This is equivalent to $n-if^{-1}\leqslant nf-i$, which is in turn equivalent to $(1-f)(n-if^{-1})\leqslant 0$. And this holds because $1-f\leqslant 0$ and $n-if^{-1}\geqslant 0$. (Recall that $j\leqslant q^n$.) This completes the proof of (e).

(f) As above, we may assume that $\mathfrak{m}$ can be generated by a single element π. For any element $a=(a_0,\dots,a_n)_\pi \in W_n(A)$, we have

$$\alpha_n(a) = \big((a_0,\dots,a_{n-1}),\ a_0^{q^n} + \cdots + \pi^{n-1}a_{n-1}^q + \pi^n a_n\big).$$

Therefore an element $\big((a_0,\dots,a_{n-1}),b\big)\in W_{n-1}(A)\times A$ lies in the image of α_n if and only if

$$a_0^{q^n} + \cdots + \pi^{n-1}a_{n-1}^q \equiv b \mod \mathfrak{m}^n A,$$

which is exactly what we needed to show. □

8.2. Corollary. *For any R-algebra A, the ghost map*

$$w_{\leqslant n}\colon W_n(A) \longrightarrow A^{[0,n]}$$

is integral, and its kernel J satisfies $J^{2^n}=0$.

Proof. By 8.1 and induction on n. □

8.3. Theorem. (a) *The map α_n is an effective descent map for the fibered category of étale algebras.*

(b) *Relative to the diagram*

$$W_n(A) \xrightarrow{\alpha_n} W_{n-1}(A) \times A \underset{\overline{\mathrm{pr}}_2}{\overset{\bar{w}_n \circ \mathrm{pr}_1}{\rightrightarrows}} A/\mathfrak{m}^n A, \tag{8-3-1}$$

gluing data on any étale $W_{n-1}(A) \times A$-algebra is descent data (7.7).

(c) *If A is $\mathfrak{m}$-flat, then for any A'-algebra B' equipped with gluing data φ, the descended A-algebra is the subring B of B' on which the following diagram commutes*:

$$\begin{array}{ccc} & & A/\mathfrak{m}^n A \otimes_{\bar{w}_n \circ \mathrm{pr}_1} B' \\ & \overset{1\otimes \mathrm{id}_{B'}}{\nearrow} & \uparrow \varphi \\ B' & & \\ & \underset{1\otimes \mathrm{id}_{B'}}{\searrow} & \\ & & A/\mathfrak{m}^n A \otimes_{\overline{\mathrm{pr}}_2} B'. \end{array}$$

Proof. (a) This follows from Grothendieck's Theorem 7.11 and 8.1(a)–(b).

(b) We will use 7.10, where C and E are as in (7-1-1). In the notation of 7.8, put

$$S_a = \operatorname{Spec} W_n(A) \quad \text{and} \quad S_b = \operatorname{Spec} A.$$

Let Γ be the equivalence relation $S \times_{\operatorname{Spec} W_n(A)} S$ on S. By 8.1(d), we have $\Gamma_{ba} = \operatorname{Spec} A/\mathfrak{m}^n A$. The map e_a is an isomorphism because $W_{n-1}(A)$ is a quotient ring of $W_n(A)$. The map e_b is a nil immersion, by 8.1(e), and hence is an E-equivalence. Thus we can apply 7.10, which says that a Γ-action is the same as a Γ_{ba} pre-action. In other words, gluing data is descent data.

(c) This will follow from 7.12 once we verify the hypotheses. 7.12(a)–(b) are clear; 7.12(c) follows from (b) above; 7.12(d) follows from (a) above; and 7.12(e) follows from the definition of B, for the top row of (7-12-1), and from 8.1(c) and (f), for the bottom row. □

8.4. *Remark.* For any ring C, let EtAlg_C denote the category of étale C-algebras. Then another way of expressing part (b) of this theorem is that the induced functor

$$\mathsf{EtAlg}_{W_n(A)} \longrightarrow \mathsf{EtAlg}_{W_{n-1}(A)} \times_{\mathsf{EtAlg}_{A/\mathfrak{m}^n A}} \mathsf{EtAlg}_A$$

is an equivalence. (Of course, the fibered product of categories is taken in the weak sense.) In particular, we can prove things about étale $W_n(A)$-algebras by induction on n. This is the main technique in the proof of 9.2. But it also seems interesting in its own right and will probably have applications beyond the present paper.

8.5. *Remark.* If we let $\bar{W}_n(A)$ denote the image of α_n, the induced diagram

$$\bar{W}_n(A) \longrightarrow W_{n-1}(A) \times A \underset{\overline{\mathrm{pr}}_2}{\overset{\bar{w}_n \circ \mathrm{pr}_1}{\rightrightarrows}} A/\mathfrak{m}^n A.$$

satisfies all the conclusions of the theorem above, regardless of whether A is $\mathfrak{m}$-flat.

Indeed, it is an equalizer diagram by 8.1(f) and the definition of $\bar{W}_n(A)$; it is an effective descent map by 8.3 and 8.1(b). Last, because $\bar{W}_n(A)$ is the image of α_n, gluing (resp. descent) data relative to $\bar{W}_n(A)$ agrees with gluing (resp. descent) data relative to $W_n(A)$. In particular, gluing data relative to $\bar{W}_n(A)$ is descent data.

9. W and étale morphisms

We return to the general context of 1.2. In particular, E is no longer required to consist of one ideal.

9.1. Lemma. *Consider a commutative square of affine schemes* (*or any schemes*)

$$\begin{array}{ccc} X & \xleftarrow{\ g\ } & X' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ Y & \xleftarrow{\ h\ } & Y', \end{array}$$

and let U be an open subscheme of Y. Suppose that

(a) *f and f' are étale,*

(b) *the square above becomes cartesian after the base change $U \times_Y -$, and*

(c) *g and h become surjective and universally injective after the base change $(Y - U) \times_Y -$.*

Then the square above is cartesian.

Proof. Let e denote the induced map $(g, f')\colon X' \to X \times_Y Y'$. It is enough to show e is étale, surjective, and universally injective [EGA 8, 17.9.1]. The composition of e with $\mathrm{pr}_2\colon X \times_Y Y' \to Y'$ is f'. Because f is étale, so is its base change pr_2. Combining this with the étaleness of f' implies that e is étale [EGA 8, 17.3.4].

The surjectivity and universal injectivity of e can be checked after base change over Y to U and to $Y - U$. By assumption e becomes an isomorphism after base change to U. In particular, it becomes surjective and universally injective.

Let $\bar{e}, \bar{g}, \bar{h}$ denote the maps e, g, h pulled back from Y to $Y - U$. Let $\bar{h}'$ denote the base change of $\bar{h}$ from Y to X. Then, as above, we have $\bar{g} = \bar{h}' \circ \bar{e}$. Since $\bar{h}$ is universally injective, so is $\bar{h}'$. Combining this with the fact that $\bar{g}$ is universally injective, implies that $\bar{e}$ is as well [EGA 1, 3.5.6–7]. Finally $\bar{e}$ is surjective since $\bar{h}'$ is injective and $\bar{g}$ is surjective. □

9.2. Theorem. *For any étale map $\varphi\colon A \to B$ and any element $n \in \mathbb{N}^{(E)}$, the induced map $W_{R,E,n}(\varphi)\colon W_{R,E,n}(A) \to W_{R,E,n}(B)$ is étale.*

Proof. By 5.4, it is enough to assume E consists of a single maximal ideal $\mathfrak{m}$. Also, it will simplify notation if we assume $\mathfrak{m}$ is principal, generated by an element π. We may do this by 6.1 and because it is enough to show étaleness after applying $R_{\mathfrak{m}} \otimes_R -$ and $R[1/\mathfrak{m}] \otimes_R -$. Let us write $W_n = W_{R,E,n}$.

We will reason by induction on n, the case $n = 0$ being clear because W_0 is the identity functor. So from now on, assume $n \geqslant 1$.

Let $\bar{W}_n(A)$ denote the image of $\alpha_n\colon W_n(A) \to W_{n-1}(A) \times A$, and let $\bar{\alpha}_n$ denote the induced injection $\bar{W}_n(A) \to W_{n-1}(A) \times A$. Define $\bar{W}_n(B)$ and $\bar{\alpha}_n$ for B similarly.

Step 1: *$\bar{W}_n(B)$ is étale over $\bar{W}_n(A)$.* To show this, it suffices to verify conditions (a)–(e) of 7.12 for the diagram

$$\begin{array}{ccccc}
\bar{W}_n(B) & \xrightarrow{\bar{\alpha}_n} & W_{n-1}(B) \times B & \overset{\bar{w}_n \circ \mathrm{pr}_1}{\underset{\overline{\mathrm{pr}}_2}{\rightrightarrows}} & B/\mathfrak{m}^n B \\
\uparrow & & \uparrow & & \uparrow \\
\bar{W}_n(A) & \xrightarrow{\bar{\alpha}_n} & W_{n-1}(A) \times A & \overset{\bar{w}_n \circ \mathrm{pr}_1}{\underset{\overline{\mathrm{pr}}_2}{\rightrightarrows}} & A/\mathfrak{m}^n A,
\end{array}$$

where the vertical maps are induced by φ and functoriality. We know 7.12(a) holds by induction. Conditions 7.12(c)–(d) hold by 8.3 (or 8.5). Condition 7.12(e) was shown already in 8.1(f). Now consider 7.12(b). It is clear that the square of $\overline{\mathrm{pr}}_2$ maps is cocartesian. So, all that remains is to check that the square of $\bar{w}_n \circ \mathrm{pr}_1$ maps is cocartesian. By induction, $W_{n-1}(B)$ is étale over $W_{n-1}(A)$, and so this follows from 9.1, which we can apply by 6.1 and 6.8.

Step 2: *$W_n(B)$ is étale over $W_n(A)$.* We know from 8.1(b) that the kernel $I_n(A)$ of the map $\alpha_n\colon W_n(A) \to \bar{W}_n(A)$ has square zero. Therefore by [EGA 8, 18.1.2], there is an étale $W_n(A)$-algebra C and an isomorphism $f\colon C \otimes_{W_n(A)} \bar{W}_n(A) \to \bar{W}_n(B)$. Now consider the square

$$\begin{array}{ccc}
C & \longrightarrow & \bar{W}_n(B) \\
\uparrow & \overset{d}{\searrow} & \uparrow\uparrow \\
W_n(A) & \longrightarrow & W_n(B),
\end{array}$$

where the upper map is the one induced by f and where d will soon be defined. By 8.1(b), the kernel $I_n(B)$ of the right-hand map has square zero. Therefore since C is étale over $W_n(A)$, there exists a unique map d making the diagram commute. Let us now show that d is an isomorphism.

Because C is étale and hence flat over $W_n(A)$, we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I_n(B) & \longrightarrow & W_n(B) & \longrightarrow & \bar{W}_n(B) & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle e} & & \uparrow{\scriptstyle d} & & \uparrow{\scriptstyle f}\,{\scriptstyle\sim} & & \\
0 & \longrightarrow & C\otimes_{W_n(A)} I_n(A) & \longrightarrow & C & \longrightarrow & C\otimes_{W_n(A)} \bar{W}_n(A) & \longrightarrow & 0.
\end{array}$$

So to show d is an isomorphism, it is enough to show e is an isomorphism. Because $I_n(A)$ is a square-zero ideal, the action of $W_n(A)$ on it factors through $\bar{W}_n(A)$. Therefore, e factors as follows:

$$\begin{aligned}
C\otimes_{W_n(A)} I_n(A) &= C\otimes_{W_n(A)} \bar{W}_n(A)\otimes_{\bar{W}_n(A)} I_n(A) \\
&\xrightarrow{f\otimes\mathrm{id}} \bar{W}_n(B)\otimes_{\bar{W}_n(A)} I_n(A) \xrightarrow{g} I_n(B),
\end{aligned}$$

Since f is an isomorphism, it is enough to show g is an isomorphism.

Using the description (8-0-3) of I_n, the map g can be extended to the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I_n(B) & \longrightarrow & B & \xrightarrow{\cdot\pi^n} & \pi^n B & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle (\mathrm{pr}_2\circ\bar{\alpha}_n)\cdot\varphi} & & \uparrow{\scriptstyle (\mathrm{pr}_2\circ\bar{\alpha}_n)\cdot\varphi} & & \\
0 & \longrightarrow & \bar{W}_n(B)\otimes I_n(A) & \longrightarrow & \bar{W}_n(B)\otimes A & \xrightarrow{\cdot\pi^n} & \bar{W}_n(B)\otimes \pi^n A, & \longrightarrow & 0
\end{array}$$

where $\otimes$ denotes $\otimes_{\bar{W}_n(A)}$, for short. Therefore it is enough to show the right two vertical maps are isomorphisms, and to do this, it is enough to show the right-hand square in the diagram

$$\begin{array}{ccccc}
W_n(B) & \twoheadrightarrow & \bar{W}_n(B) & \xrightarrow{\mathrm{pr}_2\circ\bar{\alpha}_n} & B \\
\uparrow & & \uparrow & & \uparrow \\
W_n(A) & \twoheadrightarrow & \bar{W}_n(A) & \xrightarrow{\mathrm{pr}_2\circ\bar{\alpha}_n} & A
\end{array}$$

is cocartesian. We will do this by applying 9.1, with $U = \operatorname{Spec} R[1/\mathfrak{m}]\otimes_R \bar{W}_n(A)$.

By step 1, condition 9.1(a) holds. Now consider conditions 9.1(b)–(c). By 8.3(b), the horizontal maps in the left-hand square have square-zero kernel. In particular, the scheme maps they induce are universal homeomorphisms. And by 6.1, they become isomorphisms after applying $R[1/\mathfrak{m}]\otimes_R -$. Therefore it is enough to show 9.1(b)–(c) hold for the perimeter of the diagram above. In this case, 9.1(b) follows from 6.1, and 9.1(c) follows from 6.8. □

9.3. *Remark.* Observe that when A is E-flat, the proof terminates after step 1, which is just an application of 7.12. Thus in the central case, the argument is not much more than 8.1 and some general descent theory.

9.4. Corollary. *Let B an étale A-algebra, and let C be any A-algebra. Then for any $n \in \mathbb{N}^{(E)}$, the induced diagram*

$$\begin{array}{ccc} W_{R,E,n}(B) & \longrightarrow & W_{R,E,n}(B \otimes_A C) \\ \uparrow & & \uparrow \\ W_{R,E,n}(A) & \longrightarrow & W_{R,E,n}(C) \end{array}$$

is cocartesian.

Proof. By 5.4, we can assume E consists of a single ideal $\mathfrak{m}$. The proof will be completed by 9.1, once we check its hypotheses are satisfied. Condition (a) of 9.1 holds by 9.2, condition (b) holds by 6.1 and 2.7, and condition (c) holds by 6.8. □

9.5. *W_n does not generally commute with coproducts.* Almost anything is an example. For instance, with the p-typical Witt vectors, $W_1(A \otimes_{\mathbb{Z}} A)$ is not isomorphic to $W_1(A) \otimes_{W_1(\mathbb{Z})} W_1(A)$, when A is $\mathbb{F}_p[x]$ or $\mathbb{Z}[x]$.

9.6. *W does not generally preserve étale maps.* Let W denote p-typical Witt functor (non-truncated), and let φ denote the evident inclusion $\mathbb{Q}[x] \to \mathbb{Q}[x^{\pm 1}]$, which is étale. While $W(\varphi)$ is best viewed as a map of pro-rings, it is possible to view it as a map of ordinary rings, and ask whether it is étale. It is not: $W(\varphi)$ can be identified with $\varphi^{\mathbb{N}}\colon \mathbb{Q}[x]^{\mathbb{N}} \to \mathbb{Q}[x^{\pm 1}]^{\mathbb{N}}$, which is not étale because $\mathbb{Q}[x^{\pm 1}]^{\mathbb{N}}$ is not finitely generated as an $\mathbb{Q}[x]^{\mathbb{N}}$-algebra. This is an elementary exercise.

9.7. *Other truncation sets for the big Witt vectors.* Some writers have considered more general systems of truncations for the big Witt functor 1.15. See [Hesselholt and Madsen 1997, §4.1], for example. Given a finite set T of positive integers closed under extraction of divisors, they define an endofunctor W_T of the category of rings. When T consists of all the divisors of some integer $d \geqslant 1$, then W_T agrees with our $W_{\mathbb{Z},E,n}$, where E consists of the maximal ideals $\mathfrak{m} \subset \mathbb{Z}$ that contain d and where $n_{\mathfrak{m}} = \mathrm{ord}_{\mathfrak{m}}(d)$. Thus the two systems of truncations are cofinal with respect to each other.

The functors W_T also preserve étale maps. Indeed, it is enough to show that the base change to $\mathbb{Z}[1/T]$ and to $\mathbb{Z}_{(p)}$, for each prime $p \in T$, is étale. (See [EGA 8, 17.7.2(ii)].) Applying the identity $W_T(A)[1/p] = W_T(A[1/p])$, which can be established by looking at the graded pieces of the Verschiebung filtration, it is enough to consider $\mathbb{Z}[1/T]$-algebras and $\mathbb{Z}_{(p)}$-algebras. In the either case, $W_T(A)$ is simply a product of p-typical Witt rings $W_n(A)$ for various primes p and lengths

n (see [Hesselholt and Madsen 1997, (4.1.10)]), in which case the result follows from 9.2, or van der Kallen's original theorem [1986, (2.4)].

Acknowledgements

I thank Amnon Neeman for helpful discussions on some technical points and Lance Gurney for comments on earlier versions of this paper.

References

[Borceux 1994a] F. Borceux, *Handbook of categorical algebra, I: Basic category theory*, Encyclopedia of Mathematics and its Applications **50**, Cambridge University Press, Cambridge, 1994. MR 96g:18001a Zbl 0803.18001

[Borceux 1994b] F. Borceux, *Handbook of categorical algebra, II: Categories and structures*, Encyclopedia of Mathematics and its Applications **51**, Cambridge University Press, Cambridge, 1994. MR 96g:18001b Zbl 0843.18001

[Borger 2010] J. Borger, "The basic geometry of Witt vectors, II: spaces", 2010. To appear in *Math. Ann.* arXiv 1006.0092

[Borger and Wieland 2005] J. Borger and B. Wieland, "Plethystic algebra", *Adv. Math.* **194**:2 (2005), 246–283. MR 2006i:13044 Zbl 1098.13033

[Bourbaki 1983] N. Bourbaki, *Algèbre commutative, chapitre 8: dimension; chapitre 9: anneaux locaux noethériens complets*, Hermann, Paris, 1983. Reprinted Springer, Berlin, 2006. MR 86j:13001 Zbl 0579.13001

[Buium 1996] A. Buium, "Geometry of p-jets", *Duke Math. J.* **82** (1996), 349–367. MR 97c:14029 Zbl 0882.14007

[Buium 2005] A. Buium, *Arithmetic differential equations*, Mathematical Surveys and Monographs **118**, American Mathematical Society, Providence, RI, 2005. MR 2006k:14035 Zbl 1088.14001

[Buium and Simanca 2009] A. Buium and S. R. Simanca, "Arithmetic Laplacians", *Adv. Math.* **220**:1 (2009), 246–277. MR 2009m:12008 Zbl 1172.14027

[Drinfeld 1976] V. G. Drinfeld, "Coverings of p-adic symmetric regions", *Funkcional. Anal. i Priložen.* **10**:2 (1976), 29–40. In Russian; translated in Funct. Anal. Appl. **10**:2 (1976), 107-115. MR 54 #10281 Zbl 0346.14010

[EGA 1] A. Grothendieck, "Éléments de géométrie algébrique, I: le langage des schémas", *Inst. Hautes Études Sci. Publ. Math.* **4** (1960), 1–228. MR 33 #7330 Zbl 0118.36206

[EGA 6] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas (seconde partie)", *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 1–231. MR 33 #7330 Zbl 0135.39701

[EGA 8] A. Grothendieck, "Éléments de géométrie algébrique, IV: étude locale des schémas et des morphismes de schémas (quatrième partie)", *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 1–361. MR 39 #220 Zbl 0153.22301

[Grothendieck 1958] A. Grothendieck, "La théorie des classes de Chern", *Bull. Soc. Math. France* **86** (1958), 137–154. MR 22 #6818 Zbl 0091.33201

[Grothendieck 1966] A. Grothendieck, "Technique de descente et théorèmes d'existence en géometrie algébrique, I: généralités; descente par morphismes fidèlement plats", exposé 190 in *Séminaire Bourbaki,* 1959/1960, Benjamin, New York, 1966. Reprinted as pp. 299–327 in *Séminaire Bourbaki*, vol. 5, Soc. Math. France, Paris, 1995. MR 1603475 Zbl 0229.14007

[Hazewinkel 1978] M. Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics **78**, Academic Press, New York, 1978. MR 82a:14020 Zbl 0454.14020

[Hesselholt and Madsen 1997] L. Hesselholt and I. Madsen, "Cyclic polytopes and the K-theory of truncated polynomial algebras", *Invent. Math.* **130** (1997), 73–97. MR 98k:19002 Zbl 0884.19004

[Joyal 1985a] A. Joyal, "δ-anneaux et λ-anneaux", *C. R. Math. Rep. Acad. Sci. Canada* **7**:4 (1985), 227–232. MR 86j:13024 Zbl 0583.13004

[Joyal 1985b] A. Joyal, "δ-anneaux et vecteurs de Witt", *C. R. Math. Rep. Acad. Sci. Canada* **7**:3 (1985), 177–182. MR 86j:13023 Zbl 0594.13023

[van der Kallen 1986] W. van der Kallen, "Descent for the K-theory of polynomial rings", *Math. Z.* **191**:3 (1986), 405–415. MR 87h:13012 Zbl 0563.13011

[Lazard 1975] M. Lazard, *Commutative formal groups*, Lecture Notes in Mathematics **443**, Springer, Berlin, 1975. MR 52 #13861 Zbl 0304.14027

[Rydh 2009] D. Rydh, "Noetherian approximation of algebraic spaces and stacks", preprint, 2009. arXiv 0904.0227

[Rydh 2010] D. Rydh, "Submersions and effective descent of étale morphisms", *Bull. Soc. Math. France* **138**:2 (2010), 181–230. MR 2679038 Zbl 05769982

[SGA 1] A. Grothendieck and M. Raynaud, *Séminaire de Géométrie Algébrique du Bois Marie* 1960/61*: Revêtements étales et groupe fondamental* (SGA 1), Lecture Notes in Mathematics **224**, Springer, Berlin, 1971. Updated and annotated reprint, Soc. Math. de France, Paris, 2003. MR 50 #7129 Zbl 0234.14002

[Tall and Wraith 1970] D. O. Tall and G. C. Wraith, "Representable functors and operations on rings", *Proc. London Math. Soc.* (3) **20** (1970), 619–643. MR 42 #258 Zbl 0226.13007

[Wilkerson 1982] C. Wilkerson, "Lambda-rings, binomial domains, and vector bundles over CP(∞)", *Comm. Algebra* **10**:3 (1982), 311–328. MR 83f:55003 Zbl 0492.55004

[Witt 1937] E. Witt, "Zyklische Körper und Algebren der Charakteristik p vom Grad p^n: Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p", *J. Reine Angew. Math.* **176** (1937), 126–140. Reprinted in [Witt 1998], 142–156. Zbl 0016.05101

[Witt 1998] E. Witt, *Collected papers / Gesammelte Abhandlungen*, edited by I. Kersten, Springer, Berlin, 1998. MR 99i:01038 Zbl 0917.01054

Communicated by Hendrik W. Lenstra
Received 2010-05-13 Revised 2010-08-08 Accepted 2010-10-13

james.borger@anu.edu.au *Department of Mathematics, Australian National University, Mathematical Sciences Institute, Building 27, Canberra 2602, Australia*
http://wwwmaths.anu.edu.au/~borger/

msp

ALGEBRA AND NUMBER THEORY 5:2 (2011)
https://doi.org/10.2140/ant.2011.5.287

Correction to a proof in the article Patching and admissibility over two-dimensional complete local domains

Danny Neftin and Elad Paran

Volume **4**:6 (2010), 743–762

The proof of Lemma 1.8 of the article in the title is incorrect. We supply an alternate argument for Proposition 1.10, whose proof invoked that lemma.

We are grateful to Yong Hu for pointing out to us a gap in the proof of Lemma 1.8 of our article "Patching and admissibility over two-dimensional complete local domains", namely, the isomorphism $R/\mathfrak{p} \cong S/\mathfrak{q}$ implies only that $S = R + \mathfrak{q}$ and not $S = R + \mathfrak{p}S$, as required for this argument.

The lemma is applied for the rings

$$R_0 = D_{J\cup J'}, \quad R_1 = D_J, \quad R_2 = D_{J'}, \quad R = D_\varnothing,$$

where $J \cap J' = \varnothing$, to show that $S := R_1 \cap R_2 = R$. Let us show this assertion directly. In particular, this will trivially imply that for these rings $\mathfrak{q} = \mathfrak{p}S$.

All references are to the article in question.

Recall that I is a finite set and that v is the extension of the order function of the ideal $\mathfrak{p} := (x, y) \lhd K[x, y]$ to $K(x, y)$. For $i \in I$, let $z_i = y/(x - c_i y)$ and for a subset $J \subset I$, D_J is defined as the completion of $K[z_j \mid j \in J][x, y]$ with respect to v.

Lemma. *Let $i, j \in I$ be two distinct indices. Then $D_{\{i\}} \cap D_{\{j\}} = D_\varnothing$.*

Proof. By Proposition 1.5, $D_{\{i\}} = K[z_i][\![x - c_i y]\!]$ and hence an element $f \in D_{\{i\}}$ can be written as $\sum_{k=0}^{\infty} f_k(z_i)(x - c_i y)^k$ for some polynomials f_k, $k \geq 0$. Assume $f \in D_{\{i,j\}}$ can also be written as $\sum_{k=0}^{\infty} g_k(z_j)(x - c_j y)^k \in D_{\{j\}} = K[z_j][\![x - c_j y]\!]$, where g_k are polynomials for $k \geq 0$.

In particular,

$$f_k(z_i)(x - c_i y)^k = g_k(z_j)(x - c_j y)^k \pmod{\mathfrak{p}^{k+1} D_{\{i,j\}}} \tag{1}$$

MSC2010: primary 12F12; secondary 12E30, 12E15, 12F10.

Keywords: patching, crossed product, admissible groups, division algebras, complete local domains.

for all $k \geq 0$. We claim that equality (1) in fact holds in $D_{\{i,j\}}$. Indeed, since $x - c_i y = \big(1 + (c_j - c_i)z_j\big)(x - c_j y)$, the difference between the sides of (1) is

$$\big(f_k(z_i)(1 + (c_j - c_i)z_j)^k - g_k(z_j)\big)(x - c_j y)^k \in K[z_i, z_j](x - c_j y)^k. \quad (2)$$

Since $\mathfrak{p}$ is contained in the center of the valuation v, Proposition 1.5 implies that the difference (2) is in $\mathfrak{p}^{k+1} D_{\{i,j\}}$ only if it is zero, proving the claim.

By finding a common denominator, one can write an element $f_k(z_i)(x - c_i y)^k$ as $p_k(x, y)/(x - c_i y)^m$ where $m \geq 0$ and p_k is a homogenous polynomial of degree $k + m$ that is prime to $(x - c_i y)^m$. Writing $g_k(z_j)(x - c_j y)^k = q_k(x, y)/(x - c_j y)^l$ for $l \geq 0$ and q_k a homogenous polynomial of degree $k + l$ that is prime to $(x - c_i y)^l$, the equality

$$\frac{p_k(x, y)}{(x - c_i y)^m} = \frac{q_k(x, y)}{(x - c_j y)^l}$$

implies that $m = l = 0$ and hence that $f_k(z_i)(x - c_i y)^k \in K[x, y]$ for all $k \geq 0$. It follows that $f = \sum_{k=0}^{\infty} f_k(z_i)(x - c_i y)^k \in K[\![x, y]\!]$, as required. □

Let us complete the proof of Proposition 1.10:

Proposition. *Suppose $J, J' \subseteq I$. Then $D_J \cap D_{J'} = D_{J \cap J'}$.*

Proof. Clearly $D_{J \cap J'} \subseteq D_J \cap D_{J'}$. For the converse inclusion, we distinguish between two cases. First suppose that $J \cap J' \neq \varnothing$ and fix $j \in J \cap J'$. Then $D_J = K[z_k \mid k \in J][\![x - c_j y]\!]$, $D_{J'} = K[z_k \mid k \in J'][\![x - c_j y]\!]$ and hence

$$D_J \cap D_{J'} = (K[z_k \mid k \in J] \cap K[z_k \mid k \in J'])[\![x - c_j y]\!].$$

By Lemma 1.9, $K[z_k \mid k \in J] \cap K[z_k \mid k \in J'] = K[z_k \mid k \in J \cap J']$.

Now suppose that $J \cap J' = \varnothing$. If $|J| = |J'| = 1$, then the claim follows from the Lemma. Assume without loss of generality $|J| \geq 2$. For distinct $j_1, j_2 \in J$, we have by the previous case $D_J \cap D_{J' \cup \{j_i\}} = D_{\{j_i\}}$, for $i = 1, 2$. In particular, $D_J \cap D_{J'} \subseteq D_{\{j_1\}} \cap D_{\{j_2\}}$. By the Lemma, $D_{\{j_1\}} \cap D_{\{j_2\}} = D_{\varnothing}$ implying that $D_J \cap D_{J'} = D_{\varnothing}$ as required. □

Communicated by Jean-Louis Colliot-Thélène
Received 2011-07-06 Revised 2011-07-13 Accepted 2011-08-10

neftin@umich.edu *Department of Mathematics, University of Michigan, Ann Arbor, 530 Church St., Ann Arbor 48109, United States*

paranela@post.tau.ac.il *School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, 69978 Tel Aviv, Israel*
http://www.tau.ac.il/~paranela/

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@mathscipub.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 5 No. 2 2011