Algebra & Number Theory

Volume 18
2024
No. 2

msp

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2024 is US $525/year for the electronic version, and $770/year (+$65, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

ALGEBRA AND NUMBER THEORY 18:2 (2024)
https://doi.org/10.2140/ant.2024.18.209

Decidability via the tilting correspondence

Konstantinos Kartas

We prove a relative decidability result for perfectoid fields. This applies to show that the fields $\mathbb{Q}_p(p^{1/p^\infty})$ and $\mathbb{Q}_p(\zeta_{p^\infty})$ are (existentially) decidable relative to the perfect hull of $\mathbb{F}_p((t))$ and $\mathbb{Q}_p^{ab}$ is (existentially) decidable relative to the perfect hull of $\overline{\mathbb{F}}_p((t))$. We also prove some unconditional decidability results in mixed characteristic via reduction to characteristic p.

Introduction

After the decidability of the p-adic numbers $\mathbb{Q}_p$ was established by Ax and Kochen [1965] and independently by Eršov [1965], several decidability questions about local fields and their extensions have been raised and answered:

- In mixed characteristic, Kochen [1975] showed that $\mathbb{Q}_p^{ur}$, the maximal unramified extension of $\mathbb{Q}_p$, is decidable in the language $L_{\text{val}} = \{0, 1, +, \cdot, \mathcal{O}\}$ (see notation). More generally, by work of Eršov [1965], Ziegler [1972], Basarab [1978] and Bélair [1999] and more recently by Lee [2020], Lee and Lee [2021] and Anscombe and Jahnke [2022], we have a good understanding of the model theory of unramified and finitely ramified mixed characteristic henselian fields.

During this research, the author was funded by EPSRC grant EP/20998761 and was also supported by the Onassis Foundation - Scholarship ID: F ZP 020-1/2019-2020.
MSC2010: primary 11U05; secondary 11U09.
Keywords: perfectoid fields, model theory, valued fields, decidability, tilting, tame fields.

- In positive characteristic, our understanding is much more limited. Nevertheless, by work of Denef and Schoutens [2003], we know that $\mathbb{F}_p((t))$ is *existentially* decidable in $L_{\mathrm{val}}(t) = \{0, 1, t, +, \cdot, \mathcal{O}\}$ (see notation), modulo resolution of singularities.[1] In fact, [Denef and Schoutens 2003, Theorem 4.3] applies to show that (assuming resolution) any finitely ramified extension of $\mathbb{F}_p((t))$ is existentially decidable relative to its residue field. Anscombe and Fehm [2016] showed *unconditionally* that $\mathbb{F}_p((t))$ is existentially decidable but in the language L_{val}, which does not include a constant symbol for t.

Our understanding is less clear for *infinitely ramified* fields and there are many extensions of $\mathbb{Q}_p$ (resp. $\mathbb{F}_p((t))$) of great arithmetic interest, whose decidability problem is still open:

- In mixed characteristic, these include $\mathbb{Q}_p^{ab}$, the maximal abelian extension of $\mathbb{Q}_p$ and the totally ramified extension $\mathbb{Q}_p(\zeta_{p^\infty})$, obtained by adjoining all p^n-th roots of unity. These extensions had already been discussed in Macintyre's survey [1986, page 140] and a conjectural axiomatization of $\mathbb{Q}_p^{ab}$ was given by Koenigsmann [2018, page 55]. Another interesting extension is $\mathbb{Q}_p(p^{1/p^\infty})$, a totally ramified extension of $\mathbb{Q}_p$ obtained by adjoining a compatible system of p-power roots of p.
- In positive characteristic, two very natural infinitely ramified fields are the perfect hulls of $\mathbb{F}_p((t))$ and $\overline{\mathbb{F}}_p((t))$. Both of these fields have been conjectured to be decidable; see [Kuhlmann and Rzepka 2023, page 4] for the former. The recent work of Kuhlmann and Rzepka [2023] ultimately aims at extending Kuhlmann's earlier results for tame fields to cover fields like the ones mentioned above.

The above fields will be the main objects of interest throughout the paper. Their p-adic (resp. t-adic) completions are typical examples of *perfectoid fields* in the sense of Scholze [2012] (see Section 3). A perfectoid field (K, v) is a valued field which is complete with respect to a nondiscrete valuation of rank 1, with residue characteristic equal to $p > 0$ and such that the Frobenius map $\Phi : \mathcal{O}_K/(p) \to \mathcal{O}_K/(p) : x \mapsto x^p$ is surjective. Loosely speaking, the last condition says that one can extract approximate p-power roots of any element in the field. For any perfectoid field K, one can define its tilt $K^\flat$ (see Section 3.2), which intuitively is its *local* function field analogue and serves as a good characteristic p approximation of K. In practice, this means that one can often reduce arithmetic problems about K to arithmetic problems about $K^\flat$. This kind of transfer principle, which works for a fixed p, should be contrasted with the Ax–Kochen/Ershov principle which achieves such a reduction only *asymptotically*, i.e., with the residue characteristic $p \to \infty$. This is explained in detail in Scholze's ICM report; see [Scholze 2014, page 2].

Our main goal is to set the stage for incorporating ideas from perfectoid geometry in the model theory of henselian fields. In the present paper we focus on decidability, although it is conceivable that our methods can be used in different model-theoretic contexts. We will prove the following relative decidability result for the fields discussed above:

[1] The formalism of [Denef and Schoutens 2003] does not include a unary predicate $\mathcal{O}$ for the valuation ring. This does not make a difference because of the equivalences $x \in \mathcal{O} \leftrightarrow \exists y (y^2 = 1 + t \cdot x^2)$ (for $p > 2$; replace squares with cubes for $p = 2$) and $x \notin \mathcal{O} \leftrightarrow x^{-1} \in t \cdot \mathcal{O}$.

Corollary A. (a) *Assume* $\mathbb{F}_p((t))^{1/p^\infty}$ *is decidable* (*resp.* $\exists$-*decidable*) *in* $L_{\text{val}}(t)$. *Then* $\mathbb{Q}_p(p^{1/p^\infty})$ *and* $\mathbb{Q}_p(\zeta_{p^\infty})$ *are decidable* (*resp.* $\exists$-*decidable*) *in* L_{val}.

(b) *Assume* $\bar{\mathbb{F}}_p((t))^{1/p^\infty}$ *is decidable* (*resp.* $\exists$-*decidable*) *in* $L_{\text{val}}(t)$. *Then* $\mathbb{Q}_p^{ab}$ *is decidable* (*resp.* $\exists$-*decidable*) *in* L_{val}.

As usual, we write $\mathbb{F}_p((t))^{1/p^\infty}$ (resp. $\bar{\mathbb{F}}_p((t))^{1/p^\infty}$) for the perfect hull of $\mathbb{F}_p((t))$ (resp. $\bar{\mathbb{F}}_p((t))$), L_{val} for the language of valued fields and $L_{\text{val}}(t)$ for the language L_{val} enriched with a constant symbol for t (see notation). Corollary A is essentially a special case of a general relative decidability result for perfectoid fields, which is discussed next. (Strictly speaking, the fields in Corollary A are not perfectoid but one can still derive Corollary A from Theorem A directly.)

Let F be a perfectoid field of characteristic p (e.g., $F = \mathbb{F}_p\widehat{((t))^{1/p^\infty}}$). An *untilt* of F is a mixed characteristic perfectoid field K together with an isomorphism $\iota : K^\flat \xrightarrow{\cong} F$. In general, there will be many nonisomorphic untilts of F. In fact, there will be too many untilts even up to elementary equivalence (see Proposition 3.6.9(b)), thus shattering the naive guess of K being decidable relative to its tilt $K^\flat$. On a more elementary level, one needs to assume decidability with *parameters* on the positive characteristic side (see Example 4.3.7). Nevertheless, a relative decidability result for perfectoids can be salvaged by asking that K be an R_0-*computable* untilt of F, a notion which is briefly explained below (see Section 4.2 for details).

Write $W(\mathcal{O}_F)$ for the ring of Witt vectors over $\mathcal{O}_F$ (see Section 3.3). An element $\xi \in W(\mathcal{O}_F)$ is identified with its associated Witt vector, which is an infinite sequence $(\xi_0, \xi_1, \dots)$ with $\xi_n \in \mathcal{O}_F$. Whenever there is a *computable* subring $R_0 \subseteq \mathcal{O}_F$ such that $\xi_n \in R_0$ and the function $\mathbb{N} \to R_0 : n \mapsto \xi_n$ is *recursive*, we say that ξ is R_0-computable. As usual, a computable ring R_0 is one whose underlying set is (or may be identified with) a recursive subset of $\mathbb{N}$, so that the ring operations are (or are identified with) recursive functions (e.g., $\mathbb{F}_p[t]$ is a computable ring). An important result by Fargues and Fontaine gives a one-to-one correspondence between untilts of F and certain principal ideals of $W(\mathcal{O}_F)$ (Theorem 3.5.11). An untilt K of F is then said to be an R_0-*computable untilt* whenever there exists an R_0-computable generator $\xi \in W(\mathcal{O}_F)$ of the ideal corresponding to K. We then have the following relative decidability result (the name is due to Scanlon):

Theorem A (perfectoid transfer). *Suppose* K *is an* R_0-*computable untilt of* F. *If* F *is decidable in* $L_{\text{val}}(R_0)$, *then* K *is decidable in* L_{val}.

Here $L_{\text{val}}(R_0)$ is the language L_{val} enriched with constant symbols for the elements of R_0. We also obtain an *existential* version of Theorem A in Section 4.3. The condition on K being an R_0-computable untilt of F is true in virtually all cases of interest (although generically false), even for a natural choice of R_0. Corollary A is an immediate consequence of Theorem A, by considering the t-adic completion of $\mathbb{F}_p((t))^{1/p^\infty}$ (resp. $\bar{\mathbb{F}}_p((t))^{1/p^\infty}$ for part (b)) and $R_0 = \mathbb{F}_p[t]$. The two key ingredients in the proof of Theorem A are:

(1) An (unpublished) Ax–Kochen/Ershov style result by van den Dries for general mixed characteristic henselian fields, presented in Section 2.

(2) The Fargues–Fontaine correspondence described above, presented in Section 3.5.

Let us now outline how these two ingredients will be combined towards the proof of Theorem A. The result by van den Dries will enable us to reduce the decidability of K to the *uniform* decidability of the sequence of residue rings $(\mathcal{O}_K/(p^n))_{n\in\omega}$ and also the decidability of (Γ_v, vp). The Fargues–Fontaine correspondence then gives us a way to interpret each individual residue ring $\mathcal{O}_K/(p^n)$ inside the tilt F (with parameters from R_0), via an interpretation E_n. The assumption on K being R_0-computable will then imply that the sequence of interpretations $(E_n)_{n\in\omega}$ is *uniformly recursive* (see Section 1.2.12). Having assumed the decidability of F in $L_{\text{val}}(R_0)$, this will then give us that the sequence $(\mathcal{O}_K/(p^n))_{n\in\omega}$ is uniformly decidable. The pointed value group (Γ_v, vp) is easily seen to be interpretable in F (with parameters from R_0) and the decidability of K follows.

It should be mentioned that — prior to this work — Rideau, Scanlon and Simon had made a formative observation, namely that the Fargues–Fontaine correspondence already provides us with an interpretation of the valuation ring $\mathcal{O}_K$ in $\mathcal{O}_F$ (with parameters) in the sense of continuous logic. This however does not yield an interpretation in the sense of ordinary first-order logic (see Section 4.1.1). On the other hand, there do exist honest first-order interpretations of the *truncated* residue rings $\mathcal{O}_K/(p^n)$ in $\mathcal{O}_F$, which is why it is convenient to work with them instead.

Theorem A allows us to reduce decidability problems from the mixed characteristic to the positive characteristic world. Although our model-theoretic understanding of the latter is notoriously limited, this method still yields several applications. In Sections 5 and 6 we obtain new *unconditional* decidability results in mixed characteristic via reduction to characteristic p. In Section 5, we prove the following:

Corollary B. *The valued field* $(\mathbb{Q}_p(p^{1/p^\infty}), v_p)$ (*resp.* $(\mathbb{Q}_p(\zeta_{p^\infty}), v_p)$) *admits a maximal immediate extension which is decidable in* L_{val}.

Note that the fields $\mathbb{Q}_p(p^{1/p^\infty})$ and $\mathbb{Q}_p(\zeta_{p^\infty})$ are *not* Kaplansky and have many nonisomorphic maximal immediate extensions, all of which are *tame* in the sense of Kuhlmann [2016] (see Example 5.1.6). Although the work of Kuhlmann yields several decidability results for equal characteristic tame fields, Corollary B is, to my knowledge, the first decidability result for tame fields of mixed characteristic (see Section 5). The proof uses a recent decidability result of Lisinski [2021] for the Hahn field $\mathbb{F}_p((t^\Gamma))$ with $\Gamma = \frac{1}{p^\infty}\mathbb{Z}$ in the language $L_{\text{val}}(t)$, strengthening Kuhlmann's earlier result for $\mathbb{F}_p((t^\Gamma))$ in the language L_{val}; see [Kuhlmann 2016, Theorem 1.6]. Corollary B then follows from Theorem A and basic properties of the tilting equivalence (see Section 3.5.13). It is worth remarking that most maximal immediate extensions of $\mathbb{Q}_p(p^{1/p^\infty})$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$) are *undecidable* (see Remark 5.2.3).

Without making essential use of the perfectoid machinery but only the philosophy thereof, we show in Section 6 the following:

Theorem B. *Let K be any of the valued fields $\mathbb{Q}_p(p^{1/p^\infty})$, $\mathbb{Q}_p(\zeta_{p^\infty})$ or $\mathbb{Q}_p^{ab}$. The existential theory of $\mathcal{O}_K/p\mathcal{O}_K$ in the language of rings L_{rings} is decidable.*

The proof is again via reduction to characteristic p, using a recent existential decidability result for equal characteristic henselian valued fields in the language L_{val}, due to Anscombe and Fehm [2016]. However, as Corollary A suggests, if we aim to understand the theories of $\mathbb{Q}_p(p^{1/p^\infty})$, $\mathbb{Q}_p(\zeta_{p^\infty})$ and $\mathbb{Q}_p^{ab}$ via reduction to positive characteristic, we will need stronger results in the language $L_{\text{val}}(t)$ on the characteristic p side. This is also supported by Proposition 7.2.3 which shows that the Diophantine problem for $\mathbb{F}_p((t))^{1/p^\infty}$ in $L_{\text{val}}(t)$ is Turing reducible to the $\forall^1\exists$-theory of $\mathbb{Q}_p(p^{1/p^\infty})$.

An application of a different flavor, which yields an *undecidability* result in mixed characteristic via reduction to characteristic p, was recently found in [Kartas 2023]. Kartas [2023, Theorem A] shows that the asymptotic theory of $\{K : [K : \mathbb{Q}_p] < \infty\}$ in the language L_{val} with a cross-section is undecidable.

Notation

- If (K, v) is a valued field, we denote by $\mathcal{O}_v$ the valuation ring. If the valuation is clear from the context, we shall also write $\mathcal{O}_K$. We write Γ_v for the value group and k_v for the residue field. If the valuation v is clear from the context, we also denote them by Γ and k respectively.
- When (K, v) is of mixed characteristic, we write p for the number $\text{char}(k)$. The notation $p^n\mathcal{O}_v$ stands for the ideal of $\mathcal{O}_v$ generated by the element p^n. If both the field in question and the valuation v are clear from the context, we shall write (p^n) for $p^n\mathcal{O}_v$.
- $\mathbb{Z}_p^{ur}$: The valuation ring of $(\mathbb{Q}_p^{ur}, v_p)$, the maximal unramified extension of $\mathbb{Q}_p$ equipped with the unique extension of the p-adic valuation.
- $\mathbb{Z}_p^{ab}$: The valuation ring of $(\mathbb{Q}_p^{ab}, v_p)$, the maximal Galois extension of $\mathbb{Q}_p$ whose Galois group over $\mathbb{Q}_p$ is abelian.
- We write $\mathbb{F}_p((t))^{1/p^\infty}$ (resp. $\bar{\mathbb{F}}_p((t))^{1/p^\infty}$) for the perfect hull of $\mathbb{F}_p((t))$ (resp. $\bar{\mathbb{F}}_p((t))$).
- For a given language L, we denote by Sent_L the set of L-sentences and by Form_L the set of L-formulas. If M is an L-structure and $A \subseteq M$ is an arbitrary subset, we write $L(A)$ for the language L enriched with a constant symbol c_a for each element $a \in A$. The L-structure M can be updated into an $L(A)$-structure in the obvious way.
- We write $L_{\text{rings}} = \{0, 1, +, \cdot\}$ for the language of rings, $L_{\text{oag}} = \{0, +, <\}$ for the language of ordered abelian groups, $L_{\text{val}} = L_{\text{rings}} \cup \{\mathcal{O}\}$ for the language of valued fields (where $\mathcal{O}$ is a unary predicate for the valuation ring), $L_{\text{val}}(t) = L_{\text{val}} \cup \{t\}$, where t is a constant symbol whose intended interpretation will always be clear from the context. A local ring $(R, \mathfrak{m}_R)$ may be viewed as an L_{lcr}-structure, where L_{lcr} is the *language of local rings* consisting of the language of rings L_{rings} together with a unary predicate $\mathfrak{m}$, whose intended interpretation is the maximal ideal $\mathfrak{m}_R \subseteq R$.

1. Preliminaries

1.1. *Decidability.*

1.1.1. *Introduction.* Fix a *countable* language L and let Sent_L be the set of well-formed L-sentences, identified with $\mathbb{N}$ via some Gödel numbering. Let M be an L-structure. Recall that M is decidable if we have an algorithm to decide whether $M \models \phi$, for any given $\phi \in \mathrm{Sent}_L$. More formally, let $\chi_M : \mathrm{Sent}_L \to \{0, 1\}$ be the characteristic function of $\mathrm{Th}(M) \subseteq \mathrm{Sent}_L$. We say that M is *decidable* if χ_M is recursive.

1.1.2. *Uniform decidability.*

Definition 1.1.3. For each $n \in \mathbb{N}$, let $f_n : \mathbb{N} \to \mathbb{N}$ be a function. The sequence $(f_n)_{n\in\omega}$ is uniformly recursive if the function $\mathbb{N} \times \mathbb{N} \to \mathbb{N} : (n, m) \mapsto f_n(m)$ is recursive.

This concept is best illustrated with a *nonexample*:

Example 1.1.4. Let $A \subseteq \mathbb{N}$ be nonrecursive. For each $n \in \mathbb{N}$, let $\delta_n : \mathbb{N} \to \mathbb{N} : m \mapsto \delta_{nm}$, where δ_{nm} is the Kronecker symbol. For each $n \in \mathbb{N}$, define $f_n : \mathbb{N} \to \mathbb{N}$ to be (1) δ_n if $n \in A$ and (2) identically 0 if $n \notin A$. One readily verifies that each individual f_n is recursive. On the other hand, the sequence $(f_n)_{n\in\omega}$ is not uniformly recursive. Indeed, otherwise we could solve the membership problem for A, using that $n \in A \iff f_n(n) = 1$.

Using some Gödel numbering, we can also state a version of Definition 1.1.3 for sequences of functions $(f_n)_{n\in\omega}$, where $\mathrm{dom}(f_n) = \mathrm{Sent}_L$ (or $\mathrm{cdm}(f_n) = \mathrm{Sent}_L$). One can then define a notion of *uniform* decidability for sequences of L-structures:

Definition 1.1.5. A sequence $(M_n)_{n\in\omega}$ of L-structures is *uniformly decidable* if the sequence of functions $(\chi_{M_n})_{n\in\omega}$ is uniformly recursive, i.e., if the function $\chi : \mathbb{N} \times \mathrm{Sent}_L \to \{0, 1\} : (n, \phi) \mapsto \chi_{M_n}(\phi)$ is recursive.

Remark 1.1.6. If the sequence $\chi : \mathbb{N} \times \mathrm{Sent}_L \to \{0, 1\} : (n, \phi) \mapsto \chi_{M_n}(\phi)$ is recursive when restricted to *existential* sentences, we naturally say that the sequence $(M_n)_{n\in\omega}$ is *uniformly existentially decidable*. Other syntactic variants may be defined analogously.

1.2. *Interpretability.*

Our formalism follows closely [Hodges 1993, Section 5.3], where details and proofs may be found.

1.2.1. *Interpretations.* Given a language L, an *unnested* atomic L-formula is one of the form $x = y$ or $x = c$ or $F(\bar{x}) = y$ or $R(\bar{x})$, where x, y are variables, c is a constant symbol, $\bar{x}$ is a tuple of variables, F is a function symbol and R is a relation symbol of the language L.

Definition 1.2.2. An n-dimensional interpretation of an L-structure M in the L'-structure N is a triple $\Gamma = (\partial_\Gamma, \phi \mapsto \phi_\Gamma, f_\Gamma)$ consisting of

(1) an L'-formula $\partial_\Gamma(x_1, \dots, x_n)$,

(2) a map $\phi \mapsto \phi_\Gamma$, that takes an unnested atomic L-formula $\phi(x_1, \dots, x_m)$ and sends it to an L'-formula $\phi_\Gamma(\bar{y}_1, \dots, \bar{y}_m)$, where each $\bar{y}_i$ is an n-tuple of variables,

(3) a surjective map $f_\Gamma : \partial_\Gamma(N^n) \twoheadrightarrow M$,

such that for all unnested atomic L-formulas $\phi(x_1, \dots, x_m)$ and all $\bar{a}_i \in \partial_\Gamma(N^n)$, we have

$$M \models \phi(f_\Gamma(\bar{a}_1), \dots, f_\Gamma(\bar{a}_m)) \Longleftrightarrow N \models \phi_\Gamma(\bar{a}_1, \dots, \bar{a}_m).$$

An *interpretation* of an L-structure M in the L'-structure N is an n-dimensional interpretation Γ, for some $n \in \mathbb{N}$. In that case, we also say that M is *interpretable* in N. The formulas ∂_Γ and ϕ_Γ (for all unnested atomic ϕ) are the *defining formulas* of Γ.

Interpretability is a *transitive* relation on the class of structures, i.e., if the L-structure M is interpretable in the L'-structure N and N is interpretable in the L''-structure P, then there exists a *composite* interpretation of M in P [Hodges 1993, Exercise 2, page 218].

If N is an L'-structure and $\bar{a} = (a_1, \dots, a_m) \in N^m$, we write $(N, \bar{a})$ for the expansion of N in the language $L(\bar{c})$, which is L together with an m-tuple of constant symbols $(c_1, \dots, c_m)$ with $c_i^{(N,\bar{a})} = a_i$. If M is interpretable in $(N, \bar{a})$, for some $\bar{a} \in N^m$, we say that M is interpretable in N *with parameters*.

Proposition 1.2.3 [Hodges 1993, reduction Theorem 5.3.2]. *Let Γ be an n-dimensional interpretation of an L-structure M in the L'-structure N. There exists a map $\phi \mapsto \phi_\Gamma$, extending the map of Definition 1.2.2(2), such that for every L-formula $\phi(x_1, \dots, x_m)$ and all $\bar{a}_i \in \partial_\Gamma(N^n)$, we have that*

$$M \models \phi(f_\Gamma(\bar{a}_1), \dots, f_\Gamma(\bar{a}_m)) \Longleftrightarrow N \models \phi_\Gamma(\bar{a}_1, \dots, \bar{a}_m).$$

Proof. We describe how $\phi \mapsto \phi_\Gamma$ is built, for completeness (omitting details). By [Hodges 1993, Corollary 2.6.2], every L-formula is equivalent to one in which all atomic subformulas are unnested. One can then construct $\phi \mapsto \phi_\Gamma$ by induction on the complexity of formulas. The base case is handled by Definition 1.2.2(2). This definition extends inductively according to the following rules:

(1) $(\neg\phi)_\Gamma = \neg(\phi)_\Gamma$.

(2) $\left(\bigwedge_{i=1}^n \phi_i\right)_\Gamma = \bigwedge(\phi_i)_\Gamma$.

(3) $(\forall\phi)_\Gamma = \forall x_1, \dots, x_n(\partial_\Gamma(x_1, \dots, x_n) \to \phi_\Gamma)$.

(4) $(\exists\phi)_\Gamma = \exists x_1, \dots, x_n(\partial_\Gamma(x_1, \dots, x_n) \wedge \phi_\Gamma)$.

The resulting map satisfies the desired conditions of Proposition 1.2.3. □

Definition 1.2.4. The map $\mathrm{Form}_L \to \mathrm{Form}_{L'} : \phi \mapsto \phi_\Gamma$ constructed in the proof of Proposition 1.2.3 is called the *reduction* map of the interpretation Γ.

1.2.5. *Complexity of interpretations.* The complexity of the defining formulas of an interpretation defines a measure of complexity of the interpretation itself:

Definition 1.2.6 [Hodges 1993, Section 5.4(a)]. An interpretation Γ of an L-structure M in an L'-structure N is quantifier-free if the defining formulas of Γ are quantifier-free. Other syntactic variants are defined analogously (e.g., existential interpretation).

Remark 1.2.7. (a) The reduction map of a positive existential interpretation sends positive existential formulas to positive existential formulas.

(b) The reduction map of an existential interpretation sends *positive existential* formulas to existential formulas but does *not* necessarily send existential formulas to existential formulas.

Lemma 1.2.8. *If the L-structure M is $\exists^+$-interpretable in the L'-structure N and N is $\exists^+$-interpretable in the L''-structure P, then the composite interpretation of M in P is also an $\exists^+$-interpretation.*

Proof. Clear. □

1.2.9. *Recursive interpretations.*

Definition 1.2.10 [Hodges 1993, Remark 4, page 215]. Suppose L is a recursive language. Let Γ be an interpretation of an L-structure M in the L'-structure N. We say that the interpretation Γ is *recursive* if the map $\phi \mapsto \phi_\Gamma$ on unnested atomic formulas is recursive.

Remark 1.2.11 [Hodges 1993, Remark 4, page 215]. If Γ is a recursive interpretation of an L-structure M in the L'-structure N, then the reduction map of Γ is also recursive.

1.2.12. *Uniformly recursive interpretations.*

Definition 1.2.13. Suppose L and L' are languages. Let $(M_n)_{n\in\omega}$ be a sequence of L-structures and $(N_n)_{n\in\omega}$ be a sequence of L'-structure. For each $n \in \mathbb{N}$, let Γ_n be an interpretation of M_n in N_n. We say that the sequence of interpretations $(\Gamma_n)_{n\in\omega}$ is *uniformly recursive* if the sequence of reduction maps $(\phi \mapsto \phi_{\Gamma_n})_{n\in\omega}$ on unnested atomic formulas is uniformly recursive, i.e., if the map $(n, \phi) \mapsto \phi_{\Gamma_n}$ is recursive.

If an L-structure M is interpretable in the L'-structure N and the latter is decidable, then so is the former. It is not hard to prove the following uniform version:

Proposition 1.2.14. *Suppose L is a recursive language, $(M_n)_{n\in\omega}$ a sequence of L-structures and N is an L'-structure. Suppose N is decidable, Γ_n is an interpretation of M_n in N and the sequence of interpretations $(\Gamma_n)_{n\in\omega}$ is uniformly recursive. Then the sequence $(M_n)_{n\in\omega}$ is uniformly decidable.*

Proof. Rephrasing Proposition 1.2.3 for sentences, yields $\chi_{M_n}(\phi) = \chi_N(\phi_{\Gamma_n})$ for every $\phi \in \mathrm{Sent}_L$. It follows that the map $(n, \phi) \mapsto \chi_{M_n}(\phi)$ is equal to the map $(n, \phi) \mapsto \phi_{\Gamma_n} \mapsto \chi_N(\phi_{\Gamma_n})$ and the latter is recursive as a composition of recursive functions. □

If the interpretation of M in N is recursive and so is the interpretation of N in P, then the composite interpretation of M in P is recursive as well. Indeed, recursive functions are closed under composition. One also has a uniform version:

Lemma 1.2.15. *Let $(M_n)_{n\in\omega}$ be a sequence of L-structures, $(N_n)_{n\in\omega}$ be a sequence of L'-structures and $(P_n)_{n\in\omega}$ be a sequence of L''-structures. For each $n \in \mathbb{N}$, let Γ_n be an interpretation of M_n in N_n and Δ_n be an interpretation of N_n in P_n and suppose that the sequences of interpretations $(\Gamma_n)_{n\in\omega}$ and $(\Delta_n)_{n\in\omega}$ are uniformly recursive. Let E_n be the composite interpretation of M_n in P_n. Then the sequence of interpretations $(P_n)_{n\in\omega}$ is uniformly recursive.*

Proof. Clear. □

2. Ax–Kochen/Ershov in mixed characteristic

2.1. *A result by van den Dries.*

2.1.1. *Introduction.* We start with an Ax and Kochen/Ershov style result due to van den Dries (unpublished), which is briefly discussed on page 144 in [van den Dries 2014]. We shall sketch the proof (due to van den Dries), which does not seem to appear anywhere in the published literature. Some references, which use a similar *coarsening* argument, include [van den Dries 1999, page 2], [Anscombe and Jahnke 2022, proof of Corollary 12.3] and [Scanlon 2003, proof of Proposition 9.6]. For background material on coarsenings of valuations, see [van den Dries 2014, Section 7.4].

2.1.2. *Inverse systems.* The formalism of multisorted structures, used in this section, is spelled out in [Scanlon 2003, Section 3]. The proof of van den Dries' Theorem 2.1.5 requires a technical lemma for inverse systems, which we now discuss.

Let $\mathcal{R} = (R_n)_{n\in\omega}$ be a sequence of rings, viewed as a multisorted structure with sorts $(\boldsymbol{R}_n)_{n\in\omega}$, each equipped with the language of rings L_{rings}, and for each $n \in \mathbb{N}$ we have a map $f_n : \boldsymbol{R}_{n+1} \to \boldsymbol{R}_n$. Let T be the theory that requires of $\mathcal{R} = (R_n)_{n\in\omega}$ that the map $f_n : R_{n+1} \to R_n$ be a surjective ring homomorphism with $\operatorname{Ker}(f_n) = p^n R_{n+1}$, i.e., $R_n \cong R_{n+1}/p^n R_{n+1}$. If $\mathcal{R} = (R_n)_{n\in\omega}$ and $\mathcal{S} = (S_n)_{n\in\omega}$ are two models of T, they are isomorphic precisely when there is a *compatible* system $(\phi_n)_{n\in\omega}$ of isomorphisms $\phi_n : R_n \xrightarrow{\cong} S_n$, i.e., such that the diagram commutes

$$\begin{tikzcd}
R_{n+1} \arrow[r, "\phi_{n+1}"] \arrow[d, "f_n"] & S_{n+1} \arrow[d, "g_n"] \\
R_n \arrow[r, "\phi_n"] & S_n
\end{tikzcd}$$

for each $n \in \mathbb{N}$. Compatibility of the ϕ_n is essential as there are examples where $R_n \cong S_n$ for each $n \in \mathbb{N}$ but $\mathcal{R} \not\cong \mathcal{S}$ (see e.g., Remark 3.6.10). Somewhat surprisingly, compatibility comes for free in a saturated setting:

Lemma 2.1.3. *Assume* CH. *Let $\mathcal{R} = (R_n)_{n\in\omega}$ and $\mathcal{S} = (S_n)_{n\in\omega}$ be two models of T. Suppose that for each $n \in \mathbb{N}$, we have that $R_n \cong S_n$ and the rings R_n, S_n are saturated with $|R_n| = |S_n| \leq \aleph_1$. Then $\mathcal{R} \cong \mathcal{S}$.*

Proof. Let U be a nonprincipal ultrafilter on $\mathbb{N}$ and consider the ultraproducts $R_U = \prod_{n\in\omega} R_n/U$ and $S_U = \prod_{n\in\omega} S_n/U$.

Claim 1. $R_U \cong S_U$.

Proof. Since $R_n \equiv S_n$ for each $n \in \mathbb{N}$, we get that $R_U \equiv S_U$ by Łoś' s Theorem. For each $n \in \mathbb{N}$, let $\mathcal{F}_m = \{n \in \mathbb{N} : |R_n| \geq m\}$. If there exists $m \in \mathbb{N}$ with $\mathcal{F}_m \notin U$, then R_U and S_U are both finite and thus $R_U \cong S_U$. If on the other hand $\mathcal{F}_m \in U$ for all $m \in \mathbb{N}$, then R_U and S_U are both infinite. Since $|R_n| \leq \aleph_1$, we get that $|R_U| \leq \aleph_1^{\aleph_0} = 2^{\aleph_0^2} = 2^{\aleph_0} = \aleph_1$, using the continuum hypothesis (similarly $|S_U| \leq \aleph_1$). Moreover, the ultraproducts R_U and S_U are $\aleph_1$-saturated [Marker 2002, Exercise 4.5.37] and thus saturated of size

$\aleph_1$. Since R_U and S_U are elementary equivalent and both saturated of size $\aleph_1$, we conclude that $R_U \cong S_U$ [loc. cit., Theorem 4.3.20]. □

Next we prove:

Claim 2. For each $n \in \mathbb{N}$, we have $R_U/p^n R_U \cong R_n$.

Proof. Fix $n \in \mathbb{N}$. Since $R_m/p^n R_m \cong R_n$ for $m > n$, we get that $R_U/p^n R_U \equiv R_n$ in L_{rings} by Łoś Theorem. If R_n is finite, then $R_U/p^n R_U \cong R_n$ and we are done. Otherwise, we will have that R_n is saturated of size $\aleph_1$. The same is true for $R_U/p^n R_U$, being interpretable in the structure R_U, which is saturated of size $\aleph_1$ by CH (see the proof of Claim 1). We conclude that $R_U/p^n R_U \cong R_n$ [loc. cit., Theorem 4.3.20]. □

Similarly, for each $n \in \mathbb{N}$, we have $S_U/p^n S_U \cong S_n$. By Claim 1, we obtain $\phi : R_U \xrightarrow{\cong} S_U$. Note that $\phi(p^n R_U) = p^n S_U$, for each $n \in \mathbb{N}$. By Claim 2, this gives rise to a *compatible* system $(\phi_n)_{n\in\omega}$ of isomorphisms $\phi_n : R_n \xrightarrow{\cong} S_n$, which yields $\mathcal{R} \xrightarrow{\cong} \mathcal{S}$. □

2.1.4. *Statement and proof.* The following result will be of fundamental importance for the rest of the paper:

Theorem 2.1.5 (van den Dries). *Let (K, v), (K', v') be two henselian valued fields of mixed characteristic. Then $(K, v) \equiv (K', v')$ in L_{val} if and only if $\mathcal{O}_v/p^n\mathcal{O}_v \equiv \mathcal{O}_{v'}/p^n\mathcal{O}_{v'}$ in L_{rings} for all $n \in \mathbb{N}$ and $(\Gamma_v, vp) \equiv (\Gamma_{v'}, v'p)$ in L_{oag} together with a constant for vp.*

Proof. $\Rightarrow$: Clear.

$\Leftarrow$: As the statement at hand is *absolute*, we may assume the continuum hypothesis; see [Scanlon 2003, Section 8] or [van den Dries 2014, page 122]. We may therefore assume that both (K, v) and (K', v') are saturated of size $\aleph_1$ [Marker 2002, Corolllary 4.3.13]. By our assumption, we have an isomorphism of ordered abelian groups $(\Gamma_v, vp) \cong (\Gamma_{v'}, v'p)$ and a ring isomorphism $\mathcal{O}_{v'}/p^n\mathcal{O}_{v'} \cong \mathcal{O}_v/p^n\mathcal{O}_v$ for each $n \in \mathbb{N}$. We shall argue that $(K, v) \cong (K', v')$.

Consider the finest coarsening w of v for which the associated residue field k_w has characteristic 0. The corresponding valuation ring is $\mathcal{O}_w = \mathcal{O}_v\big[\frac{1}{p}\big]$ and the corresponding value group is $\Gamma_w = \Gamma_v/\operatorname{Conv}(\mathbb{Z}vp)$, where $\operatorname{Conv}(\mathbb{Z}vp)$ is the convex hull of $\mathbb{Z}vp$ in Γ_v. Let $\bar{v}$ be the induced valuation from v on the residue field k_w. We then have that $\mathcal{O}_{\bar{v}} = \mathcal{O}_v/\bigcap_{n\in\omega} p^n\mathcal{O}_v$. We also consider the analogous objects for K'.

Claim 1. We have a ring isomorphism $\mathcal{O}_{\bar{v}} \cong \varprojlim \mathcal{O}_v/p^n\mathcal{O}_v$.

Proof. Consider the ring homomorphism $f : \mathcal{O}_{\bar{v}} \to \varprojlim \mathcal{O}_v/p^n\mathcal{O}_v : x + \bigcap_{n\in\omega} p^n\mathcal{O}_v \mapsto (x + p^n\mathcal{O}_v)_{n\in\omega}$, which is clearly injective. We shall argue that it is also surjective. For a given $(x_n + p^n\mathcal{O}_v)_{n\in\omega} \in \varprojlim \mathcal{O}_v/p^n\mathcal{O}_v$, we may find $x \in \mathcal{O}_v$ with $x \equiv x_n \mod p^n\mathcal{O}_v$, using that $\mathcal{O}_v$ is $\aleph_1$-saturated. It follows that $f(x) = (x_n + p^n\mathcal{O}_v)_{n\in\omega}$. □

Similarly, one obtains an isomorphism $\mathcal{O}_{\overline{v'}} \cong \varprojlim \mathcal{O}_{v'}/p^n\mathcal{O}_{v'}$.

Claim 2. We have an isomorphism of valued fields $\phi : (k_w, \bar{v}) \cong (k_{w'}, \overline{v'})$.

Proof. Let $\mathcal{R} = (\mathcal{O}_v/p^n\mathcal{O}_v)_{n\in\omega}$ and $\mathcal{S} = (\mathcal{O}_{v'}/p^n\mathcal{O}_{v'})_{n\in\omega}$. Then $\mathcal{R} \cong \mathcal{S}$ by Lemma 2.1.3. This yields $\varprojlim \mathcal{O}_v/p^n\mathcal{O}_v \cong \varprojlim \mathcal{O}_{v'}/p^n\mathcal{O}_{v'}$ and thus $\mathcal{O}_{\bar{v}} \cong \mathcal{O}_{\overline{v'}}$ by Claim 1. □

We also have that $\Gamma_w \cong \Gamma_{w'}$, since the isomorphism $(\Gamma_v, vp) \cong (\Gamma_{v'}, v'p)$ descends to the quotients $\Gamma_v/\operatorname{Conv}(\mathbb{Z}vp) \cong \Gamma_{v'}/\operatorname{Conv}(\mathbb{Z}v'p)$. By [van den Dries 2014, Lemma 7.13], the coarsened valued fields (K, w) and (K', w') are henselian too. By the Ax–Kochen/Ershov principle in pure characteristic 0 (see, e.g., [van den Dries 2014, Corollary 5.22]), we get that $(K, w) \equiv (K', w')$ in L_{val}.

Passing once again to elementary extensions, in a suitable language that includes unary predicates for both $\mathcal{O}_v$ and $\mathcal{O}_w$, we may even assume that $(K, w) \cong (K', w')$ to begin with. By stable embeddedness of residue fields for henselian valued fields of pure characteristic 0 (see [van den Dries 2014, Corollary 5.25]), there is even an isomorphism $\Phi : (K, w) \xrightarrow{\cong} (K', w')$ inducing $\phi : (k_w, \bar{v}) \xrightarrow{\cong} (k_{w'}, \bar{v}')$.

Claim 3. The map Φ is an isomorphism of the valued fields (K, v) and (K', v').

Proof. Given $x \in K$, we need to show that $vx \geq 0 \Longleftrightarrow v'(\Phi(x)) \geq 0$. If $vx \geq 0$, then either (i) $wx > 0$ or (ii) $wx = 0$ and $\bar{v}\bar{x} \geq 0$, where $\bar{x} \in k_v$ is the image of x via $\operatorname{res}_w : \mathcal{O}_w \to k_w$. In the first case, we get that $w'(\Phi(x)) > 0$ as $\Phi : (K, w) \to (K', w')$ is a valued field homomorphism and therefore $v'(\Phi(x)) > 0$ as $\mathfrak{m}_{w'} \subset \mathfrak{m}_{v'}$. Suppose now that $wx = 0$ and $\bar{v}\bar{x} \geq 0$. Then we also get that $w'(\Phi(x)) = 0$ and $\bar{v}'(\phi(\bar{x})) \geq 0$ as $\phi : (k_w, \bar{v}) \to (k_{w'}, \bar{v}')$ is a valued field homomorphism. Since Φ induces ϕ, we get that $\bar{v}'(\overline{\Phi(x)}) = \bar{v}'(\phi(\bar{x})) \geq 0$ and conclude that $v'(\Phi(x)) \geq 0$. □

Claim 3 finishes the proof. □

2.2. *Existential AKE in mixed characteristic.* In this section we prove an existential version of Theorem 2.1.5. We first review some known AKE results in the equal characteristic setting.

2.2.1. *Comparison with the equal characteristic case.* For equal characteristic henselian valued fields one has the following simple Ax–Kochen/Ershov principles due to Anscombe and Fehm:

Theorem 2.2.2 [Anscombe and Fehm 2016, Corollary 1.2]. *Let (K, v), (K', v') be two equal characteristic nontrivially valued henselian fields. Then $(K, v) \equiv_\exists (K', v')$ in L_{val} if and only if $k \equiv_\exists k'$ in L_{rings}.*

Theorem 2.2.3 [Anscombe and Fehm 2016, Corollary 7.5]. *Let (K, v) be an equal characteristic henselian valued field. Then $Th_\exists(K, v)$ is decidable in L_{val} if and only if $Th_\exists(k)$ is decidable in L_{rings}.*

Remark 2.2.4. In residue characteristic 0, Theorems 2.2.2 and 2.2.3 were essentially known by work of Ax and Kochen/Ershov prior to the work of Anscombe and Fehm [2016, Remark 7.3].

2.2.5. *Existential AKE in mixed characteristic.* In mixed characteristic, one can easily construct counterexamples of Theorems 2.2.2 and 2.2.3; see [Anscombe and Fehm 2016, Remark 7.6]. It is then natural to ask what an existential AKE principle in mixed characteristic would look like. This will be Theorem 2.2.6 below, whose proof follows closely the proof of Theorem 2.1.5.

We write $\mathfrak{m}_n$ for the maximal ideal of $\mathcal{O}_v/p^n\mathcal{O}_v$ and $(\mathcal{O}_v/p^n\mathcal{O}_v, \mathfrak{m}_n)$ for the local ring, viewed as an L_{lcr}-structure (see notation).

Theorem 2.2.6. *Let (K, v), (K', v') be two henselian valued fields of mixed characteristic. Then the following are equivalent*:

(1) $(K, v) \equiv_{\exists} (K', v')$ *in* L_{val}.

(2) $\mathcal{O}_v/p^n\mathcal{O}_v \equiv_{\exists} \mathcal{O}_{v'}/p^n\mathcal{O}_{v'}$ *in* L_{rings} *for all* $n \in \mathbb{N}$.

(3) $(\mathcal{O}_v/p^n\mathcal{O}_v, \mathfrak{m}_n) \equiv_{\exists^+} (\mathcal{O}_{v'}/p^n\mathcal{O}_{v'}, \mathfrak{m}'_n)$ *in* L_{lcr} *for all* $n \in \mathbb{N}$.

Proof. (1) $\Rightarrow$ (2), (3): Clear.

(2) $\Rightarrow$ (1): By symmetry, it will suffice to show that $(K, v) \models \text{Th}_{\exists}(K', v')$. We may further assume (K', v') is countable by downward Löwenheim and Skolem and that (K, v) is $\aleph_1$-saturated.

We again consider the valuations w, $\bar{v}$ (resp. w', $\overline{v'}$) that were introduced in the proof of Theorem 2.1.5. By our assumption, we have for each $n \in \mathbb{N}$ an embedding of rings $\mathcal{O}_{v'}/p^n\mathcal{O}_{v'} \hookrightarrow \mathcal{O}_v/p^n\mathcal{O}_v$.

Claim. There is an injective ring embedding $\phi : \mathcal{O}_{\bar{v}'} \hookrightarrow \mathcal{O}_{\bar{v}}$.

Proof. Let us fix an enumeration of $\mathcal{O}_{v'}$, say $\mathcal{O}_{v'} = (a_i)_{i\in\mathbb{N}}$. Consider the set of formulas in countably many variables $x = (x_n)_{n\in\omega}$ of the form

$$\Sigma(x) = \{x_i \diamond x_j = x_k(p^n), x_m \Box x_\rho(p^n) : a_i \in \mathcal{O}_{v'}, a_i \diamond a_j = a_k(p^n), a_m \Box a_\rho(p^n)\}$$

where $\diamond$ is either $+$ or $\cdot$ and $\Box$ is either $=$ or $\neq$. Since for each $n \in \mathbb{N}$ we have an embedding of rings $\mathcal{O}_{v'}/p^n\mathcal{O}_{v'} \hookrightarrow \mathcal{O}_v/p^n\mathcal{O}_v$, we get that $\Sigma(x)$ is finitely satisfiable. The ring $\mathcal{O}_v$ is $\aleph_1$-saturated and we thus have $b = (b_n)_{n\in\omega}$ with $b \models \Sigma(x)$. Using that $\mathcal{O}_{\bar{v}} = \mathcal{O}_v / \bigcap_{n\in\omega} p^n\mathcal{O}_v$ (resp. $\mathcal{O}_{\overline{v'}} = \mathcal{O}_{v'} / \bigcap_{n\in\omega} p^n\mathcal{O}_{v'}$), one readily checks that the map $\mathcal{O}_{v'} \to \mathcal{O}_v : a_i \mapsto b_i$ descends to a ring embedding $\mathcal{O}_{\bar{v}'} \hookrightarrow \mathcal{O}_{\bar{v}}$. □

The claim provides us with a valued field embedding $\phi : (k_{w'}, \bar{v}') \hookrightarrow (k_w, \bar{v})$. By the existential Ax–Kochen/Ershov principle in pure characteristic 0 (see Theorem 2.2.2 and Remark 2.2.4), we get that $(K, w) \models \text{Th}_{\exists}(K', w')$. Replacing K with an $\aleph_1$-saturated extension in a suitable language that includes unary predicates for both $\mathcal{O}_v$ and $\mathcal{O}_w$, we will also have an embedding $(K', w') \hookrightarrow (K, w)$.

By the relative embedding property for equal characteristic 0 henselian valued fields (see in [Kuhlmann 2016, Theorem 7.1] for a more general statement), we can even find $\Phi : (K', w') \hookrightarrow (K, w)$ that induces $\phi : (k_{w'}, \bar{v}') \hookrightarrow (k_w, \bar{v})$. Finally, we get that the map $\Phi : (K', v') \hookrightarrow (K, v)$ is an embedding of valued fields, as in the proof of Claim 3, Theorem 2.1.5.

(3) $\Rightarrow$ (2): For $f(x_1, \dots, x_m) \in \mathbb{Z}[x_1, \dots, x_m]$ and $(a_1, \dots, a_m) \in \mathcal{O}_v^m$, note that $f(a_1, \dots, a_m) \neq 0 \bmod p^n\mathcal{O}_v$ if and only if there exists $y \in \mathfrak{m}_v$ such that $f(a_1, \dots, a_m) \cdot y = p^n \bmod p^{n+1}\mathcal{O}_v$ (similarly for $\mathcal{O}_{v'}$). Consequently, for each $n \in \mathbb{N}$, we see that if $(\mathcal{O}_v/p^{n+1}\mathcal{O}_v, \mathfrak{m}_{n+1}) \equiv_{\exists^+} (\mathcal{O}_{v'}/p^{n+1}\mathcal{O}_{v'}, \mathfrak{m}'_{n+1})$ in L_{lcr}, then $\mathcal{O}_v/p^n\mathcal{O}_v \equiv_{\exists} \mathcal{O}_{v'}/p^n\mathcal{O}_{v'}$ in L_{rings}. □

2.3. ***Decidability.*** We now harvest the consequences of Theorems 2.1.5 and 2.2.6 in relation to decidability. Since the countable union of recursive sets is not guaranteed to be recursive, we need to ask not only that each individual $\mathcal{O}_K/(p^n)$ be decidable in L_{rings} but also that the sequence $(\mathcal{O}_K/(p^n))_{n\in\omega}$ be *uniformly decidable* in L_{rings}:

Corollary 2.3.1. *Let (K, v) be a henselian valued field of mixed characteristic. Then the following are equivalent*:

(1) *The valued field (K, v) is decidable in L_{val}.*

(2) *The sequence $(\mathcal{O}_K/(p^n))_{n\in\omega}$ is uniformly decidable in L_{rings} and (Γ_v, vp) is decidable in L_{oag} with a constant for vp.*

Proof. (1) $\Rightarrow$ (2): Clear.

(2) $\Rightarrow$ (1): The identification $\Gamma_v = K^\times/\mathcal{O}^\times$ furnish us with a recursive interpretation E of (Γ_v, vp) in the valued field (K, v). Let also E_n be the natural interpretation of $\mathcal{O}_K/(p^n)$ in the L_{val}-structure (K, v), for each $n \in \mathbb{N}$. If $g_n : \mathrm{Sent}_{L_{\mathrm{rings}}} \to \mathrm{Sent}_{L_{\mathrm{val}}}$ denotes the reduction map of E_n, then one can see that the sequence $(g_n)_{n\in\omega}$ is uniformly recursive (using that E_n is uniform in $n \in \mathbb{N}$). Let

$$\Sigma := \mathrm{Hen}_{(0,p)} \cup \Bigl(\bigcup_{n\in\omega} \{\phi_{E_n} : \mathcal{O}_K/(p^n) \models \phi\} \Bigr) \cup \{\phi_E : (\Gamma_v, vp) \models \phi\}$$

where $\mathrm{Hen}_{(0,p)}$ is a first-order axiom schema capturing Hensel's lemma (see, e.g., [Kuhlmann 2016, page 21]), together with a set of sentences capturing that the valued field has mixed characteristic $(0, p)$.

Claim. The axiomatization Σ is r.e.

Proof. The set $\mathrm{Hen}_{(0,p)}$ is clearly r.e. The set $\{\phi_E : (\Gamma_v, vp) \models \phi\} \subseteq L_{\mathrm{val}}$ is r.e., being the image of a recursive set via the recursive reduction map of E. Since recursively enumerable sets are closed under finite unions, it remains to show that $\bigcup_{n\in\omega}\{\phi_{E_n} : \mathcal{O}_K/(p^n) \models \phi\}$ is r.e.

Let $\chi : \mathbb{N} \times \mathrm{Sent}_{L_{\mathrm{rings}}} \to \mathbb{N}$ be the recursive function associated to the uniformly decidable sequence $(\mathcal{O}_K/(p^n))_{n\in\omega}$. We construct the partial recursive function $\chi' : \mathbb{N} \times \mathrm{Sent}_{L_{\mathrm{rings}}} \to \mathbb{N} \times \mathrm{Sent}_{L_{\mathrm{rings}}}$ which maps $(n, \phi) \mapsto (n, \phi)$ if $\chi(n, \phi) = 1$ and is undefined if $\chi(n, \phi) = 0$. Consider also the recursive function $g : \mathbb{N} \times \mathrm{Sent}_{L_{\mathrm{rings}}} \to \mathrm{Sent}_{L_{\mathrm{val}}} : (n, m) \mapsto g_n(m)$ associated to the uniformly recursive sequence $(g_n)_{n\in\omega}$. Observe that $\bigcup_{n\in\omega}\{\phi_{E_n} : \mathcal{O}_K/(p^n) \models \phi\} = \mathrm{Im}(F)$ where F is the (partial) recursive function $F = g \circ \chi'$. It follows that $\bigcup_{n\in\omega}\{\phi_{E_n} : \mathcal{O}_K/(p^n) \models \phi\}$ is r.e. □

If $(K', v') \models \Sigma$, then $(K', v') \equiv (K, v)$ in L_{val} by Theorem 2.1.5. We therefore get that Σ is a complete axiomatization of (K, v). We conclude that the L_{val}-theory of (K, v) admits a r.e. and complete axiomatization, whence (K, v) is decidable. □

Corollary 2.3.2. *Let (K, v) be a henselian valued field of mixed characteristic. Then the following are equivalent*:

(1) *The valued field (K, v) is $\exists$-decidable in L_{val}.*

(2) *The sequence $(\mathcal{O}_K/(p^n))_{n\in\omega}$ is uniformly $\exists$-decidable in L_{rings}.*

(3) *The sequence $((\mathcal{O}_K/(p^n), \mathfrak{m}_n)_{n\in\omega}$ is uniformly $\exists^+$-decidable in L_{lcr}.*

Proof. Similar to Corollary 2.3.1, ultimately using Theorem 2.2.6. □

3. Perfectoid fields

3.1. *Introduction.*

3.1.1. *Motivation.* The theory of perfectoid fields (and spaces), introduced by Scholze [2012], was initially designed as a means of transferring results available in positive characteristic to mixed characteristic; see [Scholze 2014, Section 1]. It formalizes the earlier Krasner–Kazhdan–Deligne philosophy (due to Krasner [1957], Kazhdan [1986] and Deligne [1984]), of approximating a *highly ramified* mixed characteristic field with a positive characteristic field. Within the framework of perfectoid fields, this kind of approximation becomes precise and robust with the use of the tilting functor (see Section 3.2).

All this is substantially different from the Ax–Kochen method (see, e.g., [van den Dries 2014, 2.20]), which achieves a model-theoretic transfer principle *asymptotically*, i.e., with the residue characteristic $p \to \infty$. The theory of perfectoid fields will allow us to transport decidability information for a fixed residue characteristic (but with high ramification), setting the stage for a different type of model-theoretic transfer principle.

3.1.2. *Definition.*

Definition 3.1.3. A perfectoid field is a complete valued field (K, v) of residue characteristic $p > 0$ such that Γ_v is a dense subgroup of $\mathbb{R}$ and the Frobenius map $\Phi : \mathcal{O}_K/(p) \to \mathcal{O}_K/(p) : x \mapsto x^p$ is surjective.

Example 3.1.4. (a) The p-adic completions of $\mathbb{Q}_p(p^{1/p^\infty})$, $\mathbb{Q}_p(\zeta_{p^\infty})$ and $\mathbb{Q}_p^{ab}$ are mixed characteristic perfectoid fields.

(b) The t-adic completions of $\mathbb{F}_p((t))^{1/p^\infty}$ and $\overline{\mathbb{F}}_p((t))^{1/p^\infty}$ are perfectoid fields of characteristic p.

Remark 3.1.5. In characteristic p, a perfectoid field is simply a perfect, complete nonarchimedean valued field of rank 1.

3.2. *Tilting.*

3.2.1. *Introduction.* A construction, originally due to Fontaine, provides us with a tilting functor that takes any perfectoid field K and transforms it into a perfectoid field $K^\flat$ of characteristic p. We shall now describe this tilting functor. For more details, see [Scholze 2012, Section 3].

3.2.2. *Definition.* Given a perfectoid field (K, v), we shall now define its tilt $(K^\flat, v^\flat)$. Let $\varprojlim_{x \mapsto x^p} K$ be the limit of the inverse system

$$\cdots \xrightarrow{x \mapsto x^p} K \xrightarrow{x \mapsto x^p} K \xrightarrow{x \mapsto x^p} K$$

which is identified as $\varprojlim_{x \mapsto x^p} K = \{(x_n)_{n\in\omega} : x_{n+1}^p = x_n\}$, viewed as a multiplicative monoid via $(x_n)_{n\in\omega} \cdot (y_n)_{n\in\omega} = (x_n \cdot y_n)_{n\in\omega}$. Similarly, one can define the multiplicative monoid $\varprojlim_{x \mapsto x^p} \mathcal{O}_K$.

Let $\varpi \in \mathcal{O}_K$ be such that $0 < v\varpi \le vp$ (e.g., $\varpi = p$ when $\mathrm{char}(K) = 0$ and $\varpi = 0$ when $\mathrm{char}(K) = p$) and consider the ring $\varprojlim_\Phi \mathcal{O}_K/(\varpi)$ which is the limit of the inverse system of rings

$$\cdots \xrightarrow{\Phi} \mathcal{O}_K/(\varpi) \xrightarrow{\Phi} \mathcal{O}_K/(\varpi) \xrightarrow{\Phi} \mathcal{O}_K/(\varpi)$$

where $\Phi : \mathcal{O}_K/(\varpi) \to \mathcal{O}_K/(\varpi) : x \mapsto x^p$ is the Frobenius homomorphism.

Lemma 3.2.3 [Scholze 2012, Lemma 3.4(i) and (ii)]. (a) *The ring* $\varprojlim_{\Phi} \mathcal{O}_K/(\varpi)$ *is independent of the choice of* ϖ *and there is a multiplicative isomorphism* $\varprojlim_{x \mapsto x^p} \mathcal{O}_K \xrightarrow{\cong} \varprojlim_{\Phi} \mathcal{O}_K/(\varpi)$. *Moreover, we get a multiplicative morphism* $\sharp : \varprojlim_{\Phi} \mathcal{O}_K/(\varpi) \to \mathcal{O}_K : x \mapsto x^\sharp$ *such that if* $x = (x_n + (\varpi))_{n\in\omega}$, *then* $x^\sharp \equiv x_0 \bmod (\varpi)$.

(b) *There is an element* $\varpi^\flat \in \varprojlim_{\Phi} \mathcal{O}_K/(\varpi)$ *with* $v(\varpi^\flat)^\sharp = v\varpi$.

The definition of $\sharp$ goes as follows: Let $x = (x_n)_{n\in\omega} \in \varprojlim_{\Phi} \mathcal{O}_K/(\varpi)$, i.e., $x_n \in \mathcal{O}_K/(\varpi)$ and $x_{n+1}^p = x_n$. Let $\tilde{x}_n \in \mathcal{O}_K$ be an arbitrary lift of $x_n \in \mathcal{O}_K/(\varpi)$. Then the limit $\lim_{n\to\infty} \tilde{x}_n^{p^n}$ exists and is independent of the choice of the $\tilde{x}_n$; see [Scholze 2012, Lemma 3.4(i)]. We define $x^\sharp := \lim_{n\to\infty} \tilde{x}_n^{p^n}$.

We now introduce $K^\flat := \varprojlim_{\Phi} \mathcal{O}_K/(\varpi)[(\varpi^\flat)^{-1}]$. A priori this is merely a ring. It is in fact a valued field according to the following:

Lemma 3.2.4 [Scholze 2012, Lemma 3.4(iii)]. (a) *There is a morphism of multiplicative monoids* $K^\flat \to K : x \mapsto x^\sharp$ (*extending the one of Lemma 3.2.3*(*a*)), *which induces a morphism of multiplicative monoids* $K^\flat \xrightarrow{\cong} \varprojlim_{x\mapsto x^p} K : x \mapsto (x^\sharp, (x^\sharp)^{1/p}, \ldots)$. *The map* $v^\flat : K^\flat \to \Gamma_v \cup \{\infty\} : x \mapsto vx^\sharp$ *is a valuation on* $K^\flat$, *which makes* $(K^\flat, v^\flat)$ *into a perfectoid field of characteristic* p. *If* $\mathcal{O}_{K^\flat}$ *is the valuation ring of* $K^\flat$, *then we have a ring isomorphism* $\mathcal{O}_{K^\flat} \cong \varprojlim_{\Phi} \mathcal{O}_K/(\varpi)$.

(b) *We have an isomorphism of ordered abelian groups* $(\Gamma_v, v\varpi) \cong (v^\flat K^\flat, v^\flat \varpi^\flat)$ *and a field isomorphism* $k_v \cong k_{v^\flat}$. *Moreover, we have a ring isomorphism* $\mathcal{O}_K/(\varpi) \cong \mathcal{O}_{K^\flat}/(\varpi^\flat)$.

Remark 3.2.5. Lemma 3.2.4(a) allows us to identify the multiplicative underlying monoid of $K^\flat$ with $\varprojlim_{x\mapsto x^p} K$. It is not hard to see that, via this identification, addition is described by $(x_n)_{n\in\omega} + (y_n)_{n\in\omega} = (z_n)_{n\in\omega}$, where $z_n = \lim_{m\to\infty}(x_{n+m} + y_{n+m})^{p^m}$.

Definition 3.2.6. We say that the valued field $(K^\flat, v^\flat)$ constructed in Lemma 3.2.4(a) is the tilt of the perfectoid field (K, v).

Remark 3.2.7 [Scholze 2012, Lemma 3.4(iv)]. If (K, v) is a perfectoid field of characteristic p, then $(K^\flat, v^\flat) \cong (K, v)$.

Example 3.2.8 (see Corollary 4.4.3). In the examples below, $\widehat{K}$ stands for the p-adic (resp. t-adic) completion of the field K depending on whether its characteristic is 0 or p:

(a) $\widehat{\mathbb{Q}_p(p^{1/p^\infty})}^\flat \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$ and $t^\sharp = p$.

(b) $\widehat{\mathbb{Q}_p(\zeta_{p^\infty})}^\flat \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$ and $(t+1)^\sharp = \zeta_p$.

(c) $\widehat{\mathbb{Q}_p^{ab}}^\flat \cong \widehat{\overline{\mathbb{F}}_p((t))^{1/p^\infty}}$ and $(t+1)^\sharp = \zeta_p$.

Remark 3.2.9. The tilting construction makes sense for nonperfectoid fields as well. However, in the absence of infinite wild ramification, it is too lossy for it to be useful (e.g., $\mathbb{Q}_p^\flat = \mathbb{F}_p$).

3.3. ***Witt vectors.*** We review the basics of Witt vectors. Details and proofs can be found in [Serre 1979, Sections 5 and 6; Kedlaya and Liu 2015, Section 3; van den Dries 2014, Section 6].

3.3.1. *p-rings.*

Definition 3.3.2. A ring R of characteristic p is called perfect if the Frobenius homomorphism $\Phi : R \to R$, $x \mapsto x^p$ is bijective.

Definition 3.3.3. (a) A p-ring is a commutative ring A provided with a filtration $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ such that $\mathfrak{a}_n \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ and so that A is Hausdorff and complete with respect to the topology induced by the filtration and $A/\mathfrak{a}_1$ is a perfect ring of characteristic p.

(b) If in addition $\mathfrak{a}_n = p^n A$ and p is not a zero-divisor, then we say that A is a strict p-ring.

If A is a p-ring, we call the quotient ring A/pA the *residue ring* of the p-ring A and write res : $A \to A/pA$ for the quotient map. A system of *multiplicative representatives* (or simply a system of representatives) is a multiplicative homomorphism $f_A : A/pA \to A$ such that $f_A(\text{res}(x)) = x$. A p-ring A always has a system of representatives $f_A : A/pA \to A$ and when A is strict every element $a \in A$ can be written uniquely in the form $a = \sum_{i=0}^{\infty} f_A(\alpha_i) \cdot p^i$ [Serre 1979, page 37].

Theorem 3.3.4 [Serre 1979, Corollary page 39]. *For every perfect ring R, there exists a unique strict p-ring, denoted by $W(R)$, with residue ring $W(R)/pW(R) \cong R$.*

The ring $W(R)$ is said to be the *ring of Witt vectors* over the ring R. The uniqueness part of Theorem 3.3.4 follows from the next result, which we record here for later use.

Fact 3.3.5 [Kedlaya and Liu 2015, Lemma 3.3.2]. Let A be a strict p-ring and $f_A : A/pA \to A$ be a system of representatives. Let A' be a p-adically complete ring and $\phi : A/pA \to A'/pA'$ be a ring homomorphism. Then there exists a unique ring homomorphism $g : A \to A'$ making the diagram below commute:

$$\begin{tikzcd}
A \arrow[r, "g"] \arrow[d] & A' \arrow[d] \\
A/pA \arrow[r, "\phi"] & A'/pA'
\end{tikzcd}$$

where the vertical arrows are the projections modulo p. More precisely, there exists a unique lift $\phi : A/pA \to A'/pA'$ to a multiplicative map $\tilde{\phi} : A/pA \to A'$ and we have $g\big(\sum_{i=0}^{\infty} f_A(\alpha_i) \cdot p^i\big) = \sum_{i=0}^{\infty} \tilde{\phi}(\alpha_i) \cdot p^i$.

3.3.6. *Teichmüller representatives.* There is a system of *Teichmüller representatives* of R in $W(R)$. This is the (unique) multiplicative homomorphism $[\ ] : R \to W(R)$ with the property that $\text{res}([x]) = x$ for all $x \in R$. Explicitly, for $x \in R$ and $n \in \mathbb{N}$, let $x_n \in R$ be such that $x_n^{p^n} = x$ and $\tilde{x}_n \in W(R)$ be an arbitrary lift of x_n. The sequence $(\tilde{x}_n^{p^n})_{n \in \omega}$ is a Cauchy sequence, whose limit is independent of the chosen lifts. We let $[x] := \lim_{n\to\infty} \tilde{x}_n^{p^n}$; see [Serre 1979, Proposition 8 page 35].

It is easy to see that any element $x \in W(R)$ can be written *uniquely* in the form $x = \sum_{n=0}^{\infty} [x_n] \cdot p^n$, for some $x_i \in R$. The vector $(x_0, x_1, \dots) \in R^{\omega}$ is called the *Teichmüller vector* of x.

3.3.7. *Witt vectors.* The advantage of Witt vectors over Teichmüller vectors, comes from the fact that the ring operations in $W(R)$ have nicer coordinatewise descriptions when using the former (see Section 3.3.8). Write $x \in W(R)$ in the form $x = \sum_{n=0}^{\infty}[x_n^{p^{-n}}] \cdot p^n$, for some $x_i \in R$. The vector $(x_0, x_1, \dots) \in R^{\omega}$ is called the *Witt vector* of x.

3.3.8. *Ring operations.* By the discussion above, the ring $W(R)$ can be thought of as the p-adic analogue of formal power series with coefficients in R. By identifying x with its Witt vector, we see that $W(R)$ has R^{ω} as its underlying set. By [van den Dries 2014, Lemma 6.5], the ring operations are given by

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \dots)$$

and

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \dots)$$

for suitable polynomials $S_i, P_i \in \mathbb{Z}[x_0, \dots, x_i, y_0, \dots, y_i]$ which are universal, in the sense that they do not depend on R.

Observation 3.3.9. The polynomials S_i (resp. P_i) are *computable*, i.e., the function $\mathbb{N} \to \mathbb{Z}[x_0, y_0, \dots]$, $n \mapsto S_n$ (resp. $\mathbb{N} \to \mathbb{Z}[x_0, y_0, \dots]$, $n \mapsto P_n$) is recursive.

Proof. For $n \in \mathbb{N}$, we introduce the n-th Witt polynomial $W_n(x_0, \dots, x_n) = x_0^{p^n} + px_1^{p^{n-1}} + \dots + p^n \cdot x_n \in \mathbb{Z}[x_0, \dots, x_n]$ [van den Dries 2014, page 135]. The proof of [van den Dries 2014, Lemma 6.5] shows that

$$S_0(x_0, y_0) = x_0 + y_0$$

and

$$W_{n-1}(S_0^p, \dots, S_{n-1}^p) + p^n \cdot S_n = W_{n-1}(S_0(x_0^p, y_0^p), \dots, S_{n-1}(x_0^p, \dots, x_{n-1}^p, y_0^p, \dots, y_{n-1}^p)) + p^n(x_n + y_n),$$

whence the polynomial S_n may be computed recursively from $S_0, \dots, S_{n-1}$. The proof is similar for the P_n. □

3.4. *Truncated Witt vectors.*

3.4.1. *Definition.* In this paper, we will mostly be working with truncated Witt vectors. These can be thought of as p-adic analogues of truncated power series, i.e., elements of the ring $R[\![t]\!]/(t^n) \cong R[t]/(t^n)$ (over some base ring R). More formally:

Definition 3.4.2. Let R be a perfect ring. Given $n \in \mathbb{N}$, the ring of n-truncated Witt vectors over R is defined as $W_n(R) := W(R)/p^n W(R)$.

3.4.3. *Language.* For a perfect ring R, the pair $(W(R), R)$ (resp. $(W_n(R), R)$) is viewed as a two-sorted structure with sorts $\boldsymbol{W}$ for the Witt ring $W(R)$ (resp. $W_n(R)$) and $\boldsymbol{R}$ for the residue ring R. The sort $\boldsymbol{W}$ is equipped with the language of rings L_{rings}, while the sort $\boldsymbol{R}$ may be equipped with any $L \supseteq L_{\text{rings}}$. We also have a function symbol for the Teichmüller map $[\ ] : \boldsymbol{R} \to \boldsymbol{W}$. For each choice of a language L for the $\boldsymbol{R}$-sort, the resulting language will be denoted by $\langle L_{\text{rings}}, L \rangle$.

3.4.4. *Interpretability in R.*

Lemma 3.4.5. *Let R be a perfect ring, viewed as an L-structure with $L \supseteq L_{\text{rings}}$. For each $n \in \mathbb{N}$, there exists a quantifier-free interpretation Γ_n of the $\langle L_{\text{rings}}, L\rangle$-structure $(W_n(R), R)$ in the L-structure R such that the sequence of interpretations $(\Gamma_n)_{n\in\omega}$ is uniformly recursive.*

Proof. By Section 3.3.8, for $n \in \mathbb{N}$ the underlying set of $W_n(R)$ can be identified with R^n, so we take $\partial_{\Gamma_n}(x_1, \dots, x_n)$ to be $\bigwedge_{i=1}^n x_i = x_i$ and the coordinate map $f_{\Gamma_n} : R^n \to W_n(R)$ as the identity map. The ring operations of $W_n(R)$ are given by

$$(a_0, \dots, a_{n-1}) + (b_0, \dots, b_{n-1}) = (S_0(a_0, b_0), \dots, S_{n-1}(a_0, b_0, \dots, a_{n-1}, b_{n-1}))$$

and

$$(a_0, \dots, a_{n-1}) \cdot (b_0, \dots, b_{n-1}) = (P_0(a_0, b_0), \dots, P_{n-1}(a_0, b_0, \dots, a_{n-1}, b_{n-1})),$$

for certain polynomials $S_i, P_i \in \mathbb{Z}[x_0, \dots, x_i, y_0, \dots, y_i]$, for $i = 0, \dots, n-1$. We now need to describe the map $\phi \mapsto \phi_{\Gamma_n}$ on *unnested* atomic L_{rings}-formulas:

(1) If $\phi(x, y, z)$ is the formula $x + y = z$ (here $x, y, z \in \boldsymbol{W}$), we may take $\phi_{\Gamma_n}(\bar{x}, \bar{y}, \bar{z})$ to be the L_{rings}-formula $\bigwedge_{i=0}^{n-1} z_i = S_i(x_0, y_0, \dots, x_{n-1}, y_{n-1})$.

(2) If $\phi(x, y, z)$ is the formula $x \cdot y = z$ (here $x, y, z \in \boldsymbol{W}$), we may take $\phi_{\Gamma_n}(\bar{x}, \bar{y}, \bar{z})$ to be the L_{rings}-formula $\bigwedge_{i=0}^{n-1} z_i = P_i(x_0, y_0, \dots, x_{n-1}, y_{n-1})$.

(3) If $\phi(x, y)$ is the formula $[x] = y$ (here $x \in \boldsymbol{R}$ and $y \in \boldsymbol{W}$), we may take $\phi_{\Gamma_n}(x, \bar{y})$ to be the formula $\bigwedge_{i=1}^{n-1} y_i = 0 \wedge y_0 = x$.

(4) If $\phi(\bar{x})$ is an unnested atomic L-formula with variables from the sort $\boldsymbol{R}$, then we may take $\phi_{\Gamma_n}(\bar{x}) := \phi(\bar{x})$ (here $x_i \in \boldsymbol{R}$ for the latter formula).

The above data define a quantifier-free interpretation Γ_n of the $\langle L_{\text{rings}}, L\rangle$-structure $(W_n(R), R)$ in the L-structure R. Moreover, since the polynomials S_i, P_i are computable (Observation 3.3.9), the sequence of interpretations $(\Gamma_n)_{n\in\omega}$ is uniformly recursive. □

3.5. *Untilting.* Expository notes on the material of this section may be found either in Section 5 of the Bourbaki seminar given by Morrow [2019] or in the lecture series notes by Lurie [2018, Lectures 2 and 3].

3.5.1. *Overview.* The functor $K \mapsto K^\flat$ is far from being faithful, i.e., there will be several nonisomorphic mixed characteristic perfectoid fields K that tilt to the same perfectoid field of characteristic p. For example, the p-adic completions of $\mathbb{Q}_p(p^{1/p^\infty})$ and $\mathbb{Q}_p(\zeta_{p^\infty})$ both tilt to the t-adic completion of $\mathbb{F}_p((t))^{1/p^\infty}$. For a perfectoid field F of characteristic p, an *untilt* of F is a pair (K, ι), where (K, v) is a perfectoid field and $\iota : (F, w) \xrightarrow{\cong} (K^\flat, v^\flat)$ is a valued field isomorphism. Fargues and Fontaine give a description of all possible untilts of F in an *intrinsic* fashion, i.e., in a way that uses only arithmetic from F itself (see Theorem 3.5.11). This result will be of vital importance for Theorem A.

3.5.2. *The ring $\boldsymbol{A}_{\text{inf}}$.* Fix any perfectoid field (F, w) of characteristic $p > 0$. We introduce $\boldsymbol{A}_{\text{inf}} := W(\mathcal{O}_F)$, called the *infinitesimal* period ring, which is the ring of Witt vectors over $\mathcal{O}_F$.

Definition 3.5.3. An element $\xi \in \boldsymbol{A}_{\text{inf}}$ is said to be *distinguished* if it is of the form $\xi = \sum_{n=0}^{\infty}[c_n]p^n$, with $c_0 \in \mathfrak{m}_F$ and $c_1 \in \mathcal{O}_F^{\times}$.

In other words, distinguished elements are those of the form $\xi = [\pi] - up$ where $w\pi > 0$ and $u \in \boldsymbol{A}_{\text{inf}}$ is a unit.

Remark 3.5.4. Let $\text{res} : \mathcal{O}_F \to \mathcal{O}_F/\mathfrak{m}_F$ be the residue map and $W(\text{res}) : \boldsymbol{A}_{\text{inf}} \to W(\mathcal{O}_F/\mathfrak{m}_F)$ be the (unique) induced ring homomorphism provided by Fact 3.3.5 that maps $\sum_{n=0}^{\infty}[c_n]p^n \mapsto \sum_{n=0}^{\infty}[\text{res}(c_n)]\cdot p^n$. The element $\xi \in \boldsymbol{A}_{\text{inf}}$ is distinguished precisely when $W(\text{res})(\xi)$ is a unit multiple of p in $W(\mathcal{O}_F/\mathfrak{m}_F)$.

3.5.5. *Distinguished elements and untilts.* We outline how one can go from an untilt of F to an ideal of $\boldsymbol{A}_{\text{inf}}$ generated by a distinguished element and vice versa. Let (K, ι) be an untilt of F, i.e., we have $\iota : (F, w) \xrightarrow{\cong} (K^{\flat}, v^{\flat})$. By Lemma 3.2.3(a), we have a morphism of multiplicative monoids $\sharp : \mathcal{O}_{K^{\flat}} \to \mathcal{O}_K$. We also write $\sharp : \mathcal{O}_F \to \mathcal{O}_K$ for the composite map $\mathcal{O}_F \xrightarrow{\iota} \mathcal{O}_{K^{\flat}} \xrightarrow{\sharp} \mathcal{O}_K$. While $\sharp : \mathcal{O}_F \to \mathcal{O}_K$ is not a ring homomorphism (unless K has characteristic p), it does induce a ring homomorphism $\phi : \mathcal{O}_F \to \mathcal{O}_K/(p) : x \mapsto x^{\sharp} \bmod (p)$. Moreover, ϕ is *surjective* since it descends to an isomorphism $\mathcal{O}_F/(\pi) \xrightarrow{\cong} \mathcal{O}_K/(p)$ for any $\pi \in \mathcal{O}_F$ with $w\pi = vp$. The map θ in the lemma below is important. We shall sketch the proof of the lemma for the convenience of the reader.

Lemma 3.5.6 [Lurie 2018, Lecture 3, Remarks 11–13]. *There exists a ring homomorphism $\theta : \boldsymbol{A}_{\text{inf}} \to \mathcal{O}_K$ inducing ϕ above. Moreover, θ is surjective and $\theta^{-1}(\mathcal{O}_K^{\times}) = \boldsymbol{A}_{\text{inf}}^{\times}$.*

Proof sketch. Apply Fact 3.3.5 with $A = \boldsymbol{A}_{\text{inf}}$, $A' = \mathcal{O}_K$ to get that ϕ lifts uniquely to the ring homomorphism

$$\theta : \boldsymbol{A}_{\text{inf}} \to \mathcal{O}_K : \sum_{n=0}^{\infty}[c_n]\cdot p^n \mapsto \sum_{n=0}^{\infty} c_n^{\sharp}\cdot p^n.$$

We claim that θ is surjective. Recall that ϕ is surjective. Given $x \in \mathcal{O}_K$, we may thus find $c_0 \in \mathcal{O}_F$ such that $x = c_0^{\sharp} + x_1 \cdot p$, for some $x_1 \in \mathcal{O}_K$. Similarly, we may find $c_1 \in \mathcal{O}_F$ such that $x_1 = c_1^{\sharp} + x_2 \cdot p$. We then get that $x = c_0^{\sharp} + c_1^{\sharp}\cdot p + x_2 \cdot p^2$. Continuing this way and since $\mathcal{O}_K$ is p-adically complete, we may write $x = \sum_{n=0}^{\infty} c_n^{\sharp}\cdot p^n$. To show that $\theta^{-1}(\mathcal{O}_K^{\times}) = \boldsymbol{A}_{\text{inf}}^{\times}$, observe that

$$\sum_{n=0}^{\infty}[c_n]\cdot p^n \in \boldsymbol{A}_{\text{inf}}^{\times} \iff c_0 \in \mathcal{O}_F^{\times} \iff c_0^{\sharp} \in \mathcal{O}_K^{\times} \iff \sum_{n=0}^{\infty} c_n^{\sharp}\cdot p^n \in \mathcal{O}_K^{\times} \qquad \square$$

Let us examine the kernel of θ. Let $\pi \in \mathcal{O}_F$ be as above (i.e., such that $w\pi = vp$) and write $\pi^{\sharp} = \bar{u}\cdot p$ for some $\bar{u} \in \mathcal{O}_K^{\times}$. By Lemma 3.5.6, we may find $u \in \boldsymbol{A}_{\text{inf}}^{\times}$ such that $\theta(u) = \bar{u}$. Note that $\xi = [\pi] - u\cdot p \in \boldsymbol{A}_{\text{inf}}$ is a distinguished element and that $\xi \in \text{Ker}(\theta)$. In fact, the following is true:

Proposition 3.5.7 [Lurie 2018, Corollary 17]. *Let (F, w) be a perfectoid field of characteristic p and (K, ι) be an untilt. Let $\theta : \boldsymbol{A}_{\text{inf}} \to \mathcal{O}_K$ be as above. Then* $\text{Ker}(\theta)$ *is a principal ideal generated by* ***any*** *distinguished element $\xi \in \text{Ker}(\theta)$.*

Starting with an untilt (K, ι), we have thus produced an ideal $(\xi_K) \subseteq \boldsymbol{A}_{\mathrm{inf}}$, where ξ_K is a distinguished element in $\boldsymbol{A}_{\mathrm{inf}}$.

Conversely, starting with $(\xi) \subseteq \boldsymbol{A}_{\mathrm{inf}}$, with ξ a distinguished element, we may produce an untilt (K, ι) of F as follows. Write $\theta : \boldsymbol{A}_{\mathrm{inf}} \to \boldsymbol{A}_{\mathrm{inf}}/(\xi)$ for the quotient map. We then have:

Lemma 3.5.8 [Lurie 2018, Lecture 3, page 4, Claim (a)]. *For every $y \in \boldsymbol{A}_{\mathrm{inf}}/(\xi)$, there exists $x \in \mathcal{O}_F$ such that $(y) = (\theta([x]))$.*

Proposition 3.5.9 [Lurie 2018, Proposition 16]. *Let (F, w) be a perfectoid field of characteristic p and $\xi \in \boldsymbol{A}_{\mathrm{inf}}$ a distinguished element. Then the quotient ring $\boldsymbol{A}_{\mathrm{inf}}/(\xi)$ is the valuation ring $\mathcal{O}_K$ of a perfectoid field (K, v) such that $(K^\flat, v^\flat) \cong (F, w)$. The valuation v is such that if $y \in \boldsymbol{A}_{\mathrm{inf}}/(\xi)$, then $vy := wx$ with $x \in \mathcal{O}_F$ so that $(y) = (\theta([x]))$ in $\boldsymbol{A}_{\mathrm{inf}}/(\xi)$.*

The isomorphism $\iota : (F, w) \to (K^\flat, v^\flat)$ of Proposition 3.5.9 is described as follows. If $\xi = [\pi] - up$, then $\mathcal{O}_K/(p) \cong W(\mathcal{O}_F)/(p, [\pi] - up) \cong \mathcal{O}_F/(\pi)$. Passing to inverse limits, this induces a ring isomorphism $\mathcal{O}_{K^\flat} \cong \mathcal{O}_F$, which in turn yields $\iota : F \xrightarrow{\cong} K^\flat$ by passing to fraction fields. Starting with $(\xi) \subseteq \boldsymbol{A}_{\mathrm{inf}}$, we have thus produced an untilt (K, ι).

Definition 3.5.10. Two untilts (K, ι) and (K', ι') are isomorphic when there exists a valued field isomorphism $\phi : K \xrightarrow{\cong} K'$ inducing a commutative diagram

$$\begin{tikzcd}
F \arrow[r, "\iota"] \arrow[d, dash, "="] & K^\flat \arrow[d, "\phi^\flat"] \\
F \arrow[r, "\iota'"] & K'^\flat
\end{tikzcd}$$

where $\phi^\flat : (x, x^{1/p}, \dots) \mapsto (\phi(x), \phi(x^{1/p}), \dots)$. Let Y_F denote the set of characteristic 0 untilts of (F, w), up to isomorphism.

We write 0 for the isomorphism class of the unique characteristic p untilt of (F, ι), represented by F itself together with the natural isomorphism $\iota : F \xrightarrow{\cong} F^\flat : x \to (x, x^{1/p}, \dots)$, and set $\overline{Y}_F = Y_F \cup \{0\}$ for the set of all untilts of (F, w), up to isomorphism.

Theorem 3.5.11 (Fargues and Fontaine). *Let (F, w) be a perfectoid field of characteristic p. The map $(\xi) \mapsto \mathrm{Frac}(\mathcal{O}_F/(\xi))$ defines a bijective correspondence between the set of ideals $(\xi) \subseteq \boldsymbol{A}_{\mathrm{inf}}$ generated by a distinguished element and the set $\overline{Y}_F$.*

Proof. See [Morrow 2019, Proposition 5.1] or [Lurie 2018, Lecture 2, Corollary 18]. □

Remark 3.5.12. Let (K, ι) be an untilt of (F, w) and $(\xi) = ([\pi] - up)$ be its associated ideal. Note that $(p) = (\theta([\pi]))$ in $\boldsymbol{A}_{\mathrm{inf}}/(\xi)$ and therefore $vp = w\pi$.

3.5.13. *Tilting equivalence.* We emphasized in Section 3.5.1 that untilting is ambiguous, in the sense that there are many ways to untilt a perfectoid field of positive characteristic. However, the ambiguity is eliminated by *fixing a base* perfectoid field K and its associated tilt $K^\flat$. This leads to an equivalence of categories of perfectoid extensions, known as the *tilting equivalence*:

Theorem 3.5.14 (tilting equivalence). *The categories of perfectoid field extensions of K and perfectoid field extensions of $K^\flat$ are equivalent.*

Proof. See [Scholze 2013, Theorem 2.8]. Theorem 5.2 in [loc. cit.] shows a more general result about perfectoid algebras; the case of perfectoid fields follows as a special case by [loc. cit., Lemma 5.21]. □

In the discussion after [loc. cit., Theorem 2.8], Scholze explains that there are two proofs of Theorem 3.5.14:

(1) His original proof in [loc. cit.], using Faltings' almost mathematics; see [loc. cit., Section 4].

(2) An alternative proof which describes the functor $\sharp$ inverse to $\flat$ as $L \mapsto W(\mathcal{O}_L) \otimes_{W(\mathcal{O}_{K^\flat})} K$; see [loc. cit., Remark 5.19].

Let us elaborate more on the second approach, which is in the spirit of Section 3.5 and will be more suitable for us. If $(\xi) \subset W(\mathcal{O}_{K^\flat})$ is the ideal associated to K, then one computes that $W(\mathcal{O}_L) \otimes_{W(\mathcal{O}_{K^\flat})} \mathcal{O}_K = W(\mathcal{O}_L) \otimes_{W(\mathcal{O}_{K^\flat})} W(\mathcal{O}_{K^\flat})/(\xi) = W(\mathcal{O}_L)/(\xi)$. In other words, if L is a perfectoid field extending $K^\flat$, then $L^\sharp$ is simply the untilt of K whose associated ideal in $W(\mathcal{O}_L)$ is (ξ).

3.6. ***Space of untilts.*** In Section 3.6.3 we exhibit an appealing model-theoretic property of the space Y_F of untilts of (F, w). This will not be used in the rest of the paper. We then study in Section 3.6.5 the size of the space of untilts up to elementary equivalence. We will see that the cardinality is often too big, so that one cannot possibly expect K to be decidable simply relative to $K^\flat$.

3.6.1. *Metric structure on Y_F.* Fargues and Fontaine equip $\overline{Y}_F$ with a metric topology, which allows us to view the space of untilts geometrically. Suppose $x = (K_x, v_x)$ and $y = (K_y, v_y)$ are two "points" of $\overline{Y}_F$, corresponding to the ideals (ξ_x) and (ξ_y) respectively, provided by Theorem 3.5.11. We choose an embedding $\Gamma_w \hookrightarrow \mathbb{R}$, which determines embeddings $\Gamma_{v_y} \hookrightarrow \mathbb{R}$ for all $y \in Y_F$ via the canonical identification $\Gamma_{v_y} \cong \Gamma_w$. One then defines $d(x, y) := |\theta_y(\xi_x)|_y$, where $\theta_y : \boldsymbol{A}_{\inf} \twoheadrightarrow \boldsymbol{A}_{\inf}/(\xi_y) = \mathcal{O}_{K_y}$ is the quotient map and as usual $|a|_y = p^{-v_y(a)}$.

Proposition 3.6.2 [Fargues and Fontaine 2018, Proposition 2.3.2(1)]. *Let $d : \overline{Y}_F \times \overline{Y}_F \to \mathbb{R}$ be as above. The pair $(\overline{Y}_F, d)$ is a complete ultrametric space.*

Proof. See [Fargues and Fontaine 2018, Propositions 2.3.2 and 2.3.4] or [Lurie 2018, Lecture 14, Propositions 6 and 7]. □

Recall that $0 \in \overline{Y}_F$ is the isomorphism class of the untilt corresponding to (F, w) itself together with the natural isomorphism $\iota : F \xrightarrow{\cong} F^\flat : x \to (x, x^{1/p}, \dots)$. We can define a radius function $r(y) := d(0, y)$ for $y \in \overline{Y}_F$, which allows us to think of $\overline{Y}_F$ intuitively as the unit disc with center 0.

3.6.3. *A model-theoretic property of Y_F.* We now show that limits in the punctured unit disc Y_F, with respect to the Fargues–Fontaine metric, agree with limits in the model-theoretic sense:

Proposition 3.6.4. *Let $(x_n)_{n\in\omega}$ be a sequence in Y_F such that $x_n \xrightarrow{d} x$ and $x \neq 0$. Let (K_n, v_n) be the untilt associated to x_n and (K, v) the untilt associated to x. We set*

$$(K^*, v^*) := \prod_{n\in\omega}(K_n, v_n)/U$$

for a nonprincipal ultrafilter U on $\mathbb{N}$. Then $(K^*, v^*) \equiv (K, v)$ in L_{val}.

Proof. Let $(\xi_n) = ([\pi_n] - u_n p)$ be the ideal in $\boldsymbol{A}_{\text{inf}}$ corresponding to (K_n, v_n) and $(\xi) = ([\pi] - up)$ be the ideal corresponding to (K, v). Note that the set $\{v_n p : n \in \mathbb{N}\} \subseteq \Gamma_w$ is bounded from above; otherwise, there would be a subsequence $(x_{n_k})_{k\in\mathbb{N}}$ with $x_{n_k} \to 0$.

Fix $m \in \mathbb{N}$ and let $(\bar{\xi}_n)$ and $(\bar{\xi})$ be the images of the ideals (ξ_n) and (ξ) in $W_m(\mathcal{O}_F)$ via $\boldsymbol{A}_{\text{inf}} \twoheadrightarrow \boldsymbol{A}_{\text{inf}}/(p^m) = W_m(\mathcal{O}_F)$.

Claim. We have that $(\bar{\xi}_n) = (\bar{\xi})$, for sufficiently large n.

Proof. We let $\theta : \boldsymbol{A}_{\text{inf}} \to \boldsymbol{A}_{\text{inf}}/(\xi) = \mathcal{O}_K$ be the quotient map. Since $d(x_n, x) \to 0$, we get that $v(\theta(\xi_n)) \to \infty$. We will thus have that $\xi_n \equiv p^m \cdot \alpha_n \mod (\xi)$, for some $\alpha_n \in \boldsymbol{A}_{\text{inf}}$ and for all $n \gg 0$. Consequently, one gets that $(\bar{\xi}_n) \subseteq (\bar{\xi})$ for $n \gg 0$. Similarly, since $v_n(\theta_n(\xi)) \to \infty$ and $\{v_n p : n \in \mathbb{N}\}$ is bounded, we get that $v_n(\theta_n(\xi)) \geq m v_n p$ for $n \gg 0$. It follows that there exists $\beta_n \in \boldsymbol{A}_{\text{inf}}$ such that $\xi \equiv p^m \cdot \beta_n \mod (\xi_n)$, for $n \gg 0$. We conclude that $(\bar{\xi}_n) = (\bar{\xi})$, for $n \gg 0$. □

It follows that $\mathcal{O}_{K_n}/(p^m) \cong W_m(\mathcal{O}_F)/(\bar{\xi}_n) = W_m(\mathcal{O}_F)/(\bar{\xi}) \cong \mathcal{O}_K/(p^m)$, for sufficiently large n. We also get that (ξ_n) and (ξ) have the same image in $\boldsymbol{A}_{\text{inf}}/(p) \cong \mathcal{O}_F$ for $n \gg 0$ and therefore $(\pi_n) = (\pi)$ for $n \gg 0$. By Lemma 3.2.4(b), we get that $(\Gamma_{v_n}, v_n p) \cong (\Gamma_w, w\pi_n) = (\Gamma_w, w\pi) \cong (\Gamma_v, vp)$, for all sufficiently large n. The conclusion follows from Theorem 2.1.5 and Łoś's Theorem. □

3.6.5. *The space Z_F.* It is natural to consider the set Y_F up to elementary equivalence. More precisely:

Definition 3.6.6. Let (F, w) be a perfectoid field of characteristic p. For $x = (K_x, \iota_x)$, $y = (K_y, \iota_y) \in Y_F$ define the equivalence relation $x \sim y \iff (K_x, v_x) \equiv (K_y, v_y)$ in L_{val}. We define $Z_F := Y_F/\sim$.

Note that the definition of Z_F only takes the underlying valued fields (K, v) into account and not the map ι. We now determine the size of Z_F in a few cases in Proposition 3.6.9. For Proposition 3.6.9(a), we will need the following:

Fact 3.6.7 [Scholze 2012, Proposition 4.3]. Let (K, v) be a perfectoid field with $K^\flat$ algebraically closed. Then K is also algebraically closed.

For Proposition 3.6.9(b) we need an algebraic fact. A finite extension L/K has the *unique subfield property* if for every $d \mid [L : K]$, there is a unique subextension F/K such that $[F : K] = d$.

Fact 3.6.8 [Acosta de Orozco and Vélez 1982, Theorem 2.1]. Let K be a field, $n \in \mathbb{N}$ be such that $\text{char}(K) \nmid n$, $a \in K$ such that $X^n - a \in K[X]$ is irreducible and set $L = K(a^{1/n})$. Suppose that for every odd prime $p \mid n$, we have that $\zeta_p \notin L \backslash K$ and in case $4 \mid n$ we have $\zeta_4 \notin L \backslash K$. Then L/K has the unique subfield property.

The construction in Proposition 3.6.9(b) is an elaborated version of Scholze's answer [2021] to a closely related mathoverflow question asked by the author.

Proposition 3.6.9. (a) *Let* $(F, w) = (\widehat{\overline{\mathbb{F}_p((t))}}, v_t)$, *the t-adic completion of an algebraic closure of* $\mathbb{F}_p((t))$. *Then* $|Z_F| = 1$.

(b) *Set* $(F, w) = (\widehat{\mathbb{F}_p((t))^{1/p^\infty}}, v_t)$. *Then* $|Z_F| = \mathfrak{c}$.

Proof. (a) **First proof.** Let (K, v) be a perfectoid field of characteristic 0 such that $(K^\flat, v^\flat) \cong (\widehat{\overline{\mathbb{F}_p((t))}}, v_t)$. By Fact 3.6.7, we get that K is algebraically closed. By Robinson's completeness of the theory $\mathrm{ACVF}_{(0,p)}$ of algebraically closed valued fields of mixed characteristic $(0, p)$ (see [van den Dries 2014, Corollary 3.34]), we get that $\mathrm{Th}(K, v) = \mathrm{ACVF}_{(0,p)}$ and hence $|Z_F| = 1$.

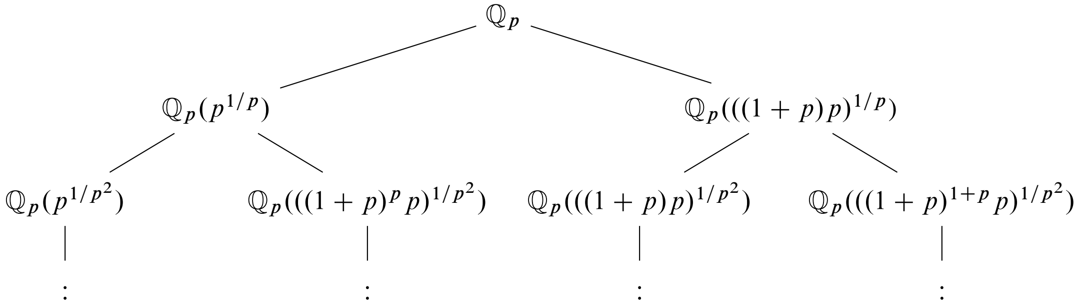
Second proof. Let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ be the completed algebraic closure of $\mathbb{Q}_p$. By [Fargues and Fontaine 2014, Remark 2.24], we have a ring isomorphism $\mathcal{O}_K/(p^n) \cong \mathcal{O}_{\mathbb{C}_p}/(p^n)$ for each $n \in \mathbb{N}$. One also has that $(\Gamma_v, vp) \equiv (\Gamma_{\mathbb{C}_p}, v_p p)$ in L_{oag} with a constant for vp, by an easy application of quantifier elimination for the theory ODAG of ordered divisible abelian groups [Marker 2002, Corollary 3.1.17]. We conclude that $(K, v) \equiv (\mathbb{C}_p, v_p)$ from Theorem 2.1.5.

(b) We assume that $p > 2$; we indicate the necessary changes for the case $p = 2$ in the end of the proof. For each $\alpha \in 2^\omega$, we define an algebraic extension K_α of $\mathbb{Q}_p$ as follows. We write $\alpha \restriction n$ for the restriction of α to $n = \{0, 1, \dots, n-1\}$ (set-theoretically $\alpha \restriction 0 = 0$). We now define inductively:

(1) $K_0 = \mathbb{Q}_p$ and $\pi_0 = p$.

(2) $K_{\alpha\restriction n} = K_{\alpha\restriction(n-1)}(((1+p)^{\alpha(n-1)} \cdot \pi_{\alpha\restriction(n-1)})^{1/p})$ and $\pi_{\alpha\restriction n} = ((1+p)^{\alpha(n-1)} \cdot \pi_{\alpha\restriction(n-1)})^{1/p}$.

Set $\bar{\alpha}_n = \sum_{k=0}^{n-1} \alpha(k) \cdot p^k$ for $n \in \mathbb{N}^{>0}$ and $\bar{\alpha}_0 = 1$ by convention. Note that $X^{p^n} - (1+p)^{\bar{\alpha}_n} p \in \mathbb{Z}_p[X]$ is an Eisenstein (hence irreducible) polynomial and that $K_{\alpha\restriction n} = \mathbb{Q}_p(((1+p)^{\bar{\alpha}_n} p)^{1/p^n})$. We let $K_\alpha = \bigcup_{n\in\omega} K_{\alpha\restriction n}$. Visually, the field K_α is obtained by taking the union of all fields along a certain branch (corresponding to α) in the binary tree below:


$\mathbb{Q}_p$
$\mathbb{Q}_p(p^{1/p})$
$\mathbb{Q}_p(((1+p)p)^{1/p})$
$\mathbb{Q}_p(p^{1/p^2})$
$\mathbb{Q}_p(((1+p)^p p)^{1/p^2})$
$\mathbb{Q}_p(((1+p)p)^{1/p^2})$
$\mathbb{Q}_p(((1+p)^{1+p} p)^{1/p^2})$
⋮
⋮
⋮
⋮

Claim 1. For each $\alpha \in 2^\omega$, we have $\zeta_p \notin K_\alpha$ and $(1+p)^{1/p} \notin K_\alpha$.

Proof. Note that $\zeta_p \notin K_\alpha$ since $e(K_{\alpha\restriction n}/\mathbb{Q}_p) = p^n$ while $e(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) = p-1$. Suppose that $(1+p)^{1/p} \in K_{\alpha\restriction n}$, for some $n \in \mathbb{N}$. By Fact 3.6.8, we would have that $K_{\alpha\restriction 1} = \mathbb{Q}_p((1+p)^{1/p})$. If $\alpha(0) = 0$, this would imply that $\mathbb{Q}_p(p^{1/p}) = \mathbb{Q}_p((1+p)^{1/p})$. If $\alpha(0) = 1$, this would imply that $\mathbb{Q}_p(((1+p)\cdot p)^{1/p}) = \mathbb{Q}_p((1+p)^{1/p})$. In either case, we would get that $\mathbb{Q}_p(p^{1/p}) = \mathbb{Q}_p((1+p)^{1/p})$. However, one sees that $(1+p)^{1/p} \notin \mathbb{Q}_p(p^{1/p})$. Indeed, suppose $a \in \mathbb{Q}_p(p^{1/p})$ is such that $a^p = 1+p$. Write $a \equiv c_0 + c_1 \cdot p^{1/p} \bmod p^{2/p}\mathbb{Z}_p[p^{1/p}]$, for some $c_0, c_1 \in \{0, \dots, p-1\}$. We then compute

$$a^p \equiv c_0^p + c_1^p \cdot p + c_0^{p-1} \cdot c_1 \cdot p^{1+1/p} \not\equiv 1 + p \bmod p^{1+2/p},$$

for any choice of c_0 and c_1. We conclude that $(1+p)^{1/p} \notin K_\alpha$. □

Using Claim 1, we show:

Claim 2. If $\alpha \neq \beta$, then $\widehat{K_\alpha} \not\equiv_{\exists^1} \widehat{K_\beta}$ in L_{rings}.

Proof. Note that $K_\alpha \equiv_{\exists^1} \widehat{K_\alpha}$ (resp. $K_\beta \equiv_{\exists^1} \widehat{K_\beta}$) by Theorem 2.2.6. It suffices to show that $K_\alpha \not\equiv_{\exists^1} K_\beta$ for $\alpha \neq \beta$. Let $n \in \omega$ be least such that $\alpha(n) \neq \beta(n)$ and say $\alpha(n) = 1$. Now if $K_\alpha \equiv_{\exists^1} K_\beta$, there would be $a, b \in K_\alpha$ such that $a^{p^n} = (1+p)^{\bar{\alpha}_n} p$ and $b^{p^n} = (1+p)^{\bar{\beta}_n} p$. Set $c := a/b$ and note that $c^{p^n} = (1+p)^{\bar{\alpha}_n} p/((1+p)^{\bar{\beta}_n} p) = (1+p)^{p^{n-1}}$. This implies that $(c^p/(1+p))^{p^{n-1}} = 1$. We conclude that either $\zeta_p \in K_\alpha$ or $c^p = 1+p$, both of which are impossible by Claim 1. □

Next we prove:

Claim 3. For every $\alpha \in 2^\omega$, we have that $\widehat{K_\alpha}^\flat = \mathbb{F}_p\widehat{((t))^{1/p^\infty}}$.

Proof. For every $n \in \mathbb{N}$, we have that $K_{\alpha\restriction(n+1)}/K_{\alpha\restriction n}$ is totally ramified and $\mathcal{O}_{K_{\alpha\restriction(n+1)}} = \mathcal{O}_{K_{\alpha\restriction n}}[\pi_{\alpha\restriction(n+1)}]$ [Serre 1979, Corollary page 19]. It follows that $\mathcal{O}_{K_\alpha} = \mathbb{Z}_p[\{\pi_{\alpha\restriction n} : n \in \mathbb{N}\}]$. We compute

$$\begin{aligned}\mathcal{O}_{K_\alpha}/(p) &= \mathbb{Z}_p[x_1, x_2, \dots]/(p, x_1^p - (1+p)^{\alpha(0)}p, x_2^p - (1+p)^{\alpha(1)}x_1, \dots)\\ &\cong \mathbb{F}_p[x_1, x_2, \dots]/(x_1^p, x_2^p - x_1, \dots)\\ &\cong \mathbb{F}_p[x_1^{1/p^\infty}]/(x_1^p)\\ &\overset{t=x_1^p}{\cong} \mathbb{F}_p[t^{1/p^\infty}]/(t).\end{aligned}$$

We thus get that $\varprojlim_\Phi \mathcal{O}_{K_\alpha}/(p) \cong \mathbb{F}_p\widehat{[\![t]\!]^{1/p^\infty}}$ and the conclusion follows. □

Claims 2,3 show that $|Z_F| \geq \mathfrak{c}$. On the other hand, the bound $|Z_F| \leq \mathfrak{c}$ is automatic, as any first-order L_{val}-theory can be identified with a subset of $\text{Sent}_{L_{\text{val}}} \simeq \mathbb{N}$. This finishes the proof in case $p > 2$. For $p = 2$, one first proves a variant of Claim 1, namely that $\zeta_4 \notin K_\alpha$ and $(\pm 3)^{1/2} \notin K_\alpha$. For the former, one can check inductively that $\zeta_4 \notin K_{\alpha\restriction n}$ using Kummer theory for quadratic extensions. The proof of Claim 2 then goes through. Finally, the proof of Claim 3 works verbatim for $p = 2$. □

Remark 3.6.10. Set $(F, w) = (\widehat{\mathbb{F}_p((t))}, v_t)$. Fargues and Fontaine [2014, Remark 2.24] ask whether every untilt (K, v) of (F, w) is isomorphic to $(\mathbb{C}_p, v_p)$. They note in Remark 2.24 that for any untilt (K, v) of (F, w) one has $\mathcal{O}_K/(p^n) \cong \mathcal{O}_{\mathbb{C}_p}/(p^n)$ for each $n \in \mathbb{N}$. However, these isomorphisms are obtained in a noncanonical way and do not necessarily yield a valued field isomorphism between K and $\mathbb{C}_p$. In fact, an example of such a K with $K \not\cong \mathbb{C}_p$ was provided by Kedlaya and Temkin [2018, Theorem 1.3]. This should be contrasted with Proposition 3.6.9(a), saying that all untilts of (F, w) are elementary equivalent.

Remark 3.6.11. In [Anscombe and Fehm 2016, Remark 7.6], the authors write:

> *At present, we do not know of an example of a mixed characteristic henselian valued field* (K, v) *for which* $\mathrm{Th}_\exists(k_v)$ *and* $\mathrm{Th}_\exists(\Gamma_v, vp)$ *are decidable but* $\mathrm{Th}_\exists(K, v)$ *is undecidable.*

We note that such an example indeed exists. By Proposition 3.6.9(b) and the fact that there are countably many Turing machines, there must exist an undecidable perfectoid (thus henselian) field (K, v) with $K^\flat \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$. Moreover, the proof even provides us with a field K whose algebraic part is undecidable. On the other hand, by Lemma 3.2.4(b), we have that $k_v \cong \mathbb{F}_p$ and $(\Gamma_v, vp) \cong \big(\frac{1}{p^\infty}\mathbb{Z}, 1\big)$, both of which are decidable — the latter being an easy application of [Robinson and Zakon 1960]. Finally, we note that Dittmann [2022] has recently provided an example which is discretely valued and whose algebraic part is decidable.

Remark 3.6.12. For future use in Proposition 7.1.1, we record here that Claim 3 gives us that $t = (\pi_{\alpha\restriction 0} + (p), \pi_{\alpha\restriction 1} + (p), \dots)$, via the identifications $\widehat{\mathbb{F}_p[[t]]^{1/p^\infty}} \cong \varprojlim_{\Phi} \mathcal{O}_{K_\alpha}/(p)$.

Question 3.6.13. Is there a perfectoid field (F, w) of characteristic p with $1 < |Z_F| < \mathfrak{c}$?

4. Relative decidability for perfectoid fields

4.1. *Introduction.* We shall now use the results of Section 3 to prove Theorem A and Corollary A.

4.1.1. *Work of Rideau, Scanlon and Simon.* It is my understanding that there is ongoing work by Rideau, Scanlon and Simon, which aims at giving a model-theoretic account of many of the concepts and facts that were discussed in Section 3, in the context of *continuous* logic. In particular, they obtain a biinterpretability result between $\mathcal{O}_K$ and $\mathcal{O}_{K^\flat}$ in the sense of continuous logic. It should be noted that their biinterpretability result was conceived prior to the present paper and in fact influenced the material that is presented here.

4.1.2. *Plan of action.* Without any adjustments, the interpretation of Rideau, Scanlon and Simon does not quite yield an interpretation in the sense of ordinary first-order logic. The problem is that when one converts statements about $\mathcal{O}_K$ to statements about $\mathcal{O}_{K^\flat}$ via $\mathcal{O}_K \cong W(\mathcal{O}_{K^\flat})/(\xi)$, one ends up with infinitely many variables, coming from the Witt vector coordinates. This problem disappears by interpreting one residue ring $\mathcal{O}_K/(p^n)$ at a time, via $\mathcal{O}_K/(p^n) \cong W_n(\mathcal{O}_{K^\flat})/(\xi \bmod (p^n))$. This approach is facilitated by Corollary 2.3.1. In Section 2.3, we emphasized that *uniform* decidability of the residue rings is key. As we will see, this eventually comes down to the computability of the distinguished element ξ itself.

4.2. *Computable untilts.*

4.2.1. *Computable Witt vectors.* In analogy with a computable real number, a computable p-adic integer is one for which there is an algorithm which outputs the sequence of its p-adic digits. More precisely, a p-adic integer $a \in \mathbb{Z}_p$ of the form $a = \sum_{n=0}^{\infty} [\alpha_n] \cdot p^n$ is said to be *computable* precisely when the function $\mathbb{N} \to \mathbb{Z}/p\mathbb{Z} : n \mapsto \alpha_n$ is recursive. The notion of a computable p-adic integer extends naturally to the more general concept of a *computable Witt vector*.

First recall that a *computable* ring R_0 is one whose underlying set is (or is identified with) a *recursive* subset of $\mathbb{N}$, via which the operations $+ : R_0 \times R_0 \to R_0$ and $\cdot : R_0 \times R_0 \to R_0$ are identified with *recursive* functions.

Definition 4.2.2. Fix a perfect ring R and let $R_0 \subseteq R$ a computable subring. Consider the ring $W(R)$, the ring of Witt vectors over R. An element $\xi \in W(R)$ with Witt vector coordinates $(\xi_0, \xi_1, \dots) \in R^\omega$ is said to be R_0-computable if:

(1) For each $n \in \mathbb{N}$, we have that $\xi_n \in R_0$.

(2) The function $\mathbb{N} \to R_0 : n \mapsto \xi_n$ is recursive.

Example 4.2.3. (a) Let $R_0 = R = \mathbb{F}_p$. Then the computable elements of $\mathbb{Z}_p = W(\mathbb{F}_p)$ are the usual computable p-adic integers.

(b) A *nonexample*: Let R be any perfect ring, $R_0 \subseteq R$ any computable subring and $S \subseteq \mathbb{N}$ be a nonrecursive set. The element $\xi = \sum_{n \in S} p^n \in W(R)$ is not computable.

4.2.4. *Computable untilts.* Let (F, w) be a perfectoid field of characteristic p and $\boldsymbol{A}_{\mathrm{inf}} = W(\mathcal{O}_F)$. Let also $R_0 \subseteq \mathcal{O}_F$ be a computable subring.

Remark 4.2.5. The reader is welcome to assume that $F = \mathbb{F}_p\widehat{((t))^{1/p^\infty}}$ or $\bar{\mathbb{F}}_p\widehat{((t))^{1/p^\infty}}$ and $R_0 = \mathbb{F}_p[t]$. This case is enough for the applications presented here, i.e., Corollaries A and B.

We shall now define what it means for an untilt K of F to be R_0-computable:

Definition 4.2.6. Let (K, ι) be an untilt of (F, w) and $R_0 \subseteq \mathcal{O}_F$ a computable subring. We say that (K, v) is an R_0-*computable* untilt of (F, w) if there is an R_0-computable distinguished element $\xi_K \in \boldsymbol{A}_{\mathrm{inf}}$ with $\mathcal{O}_K \cong \boldsymbol{A}_{\mathrm{inf}}/(\xi_K)$.

Example 4.2.7. In Corollary 4.4.6 we will see that $\widehat{\mathbb{Q}_p(p^{1/p^\infty})}$ and $\widehat{\mathbb{Q}_p(\zeta_{p^\infty})}$ are $\mathbb{F}_p[t]$-computable untilts of $\widehat{\mathbb{F}_p((t))^{1/p^\infty}}$. Also, that $\widehat{\mathbb{Q}_p^{ab}}$ is an $\mathbb{F}_p[t]$-computable untilt of $\widehat{\bar{\mathbb{F}}_p((t))^{1/p^\infty}}$.

4.3. *Relative decidability.* Let (K, v) be an untilt of (F, w) and $\xi_K \in \boldsymbol{A}_{\mathrm{inf}}$ be such that $\mathcal{O}_K = \boldsymbol{A}_{\mathrm{inf}}/(\xi_K)$ (Theorem 3.5.11). We write $\bar{\xi}_{K,n}$ for the image of ξ_K in $W_n(\mathcal{O}_F)$ via $\boldsymbol{A}_{\mathrm{inf}} \twoheadrightarrow \boldsymbol{A}_{\mathrm{inf}}/(p^n) \cong W_n(\mathcal{O}_F)$.

4.3.1. *Interpretability.* All the necessary background material related to interpretability is presented in Section 1.2.

Lemma 4.3.2. *For each $n \in \mathbb{N}$, there is a $\exists^+$-interpretation A_n of the local ring $(\mathcal{O}_K/(p^n), \mathfrak{m}_n)$ in the $\langle L_{\mathrm{rings}}, L_{\mathrm{lcr}}\rangle$-structure $((W_n(\mathcal{O}_F), \mathcal{O}_F), \bar{\xi}_{K,n})$ such that the sequence of interpretations $(\mathrm{A}_n)_{n\in\omega}$ is uniformly recursive.*

Proof. Fix $n \in \mathbb{N}$. We have that $\mathcal{O}_K/(p^n) \cong \boldsymbol{A}_{\mathrm{inf}}/(p^n, \xi_K) \cong W_n(\mathcal{O}_F)/(\bar{\xi}_{K,n})$. By Proposition 3.5.9, we get that $\mathfrak{m}_n = (\{\theta_n([x]) : x \in \mathfrak{m}_F\})$, where θ_n is the composite map

$$\boldsymbol{A}_{\mathrm{inf}} \overset{\theta}{\twoheadrightarrow} \boldsymbol{A}_{\mathrm{inf}}/(\xi_K) \xrightarrow{\bmod p^n} W_n(\mathcal{O}_F)/(\bar{\xi}_{K,n}) \xrightarrow{\cong} \mathcal{O}_K/(p^n).$$

We take $\partial_{\mathrm{A}_n}(x)$ to be $x \in \boldsymbol{W}$. Let c be a constant symbol with $c^{(W_n(\mathcal{O}_F),\mathcal{O}_F)} = \bar{\xi}_{K,n}$. The reduction map $\mathrm{Form}_{L_{\mathrm{lcr}}} \to \langle L_{\mathrm{rings}}, L_{\mathrm{lcr}}\rangle \cup \{c\} : \phi \mapsto \phi_{\mathrm{A}_n}$ on unnested atomic formulas is described as follows:

(1) If $\phi(x, y)$ is $x = y$, then we take ϕ_{A_n} to be the formula $x, y \in \boldsymbol{W} \wedge \exists z \in \boldsymbol{W}(x = y + z \cdot c)$. As usual, the conjunct $x, y \in \boldsymbol{W}$ is an informal way of saying that the variables x, y are taken from the sort $\boldsymbol{W}$. The cases of $x = 0$ and $x = 1$ are similar.

(2) If $\phi(x, y, z)$ is $x \diamond y = z$, then we take ϕ_{A_n} to be the formula $x, y, z \in \boldsymbol{W} \wedge \exists w \in \boldsymbol{W}(x \diamond y = z + w \cdot c)$, where $\diamond$ is either $\cdot$ or $+$.

(3) If $\phi(x)$ is $x \in \mathfrak{m}$, then we take $\phi_{\mathrm{A}_n}(x)$ to be the formula $x \in \boldsymbol{W} \wedge \exists z, w \in \boldsymbol{W}, y \in \boldsymbol{R}\ (y \in \mathfrak{m} \wedge x = [y] \cdot z + w \cdot c)$.

The coordinate map $f_{\mathrm{A}_n} : W_n(\mathcal{O}_F) \twoheadrightarrow \mathcal{O}_K/(p^n)$ is the one induced by the map θ_n above. The above data define a recursive $\exists^+$-interpretation A_n of $(\mathcal{O}_K/(p^n), \mathfrak{m}_n)$ in $((W_n(\mathcal{O}_F), \mathcal{O}_F), \bar{\xi}_{K,n})$. The sequence of interpretations $(\mathrm{A}_n)_{n\in\omega}$ is uniform in n and thus also (trivially) uniformly recursive. □

Proposition 4.3.3. *Suppose (K, v) is an untilt of (F, w) and that $\xi_K \in \boldsymbol{A}_{\mathrm{inf}}$ is such that $\mathcal{O}_K = \boldsymbol{A}_{\mathrm{inf}}/(\xi_K)$. Let $(\xi_0, \xi_1, \ldots) \in \mathcal{O}_F^{\omega}$ be the Witt vector coordinates of ξ_K. Then:*

(a) *The value group (Γ_v, vp) is recursively interpretable in the valued field $((F, w), \xi_0)$.*

(b) *For each $n \in \mathbb{N}$, there exists a $\exists^+$-interpretation B_n of the local ring $(\mathcal{O}_K/(p^n), \mathfrak{m}_n)$ in the local ring $((\mathcal{O}_F, \mathfrak{m}_F), \xi_0, \ldots, \xi_{n-1})$ such that the sequence of interpretations $(B_n)_{n\in\omega}$ is uniformly recursive.*

Proof. (a) By Lemma 3.2.4(b), we will have that $(\Gamma_v, vp) \cong (\Gamma_w, w\xi_0)$ and the value group $(\Gamma_w, w\xi_0)$ is clearly recursively interpretable in the $L_{\mathrm{val}} \cup \{c\}$-structure (F, w) with $c^{(F,w)} = \xi_0$.

(b) Lemma 4.3.2 provides us with a $\exists^+$-interpretation A_n of the local ring $(\mathcal{O}_K/(p^n), \mathfrak{m}_n)$ in the $\langle L_{\mathrm{rings}}, L_{\mathrm{lcr}}\rangle \cup \{c\}$-structure $((W_n(\mathcal{O}_F), \mathcal{O}_F), \bar{\xi}_{K,n})$ such that the sequence of interpretations $(\mathrm{A}_n)_{n\in\omega}$ is uniformly recursive. Lemma 3.4.5 provides us with a quantifier-free interpretation Γ_n of $((W_n(\mathcal{O}_F), \mathcal{O}_F), \bar{\xi}_{K,n})$ in the local ring $((\mathcal{O}_F, \mathfrak{m}_F), \xi_0, \ldots, \xi_{n-1})$, such that the sequence of interpretations $(\Gamma_n)_{n\in\omega}$ is uniformly recursive. Let B_n be the composite interpretation of $(\mathcal{O}_K/(p^n), \mathfrak{m}_n)$ in $((\mathcal{O}_F, \mathfrak{m}_F), \xi_0, \ldots, \xi_{n-1})$. This is also a $\exists^+$-interpretation by Lemma 1.2.8 and the sequence of interpretations $(\mathrm{B}_n)_{n\in\omega}$ is uniformly recursive by Lemma 1.2.15. □

4.3.4. *Proof of Theorem A.* Given a computable subring $R_0 \subseteq \mathcal{O}_F$, we write $L_{\mathrm{val}}(R_0)$ for the language L_{val} enriched with a constant c_a for each $a \in R_0$ (see notation). The valued field (F, w) can then be updated to an $L_{\mathrm{val}}(R_0)$-structure with $c_a^{(F,w)} = a$.

Theorem A. *Let (F, w) be a perfectoid field of characteristic p. Suppose $R_0 \subseteq \mathcal{O}_F$ is a computable subring and (K, v) is an R_0-computable untilt of (F, w):*

(a) *If (F, w) is decidable in $L_{\mathrm{val}}(R_0)$, then (K, v) is decidable in L_{val}.*

(b) *If (F, w) is $\exists$-decidable in $L_{\mathrm{val}}(R_0)$, then (K, v) is $\exists$-decidable in L_{val}.*

Proof. (a) By Proposition 4.3.3(a), we get that (Γ_v, vp) is decidable in L_{oag} with a constant for vp. By Proposition 4.3.3(b), for each $n \in \mathbb{N}$, there exists an interpretation B_n of the L_{lcr}-structure $(\mathcal{O}_K/(p^n), \mathfrak{m}_n)$ in the $L_{\mathrm{lcr}} \cup \{c_0, \dots, c_{n-1}\}$-structure $((\mathcal{O}_F, \mathfrak{m}_F), \xi_0, \dots, \xi_{n-1})$ with $c_m^{(\mathcal{O}_F, \mathfrak{m}_F)} = \xi_m$ for $m = 0, \dots, n-1$. Moreover, the sequence of interpretations $(\mathrm{B}_n)_{n\in\omega}$ is uniformly recursive.

Claim. There exists an interpretation Δ_n of the $L_{\mathrm{lcr}} \cup \{c_0, \dots, c_{n-1}\}$-structure $((\mathcal{O}_F, \mathfrak{m}_F), \xi_0, \dots, \xi_{n-1})$ in the $L_{\mathrm{val}}(R_0)$-structure (F, w) such that the sequence of interpretations $(\Delta_n)_{n\in\omega}$ is uniformly recursive.

Proof. Fix $n \in \mathbb{N}$. We take $\partial_{\Delta_n}(x)$ to be the formula $x \in \mathcal{O}$. The reduction map on unnested atomic formulas is described as follows:

(1) If $\phi(x)$ is the formula $x = c_m$, for some $m = 0, \dots, n-1$, we take $\phi_{\Delta_n}(x)$ to be the formula $x = c_{\xi_m}$. The formulas $x = y$, $x = 0$ and $x = 1$ are interpreted in the obvious way.

(2) If $\phi(x)$ is the formula $x \in \mathfrak{m}$, we take $\phi_{\Delta_n}(x)$ to be the formula $\exists y(xy = 1 \wedge y \notin \mathcal{O})$.

(3) If $\phi(x, y, z)$ is $x \diamond y = z$, then we take ϕ_{Δ_n} to be the formula $x, y, z \in \mathcal{O} \wedge \phi(x, y, z)$, where $\diamond$ is either $\cdot$ or $+$.

The coordinate map $f_{\Delta_n} : \partial_{\Delta_n}(F) \to \mathcal{O}_F$ is the identity. Since $\mathbb{N} \to R_0 : m \mapsto \xi_m$ is recursive, the reduction map $\mathbb{N} \times \mathrm{Form}_{L_{\mathrm{lcr}}\cup\{c_0,\dots,c_{n-1}\}} \to \mathrm{Form}_{L_{\mathrm{val}}(R_0)} : (n, \phi) \mapsto \phi_{\Delta_n}$ restricted to unnested atomic formulas is recursive. By definition, this means that the sequence of interpretations $(\Delta_n)_{n\in\omega}$ is uniformly recursive. □

For each $n \in \mathbb{N}$, let E_n be the composite interpretation of B_n and Δ_n. The sequence $(E_n)_{n\in\omega}$ is uniformly recursive by Lemma 1.2.15. By Proposition 1.2.14, we get that the sequence of rings $(\mathcal{O}_K/(p^n))_{n\in\omega}$ is *uniformly* decidable in L_{rings}. The conclusion follows from Corollary 2.3.1.

(b) For the existential version, one needs to keep track of the complexity of formulas. Since B_n is a $\exists^+$-interpretation and Δ_n is an $\exists$-interpretation, we see that the reduction map $L_{\mathrm{lcr}} \to L_{\mathrm{val}}(R_0) : \phi \mapsto \phi_{E_n}$ sends $\exists^+$-formulas to $\exists$-formulas (see Remark 1.2.7). It follows that the sequence of local rings $((\mathcal{O}_K/(p^n), \mathfrak{m}_n)_{n\in\omega}$ is uniformly $\exists^+$-decidable in L_{lcr}. We conclude by Corollary 2.3.2. □

The assumption of completeness in Theorem A can be easily relaxed to henselianity:

Corollary 4.3.5. *Let (F, w) be a perfect nontrivially valued field with a rank 1 value group and $R_0 \subseteq \mathcal{O}_F$ be a computable subring. Suppose (K, v) is a mixed characteristic henselian valued field such that $(\widehat{K}, \widehat{v})$ is an R_0-computable untilt of $(\widehat{F}, \widehat{w})$. Then*:

(a) *If (F, w) is decidable in $L_{\mathrm{val}}(R_0)$, then (K, v) is decidable in L_{val}.*

(b) *If (F, w) is $\exists$-decidable in $L_{\mathrm{val}}(R_0)$, then (K, v) is $\exists$-decidable in L_{val}.*

Proof. Suppose $\widehat{\mathcal{O}}_K = W(\widehat{\mathcal{O}}_F)/(\xi)$, where $\xi = [\pi] - up$, with $\pi \in \mathfrak{m}_F \cap R_0$ and $u \in W(\mathcal{O}_F)^\times$. Note that $W(\widehat{\mathcal{O}}_F)/([\pi] - up) \cong W(\mathcal{O}_F)/([\pi] - up)$; indeed, $W(\mathcal{O}_F)$ is p-adically complete and $[\pi]$ and p are associates in the quotient $W(\mathcal{O}_F)/([\pi] - up)$. For each $n \in \mathbb{N}$, one has that

$$\mathcal{O}_K/(p^n) \cong \widehat{\mathcal{O}}_K/(p^n) \cong W_n(\widehat{\mathcal{O}}_F)/([\pi] - up) \cong W_n(\mathcal{O}_F)/([\pi] - up)$$

We now proceed as in the proof of Theorem A. □

4.3.6. *Remarks on Theorem A.* Note that decidability of K in L_{val} relative to its tilt $K^\flat$ in L_{val}, i.e., without taking parameters into account, is false. Essentially, the point is that p is named in L_{val}, while t is not.

Example 4.3.7. Let $(\Gamma, +, <) \subseteq (\mathbb{R}, +, <)$ be any p-divisible ordered abelian group, which is decidable in L_{oag} but undecidable in $L_{\mathrm{oag}} \cup \{1\}$, where 1 a distinguished element of Γ. For example, let $S \subsetneq \mathbb{P}$ be a nonrecursive set of primes and $S' := \mathbb{P} - S$ be its complement. Denote by $\frac{1}{S}\mathbb{Z}$ the group generated by $\left\{\frac{1}{s} : s \in S\right\}$ and consider the ordered abelian group

$$\Gamma = \frac{1}{p^\infty}\left(\frac{1}{S}\mathbb{Z} \oplus \frac{1}{S'}\mathbb{Z}\sqrt{2}\right)$$

equipped with the order induced from the natural embedding $\Gamma \hookrightarrow \mathbb{R}$. This is a regularly dense group, in the sense of Robinson and Zakon [1960], with prime invariants $[\Gamma : p\Gamma] = 1$ and $[\Gamma : q\Gamma] = q$ for $q \neq p$. By [loc. cit.], this group is decidable in L_{oag} but is clearly undecidable in $L_{\mathrm{oag}} \cup \{1\}$. Since Γ is p-divisible, we may form the tame valued field $(F, w) = (\mathbb{F}_p((t^\Gamma)), v_t)$, which is decidable in L_{val} by [Kuhlmann 2016, Theorem 1.4]. However, the untilt (K, v), whose associated Witt vector is $[t] - p$, is undecidable in L_{val}. Indeed, even (Γ_v, vp) is undecidable in L_{oag} with a constant for vp.

Remark 4.3.8. Theorem A holds also for untilts K of F, which have an associated distinguished element ξ_K satisfying a more relaxed condition than the one of Definition 4.2.2. Namely, suppose that $\xi_K = (\xi_0, \xi_1, \dots) \in \mathcal{O}_F^\omega$ and each ξ_n is definable in the valued field (F, w) by a formula $\phi_n(x) \in L_{\mathrm{val}}(R_0)$ with parameters from R_0. Suppose furthermore that the function $\mathbb{N} \to \mathrm{Form}_{L_{\mathrm{val}}(R_0)} : n \mapsto \phi_n(x)$ is recursive. Then the conclusion of Theorem A is still valid, i.e., (K, v) is decidable in L_{val} relative to (F, w) in $L_{\mathrm{val}}(R_0)$.

It is clear that when each $\phi_n(x)$ is a quantifier-free formula, the configuration described in Remark 4.3.8 specializes to the notion of a computable untilt. We have no particular application in mind that requires the level of generality described in Remark 4.3.8, which is one reason we have restricted ourselves to the quantifier-free case (the other being clarity of exposition).

4.4. ***Corollary A.*** In order to prove Corollary A, we need to calculate the tilts of our fields of interest and compute the associated distinguished elements.

4.4.1. *Computing the distinguished elements.* All computations below are well-known to experts; see, e.g., [Fargues and Fontaine 2014, Example 2.22]. For lack of a detailed reference, we shall spell out the details.

Lemma 4.4.2. *There exist ring isomorphisms*:

(a) $\mathbb{Z}_p[p^{1/p^\infty}]/(p) \cong \mathbb{F}_p[t^{1/p^\infty}]/(t)$ *mapping* $p^{1/p^n} + (p) \mapsto t^{1/p^n} + (t)$.

(b) $\mathbb{Z}_p[\zeta_{p^\infty}]/(p) \cong \mathbb{F}_p[t^{1/p^\infty}]/(t^{p-1})$ *mapping* $\zeta_p + (p) \mapsto t + 1 + (t^{p-1})$.

(c) $\mathbb{Z}_p^{ab}/(p) \cong \overline{\mathbb{F}}_p[t^{1/p^\infty}]/(t^{p-1})$ *mapping* $\zeta_p + (p) \mapsto t + 1 + (t^{p-1})$.

Proof. (a) For each $n \in \mathbb{N}$, the irreducible polynomial of $p^{1/p^{n+1}}$ over $\mathbb{Q}_p(p^{1/p^n})$ is the Eisenstein polynomial $x^p - p^{1/p^n} \in \mathbb{Z}_p[p^{1/p^n}][x]$. We therefore compute

$$\begin{aligned}\mathbb{Z}_p[p^{1/p^\infty}]/(p) &\cong \mathbb{Z}_p[x_1, x_2, \dots]/(p, x_1^p - p, x_2^p - x_1, \dots)\\ &\cong \mathbb{F}_p[x_1, x_2, \dots]/(x_1^p, x_2^p - x_1, \dots)\\ &\overset{x_n \mapsto t^{1/p^n}}{\cong} \mathbb{F}_p[t^{1/p^\infty}]/(t)\end{aligned}$$

(b) The irreducible polynomial of ζ_p over $\mathbb{Q}_p$ is the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + \cdots + 1$. Moreover, given $n > 1$, the irreducible polynomial of ζ_{p^n} over $\mathbb{Q}_p(\zeta_{p^{n-1}})$ is $x^p - \zeta_{p^{n-1}} \in \mathbb{Z}[\zeta_{p^n}][x]$. We now proceed as in (a) and compute

$$\mathbb{Z}_p[\zeta_{p^\infty}]/(p) \cong \mathbb{Z}_p[x_1, x_2, \dots]/(p, \Phi_p(x_1), x_2^p - x_1, \dots) \overset{x_{n+1} \mapsto x^{1/p^n}}{\cong} \mathbb{F}_p[x^{1/p^\infty}]/(\overline{\Phi}_p(x)).$$

Note that $\overline{\Phi}_p(x) = \frac{x^p - 1}{x-1} = \frac{(x-1)^p}{x-1} = (x-1)^{p-1}$ and thus

$$\mathbb{Z}_p[\zeta_{p^\infty}]/(p) \cong \mathbb{F}_p[x^{1/p^\infty}]/(x-1)^{p-1} \overset{t = x-1}{=} \mathbb{F}_p[t^{1/p^\infty}]/(t^{p-1}).$$

(c) By local Kronecker–Weber (see Theorem 14.2 in [Washington 1997] and Proposition 17 in [Serre 1979]), we get that $\mathbb{Z}_p^{ab} = \mathbb{Z}_p^{ur}[\zeta_{p^\infty}]$. We now proceed as in (b). □

Corollary 4.4.3. (a) $\widehat{\mathbb{Q}_p(p^{1/p^\infty})}^\flat \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$ *and* $t^\sharp = p$.

(b) $\widehat{\mathbb{Q}_p(\zeta_{p^\infty})}^\flat \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$ *and* $(t+1)^\sharp = \zeta_p$.

(c) $\widehat{\mathbb{Q}_p^{ab}}^\flat \cong \widehat{\overline{\mathbb{F}}_p((t))^{1/p^\infty}}$ *and* $(t+1)^\sharp = \zeta_p$.

Proof. (a) By Lemma 4.4.2, we have that $\mathbb{Z}_p[p^{1/p^\infty}]/(p) \cong \mathbb{F}_p[t^{1/p^\infty}]/(t)$ via an isomorphism mapping $p^{1/p^n} + (p) \mapsto t^{1/p^n} + (t)$. One can verify directly that $\widehat{\mathbb{F}_p[\![t]\!]^{1/p^\infty}} \to \varprojlim_\Phi \mathbb{F}_p[t^{1/p^\infty}]/(t)$, where $x \mapsto (x \bmod (t), x^{1/p} \bmod (t), \dots)$, is a ring isomorphism. It follows that $\widehat{\mathbb{Q}_p(p^{1/p^\infty})}^\flat \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$ and by definition $t^\sharp = \lim_{n\to\infty}(p^{1/p^n})^{p^n} = p$.

The proofs of (b) and (c) are similar. □

Proposition 4.4.4 [Fargues and Fontaine 2014, Example 2.22]. *We have the following isomorphisms*:

(a) $\widehat{\mathbb{Z}_p[p^{1/p^\infty}]} \cong W(\widehat{\mathbb{F}_p[\![t]\!]^{1/p^\infty}})/([t] - p)$.

(b) $\widehat{\mathbb{Z}_p[\zeta_{p^\infty}]} \cong W(\widehat{\mathbb{F}_p[\![t]\!]^{1/p^\infty}})/([t+1]^{p-1} + [t+1]^{p-2} + \cdots + 1)$.

(c) $\widehat{\mathbb{Z}_p^{ab}} \cong W(\widehat{\overline{\mathbb{F}}_p[\![t]\!]^{1/p^\infty}})/([t+1]^{p-1} + [t+1]^{p-2} + \cdots + 1)$.

Proof. (a) By Corollary 4.4.3(a), we have that $\widehat{\mathbb{Q}_p(p^{1/p^\infty})}^\flat \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$. Consider the ring homomorphism $\theta : \boldsymbol{A}_{\text{inf}} \twoheadrightarrow \widehat{\mathbb{Z}_p[p^{1/p^\infty}]}$ inducing $\sharp : \widehat{\mathbb{F}_p[\![t]\!]^{1/p^\infty}} \to \widehat{\mathbb{Z}_p[p^{1/p^\infty}]}$. Since $t^\sharp = p$, we get that $\theta([t]) = p$ and therefore $[t] - p \in \operatorname{Ker}(\theta)$. By Proposition 3.5.7, it follows that $\operatorname{Ker}(\theta) = ([t] - p)$.

(b) By Corollary 4.4.3(b), we have that $\widehat{\mathbb{Q}_p(\zeta_{p^\infty})}^{\flat} \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$. mapping $1+t \mapsto \zeta_p$. Consider the ring homomorphism $\theta{:}\boldsymbol{A}_{\text{inf}} \twoheadrightarrow \widehat{\mathbb{Z}_p[\zeta_{p^\infty}]}$ inducing $\sharp{:}\widehat{\mathbb{F}_p[\![t]\!]^{1/p^\infty}} \to \widehat{\mathbb{Z}_p[\zeta_{p^\infty}]}$. Since $(t+1)^\sharp = \zeta_p$, we get that $\theta([t+1]) = \zeta_p$ and therefore $[t+1]^{p-1} + \cdots + [t+1] + 1 \in \operatorname{Ker}(\theta)$. By Proposition 3.5.7, it suffices to show that $\xi = [t+1]^{p-1} + \cdots + [t+1] + 1$ is a distinguished element of $\boldsymbol{A}_{\text{inf}}$. Set $\text{res} : \mathcal{O}_F \twoheadrightarrow \mathcal{O}_F/\mathfrak{m}_F$ for the residue map and $W(\text{res})$ for the unique induced homomorphism $W(\text{res}) : W(R) \to W(R/\mathfrak{m}_R)$ of Fact 3.3.5. We compute that $W(\text{res})(\xi) = 1 + 1 + \cdots + 1 = p$, whence ξ is a distinguished element of $\boldsymbol{A}_{\text{inf}}$ (Remark 3.5.4).

(c) Similar to (b). □

4.4.5. *Proof of Corollary A.*

Corollary 4.4.6. *We have the following*:

(a) $\widehat{\mathbb{Q}_p(p^{1/p^\infty})}$ *and* $\widehat{\mathbb{Q}_p(\zeta_{p^\infty})}$ *are* $\mathbb{F}_p[t]$*-computable untilts of* $\widehat{\mathbb{F}_p((t))^{1/p^\infty}}$.

(b) $\widehat{\mathbb{Q}_p^{ab}}$ *is an* $\mathbb{F}_p[t]$*-computable untilt of* $\widehat{\mathbb{F}_p((t))^{1/p^\infty}}$.

Proof. The case of $\widehat{\mathbb{Q}_p(p^{1/p^\infty})}$ is clear. For the other two cases, note that $\xi := [t+1]^{p-1} + [t+1]^{p-2} + \cdots + 1$ is $\mathbb{F}_p[t]$-computable, using the *computable* polynomials $S_0, \dots, S_n$ for Witt vector addition (Observation 3.3.9). □

Corollary A. (a) *Assume* $\mathbb{F}_p((t))^{1/p^\infty}$ *is* (*existentially*) *decidable in* $L_{\text{val}}(t)$. *Then* $\mathbb{Q}_p(p^{1/p^\infty})$ *and* $\mathbb{Q}_p(\zeta_{p^\infty})$ *are* (*existentially*) *decidable in* L_{val}.

(b) *Assume* $\overline{\mathbb{F}}_p((t))^{1/p^\infty}$ *is* (*existentially*) *decidable in* $L_{\text{val}}(t)$. *Then* $\mathbb{Q}_p^{ab}$ *is* (*existentially*) *decidable in* L_{val}.

Proof. (a) By Corollary 4.4.6 and Corollary 4.3.5.

(b) Similar to (a). □

5. Applications: Tame fields of mixed characteristic

5.1. *Introduction.*

5.1.1. *Motivation.* We shall prove Corollary B, which to my knowledge is the first decidability result for tame fields of mixed characteristic.

5.1.2. *Preliminaries.* The algebra and model theory of tame fields was introduced and studied by Kuhlmann [2016]. Recall the definition:

Definition 5.1.3. Let (K, v) be a henselian valued field. A finite valued field extension $(K', v')/(K, v)$ is said to be tame if

(1) $([\Gamma' : \Gamma], p) = 1$, where p is the *characteristic exponent* of k, i.e., $p = \operatorname{char}(k)$ if this is positive and $p = 1$ if $\operatorname{char}(k) = 0$.

(2) The residue field extension k'/k is separable.

(3) The extension $(K', v')/(K, v)$ is defectless, meaning that the fundamental equality $[K' : K] = [\Gamma' : \Gamma] \cdot [k' : k]$ holds.

An algebraic valued field extension is said to be tame if every finite subextension is tame.

Definition 5.1.4. A henselian valued field (K, v) is said to be tame if every finite valued field extension $(K', v')/(K, v)$ is tame.

In practice, one often needs a more intrinsic description of tame fields. This is provided by the following:

Proposition 5.1.5 [Kuhlmann 2016, Theorem 3.2]. *Let (K, v) be henselian valued field. Then the following are equivalent*:

(1) *(K, v) is a tame field.*

(2) *(K, v) is algebraically maximal, Γ is p-divisible and k is perfect.*

Example 5.1.6. Using Proposition 5.1.5, one can verify the following:

(a) Any (algebraically) maximal immediate extension of $\mathbb{Q}_p(p^{1/p^\infty})$ or $\mathbb{Q}_p(\zeta_{p^\infty})$ is tame.

(b) Any (algebraically) maximal immediate extension of $\mathbb{F}_p((t))^{1/p^\infty}$ is tame. In particular, the Hahn field $(\mathbb{F}_p((t^\Gamma)), v_t)$ with value group $\Gamma = \frac{1}{p^\infty}\mathbb{Z}$ and residue field $\mathbb{F}_p$ is tame.

5.1.7. *Equal characteristic.* Kuhlmann obtained the following Ax–Kochen/Ershov principle for tame fields of equal characteristic:

Theorem 5.1.8 [Kuhlmann 2016, Theorem 1.4]. *Let (K, v) and (K', v') be two equal characteristic tame fields. Then $(K, v) \equiv (K', v')$ in L_{val} if and only if $k \equiv k'$ in L_{rings} and $\Gamma \equiv \Gamma'$ in L_{oag}.*

Kuhlmann then deduces the following decidability result (among others):

Corollary 5.1.9 [Kuhlmann 2016, Theorem 1.6]. *Set $\Gamma = \frac{1}{p^\infty}\mathbb{Z}$, i.e., for the p-divisible hull of $\mathbb{Z}$. The Hahn field $(\mathbb{F}_p((t^\Gamma)), v_t)$ is decidable in L_{val}.*

In recent work, Lisinski combined results of Kuhlmann [2016] with work of Kedlaya [2006] and obtained the following strengthening of Corollary 5.1.9:

Theorem 5.1.10 [Lisinski 2021, Theorem 1]. *Set $\Gamma = \frac{1}{p^\infty}\mathbb{Z}$. The Hahn field $(\mathbb{F}_p((t^\Gamma)), v_t)$ is decidable in L_t.*

5.1.11. *Mixed characteristic.* Kuhlmann's Theorem 5.1.8 fails as such for mixed characteristic tame fields. A counterexample is given in [Anscombe and Kuhlmann 2016, Theorem 1.5(c)]. The lack of such a principle has been a fundamental obstacle in obtaining decidability results for such fields.

5.2. ***Mixed characteristic tame fields.*** While we do not know whether $\mathbb{Q}_p(p^{1/p^\infty})$ and $\mathbb{Q}_p(\zeta_{p^\infty})$ are (existentially) decidable, we will show that they admit decidable maximal immediate extensions. These are tame fields by Example 5.1.6(a).

Lemma 5.2.1 [Fargues and Fontaine 2014, Remark 2.23]. *Let (K, v) be a perfectoid field. Then (K, v) is maximal if and only if $(K^\flat, v^\flat)$ is maximal.*

Proof. Immediate from the tilting equivalence Theorem 3.5.14 and the fact that tilting preserves value groups and residue fields; see Lemma 3.2.4(b). □

Corollary B. *The valued field $(\mathbb{Q}_p(p^{1/p^\infty}), v_p)$ (resp. $(\mathbb{Q}_p(\zeta_{p^\infty}), v_p)$) admits a maximal immediate extension which is decidable in L_{val}.*

Proof. Recall from Corollaries 4.4.3(a) and 4.4.4(a) that

$$\widehat{\mathbb{Q}_p(p^{1/p^\infty})}^{\flat} \cong \widehat{\mathbb{F}_p((t))^{1/p^\infty}}$$

and that $\xi = [t] - p$. Let $\mathbb{F}_p((t^\Gamma))$ be the Hahn field with value group $\Gamma = \frac{1}{p^\infty}\mathbb{Z}$ and residue field $\mathbb{F}_p$. It is a (nonunique) maximal immediate extension of $\mathbb{F}_p((t))^{1/p^\infty}$. By Theorem 3.5.14, we may form $K = \mathbb{F}_p((t^\Gamma))^\sharp$ as in the diagram below:

$$\begin{tikzcd}
K \arrow[d, dash] & \mathbb{F}_p((t^\Gamma)) \arrow[l, dashed, "\sharp"'] \arrow[d, dash] \\
\widehat{\mathbb{Q}_p(p^{1/p^\infty})} \arrow[r, "\flat"] & \widehat{\mathbb{F}_p((t))^{1/p^\infty}}
\end{tikzcd}$$

such that $\xi_K = [t] - p$ (see Section 3.5.13). By Lemma 5.2.1, we see that (K, v) is a maximal immediate extension of $(\mathbb{Q}_p(p^{1/p^\infty}), v_p)$. By Theorem 5.1.10 and Theorem A, we see that (K, v) is decidable in L_{val}. The proof for $\mathbb{Q}_p(\zeta_{p^\infty})$ is similar. □

Remark 5.2.2. It is also true that $\mathbb{Q}_p^{ab}$ admits a decidable maximal immediate extension (in this case unique) but this already follows from well-known results in the model theory of algebraically maximal Kaplansky fields; see [Kuhlmann 2016, page 4, Part (f)].

In spite of Corollary B, the following is worth noting:

Remark 5.2.3. A tree-like construction similar to Proposition 3.6.9(b) shows that there exist uncountably many pairwise elementary inequivalent maximal immediate extensions of $\mathbb{Q}_p(p^{1/p^\infty})$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$). In particular, the valued field $\mathbb{Q}_p(p^{1/p^\infty})$ (resp. $\mathbb{Q}_p(\zeta_{p^\infty})$) has uncountably many *undecidable* maximal immediate extensions. Note that the tilts of all such fields will be maximal immediate extensions of $\mathbb{F}_p((t))^{1/p^\infty}$ and thus will be tame fields. As a consequence of Kuhlmann's Theorem 5.1.8, all of them will be decidable in L_{val}. Nevertheless, they will all be undecidable in $L_{\text{val}}(t)$.

6. Applications: Congruences modulo p

6.1. *Introduction.*

6.1.1. *Goal.* We shall now prove Theorem B, which shows the existence of an algorithm that decides whether a system of polynomial equations and inequalities, defined over $\mathbb{Z}$, has a solution modulo p over the valuation rings of our fields of interest.

6.1.2. *Strategy.* The proof is via a local field approximation argument, using the computations of Lemma 4.4.2. One eventually encodes the above problem in the existential theory of the tilt in L_{val}, where the Anscombe–Fehm Theorem (Theorem 2.2.3) applies. This should be contrasted with Corollary A, which requires decidability in the language $L_{\text{val}}(t)$ on the characteristic p side.

6.2. ***From residue rings to valuation rings.*** The crux of the argument lies in the following:

Proposition 6.2.1. *Let $f_i(x), g_j(x) \in \mathbb{F}_p[x]$ be multivariable polynomials in $x = (x_1, \dots, x_m)$ for $i, j = 1, \dots, n$. Then*

$$\mathbb{F}_p[t^{1/p^\infty}]/(t) \models \exists x \bigwedge_{1\le i,j\le n} (f_i(x) = 0 \wedge g_j(x) \neq 0) \iff \mathbb{F}_p[\![t]\!]^{1/p^\infty} \models \exists x \bigwedge_{1\le i,j\le n} (v(f_i(x)) > v(g_j(x))).$$

Proof. First observe that

$$\mathbb{F}_p[\![t]\!]^{1/p^\infty}/(t) \cong \varinjlim \mathbb{F}_p[\![t^{1/p^n}]\!]/(t) \cong \varinjlim \mathbb{F}_p[t^{1/p^n}]/(t) \cong \mathbb{F}_p[t^{1/p^\infty}]/(t). \tag{†}$$

$\Rightarrow$: Let $a \in (\mathbb{F}_p[t^{1/p^\infty}]/(t))^m$ be such that $f_i(a) = 0 \wedge g_j(a) \neq 0$, for $1 \le i, j \le n$ and let $\tilde{a}$ be any lift of a in $\mathbb{F}_p[\![t]\!]^{1/p^\infty}$ via the isomorphism (†). We see that $v(f_i(\tilde{a})) \ge 1 > v(g_j(\tilde{a}))$, for all $1 \le i, j \le n$.

$\Leftarrow$: Let $b \in (\mathbb{F}_p[\![t]\!]^{1/p^\infty})^m$ be such that $v(g_j(b)) < v(f_i(b))$ for all $1 \le i, j \le n$. Set $\gamma_1 = \max\{v(g_j(b)) : j = 1, \dots, n\}$ and $\gamma_2 = \min\{v(f_i(b)) : i = 1, \dots, n\}$ and consider the open interval $I = (\gamma_1, \gamma_2) \subseteq \frac{1}{p^\infty}\mathbb{Z}^{\ge 0}$. Since $\frac{1}{p^\infty}\mathbb{Z}$ is dense in $\mathbb{R}$, we can find $q \in \frac{1}{p^\infty}\mathbb{Z}$ such that $1 \in qI$.

We now make use of the fact that for each $q \in \frac{1}{p^\infty}\mathbb{Z}^{>0}$, there is an embedding

$$\rho : \mathbb{F}_p((t))^{1/p^\infty} \to \mathbb{F}_p((t))^{1/p^\infty}$$

which maps $t \mapsto t^q$. Indeed, if $q \in \frac{1}{p^N}\mathbb{Z}^{>0}$ for some $N \in \mathbb{N}$, then there exists an embedding $\rho : \mathbb{F}_p((t))^{1/p^N} \to \mathbb{F}_p((t))^{1/p^N}$ mapping $t \mapsto t^q$, exactly as in [Anscombe and Fehm 2016, Remark 7.9]. Such a map can also be extended uniquely to the perfect hull $\mathbb{F}_p((t))^{1/p^\infty}$.

Now let $\rho : \mathbb{F}_p((t))^{1/p^\infty} \to \mathbb{F}_p((t))^{1/p^\infty}$ be as above. Then, since $f_i(x), g_j(x) \in \mathbb{F}_p[x]$, we get

$$v(g_j(\rho(b))) = v(\rho(g_j(b))) = qv(g_j(b)) < qv(f_i(b)) = v(\rho(f_i(b))) = v(f_i(\rho(b)))$$

for all $1 \le i, j \le n$. We may thus replace our witness b with $a = \rho(b)$.

Since $1 \in qI$, we get $f_i(a) = 0 \bmod (t) \wedge g_j(a) \neq 0 \bmod (t)$, for all $i, j = 1, \dots, n$. The reduction of a modulo (t), seen as a tuple in $\mathbb{F}_p[t^{1/p^\infty}]/t$ via (†), is the desired witness. □

Remark 6.2.2. The same argument used in Proposition 6.2.1 shows that

$$k[t^{1/p^\infty}]/(t^{p-1}) \models \exists x \bigwedge_{1\le i,j\le n} (f_i(x)=0 \wedge g_j(x)\neq 0) \Longleftrightarrow k[\![t]\!]^{1/p^\infty} \models \exists x \bigwedge_{1\le i,j\le n} (v(f_i(x)) > v(g_j(x)))$$

where $k = \mathbb{F}_p$ or $\overline{\mathbb{F}}_p$. The argument of Proposition 6.2.1 needs only a slight modification for the converse direction; one needs to take $q \in \frac{1}{p^\infty}\mathbb{Z}$ such that $(p-1) \in qI$ instead of $1 \in qI$ and the same proof goes through.

6.3. ***Proof of Theorem B.*** We may now prove the following:

Theorem B. *Let K be any of the fields $\mathbb{Q}_p(p^{1/p^\infty})$, $\mathbb{Q}_p(\zeta_{p^\infty})$ or $\mathbb{Q}_p^{ab}$. Then the existential theory of $\mathcal{O}_K/(p)$ is decidable in L_{rings}.*

Proof. By the Anscombe–Fehm Theorem, Theorem 2.2.3, the valued fields $(\mathbb{F}_p((t))^{1/p^\infty}, v_t)$ and $(\overline{\mathbb{F}}_p((t))^{1/p^\infty}, v_t)$ are $\exists$-decidable in L_{val}. For $\mathbb{Q}_p(p^{1/p^\infty})$ the conclusion now follows from Lemma 4.4.2(a) and Proposition 6.2.1. For the other two fields, one has to use Lemma 4.4.2(b), (c) and Remark 6.2.2. □

Remark 6.3.1. Note that Corollary A requires decidability in the language $L_{\text{val}}(t)$ on the characteristic p side. However, for the purposes of Theorem B, the Anscombe–Fehm results in L_{val} turned out to be sufficient. This became possible because of Proposition 6.2.1, which "eliminates" any reference to t.

7. Final remarks

7.1. ***An almost decidable field.*** In Section 2.3, we emphasized that *uniform* decidability of $(\mathcal{O}_K/(p^n))_{n\in\omega}$ is key for the decidability of (K, v). Indeed, at least by assuming the decidability of $\mathbb{F}_p\widehat{((t))^{1/p^\infty}}$ in $L_{\text{val}}(t)$, Proposition 3.6.9(b) allows us to produce undecidable valued fields (K, v) with each individual residue ring $\mathcal{O}_K/(p^n)$ being decidable.

Proposition 7.1.1. *Assume $\mathbb{F}_p\widehat{((t))^{1/p^\infty}}$ is decidable in $L_{\text{val}}(t)$. Then there exists a mixed characteristic henselian valued field (K, v) such that:*

(1) *The valued field (K, v) is undecidable in L_{val}.*

(2) *For each $n \in \mathbb{N}$, the ring $\mathcal{O}_K/(p^n)$ is decidable in L_{rings}.*

(3) *The value group (Γ_v, vp) decidable in L_{oag}.*

Proof. For the convenience of the reader, we first review the construction from proof of Proposition 3.6.9(b). Given $\alpha \in 2^\omega$, define inductively:

(1) $K_0 = \mathbb{Q}_p$ and $\pi_0 = p$.

(2) $K_{\alpha\restriction n} = K_{\alpha\restriction(n-1)}(((1+p)^{\alpha(n-1)} \cdot \pi_{\alpha\restriction(n-1)})^{1/p})$ and $\pi_{\alpha\restriction n} = ((1+p)^{\alpha(n-1)} \cdot \pi_{\alpha\restriction(n-1)})^{1/p}$.

We let $K_\alpha = \bigcup_{n\in\omega} K_{\alpha\restriction n}$. Set $\bar{\alpha}_n = \sum_{k=0}^{n-1} \alpha(k) \cdot p^k$. Claim 3 of Proposition 3.6.9 shows that $\widehat{K_\alpha}^\flat = \mathbb{F}_p\widehat{((t))^{1/p^\infty}}$. We shall argue below that any $\widehat{K_\alpha}$ satisfies conditions (2) and (3). On the other hand, since $\widehat{K_\alpha} \not\equiv \widehat{K_\beta}$ for $\alpha \neq \beta$ (see Claim 2, Proposition 3.6.9(b)), we will have that some $\widehat{K_\alpha}$ is undecidable in L_{val}.

Fix $\alpha \in 2^\omega$, set $\bar{a} = \sum_{k\geq 0} \alpha(k)\cdot p^k \in \mathbb{Z}_p$ and $\bar{\alpha}_n = \sum_{k=0}^{n-1} \alpha(k)\cdot p^k \in \mathbb{Z}$ for all $n \in \mathbb{N}^{>0}$ ($\bar{\alpha}_0 = 0$ by convention). One sees that $(1+p)^{p^n} \equiv 1 \bmod p^{n+1}\mathbb{Z}_p$, for all $n \in \mathbb{N}$. It follows that the limit $\lim_{n\to\infty}(1+p)^{\bar{\alpha}_n}$ exists in $\mathbb{Z}_p$ and we denote it by $(1+p)^{\bar{a}}$. Fix $n \in \mathbb{N}^{>0}$ for the rest of the proof.

Claim. We have $t^\sharp = (1+p)^{\bar{a}}\cdot p$ and $t^\sharp \equiv (1+p)^{\bar{\alpha}_{n-1}}\cdot p \bmod p^n \mathcal{O}_{K_\alpha}$.

Proof. We have that $t = (\pi_{\alpha\restriction 0} + (p), \pi_{\alpha\restriction 1} + (p), \dots)$, via the identification $\widehat{\mathbb{F}_p[\![t]\!]^{1/p^\infty}} \cong \varprojlim_\Phi \mathcal{O}_{K_\alpha}/(p)$ (see Remark 3.6.12). Since $\pi_{\alpha\restriction n}^{p^n} = (1+p)^{\bar{\alpha}_n}\cdot p$, we compute $t^\sharp = \lim_{n\to\infty}\pi_{\alpha(n)}^{p^n} = \lim_{n\to\infty}(1+p)^{\bar{\alpha}_n}\cdot p = (1+p)^{\bar{a}}\cdot p$. Since $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n\mathcal{O}_{K_\alpha}$, we also get $t^\sharp \equiv (1+p)^{\bar{\alpha}_{n-1}}\cdot p \bmod p^n\mathcal{O}_{K_\alpha}$. □

As a consequence, we may take $\xi_\alpha = [t] - (1+p)^{\bar{a}}\cdot p$ as a generator of the ideal of $\boldsymbol{A}_{\text{inf}}$ associated to K_α. Consider also the distinguished element $\xi' := [t] - (1+p)^{\bar{\alpha}_{n-1}}\cdot p \in \boldsymbol{A}_{\text{inf}}$ and the associated untilt (K', v'). We have an equality of ideals $(p^n, \xi_\alpha) = (p^n, \xi')$ in $\boldsymbol{A}_{\text{inf}}$ and thus an isomorphism of rings $\mathcal{O}_{K_\alpha}/(p^n) \cong \mathcal{O}_{K'}/(p^n)$.

Having assumed that the valued field $(\widehat{\mathbb{F}_p((t))^{1/p^\infty}}, v_t)$ is decidable in $L_{\text{val}}(t)$ and since ξ' is $\mathbb{F}_p[t]$-computable, we get that the valued field (K', v') is decidable in L_{val} by Theorem A. In particular, the ring $\mathcal{O}_{K_\alpha}/(p^n) \cong \mathcal{O}_{K'}/(p^n)$ is decidable in L_{rings}. The value group $(\Gamma_\alpha, v_\alpha p) \cong \left(\frac{1}{p^\infty}\mathbb{Z}, 1\right)$ is also decidable in L_{oag} with a constant symbol for 1. Since n was arbitrary, this concludes the proof. □

Remark 7.1.2. It seems plausible that a similar construction can be carried out with $\mathbb{F}_p((t^\Gamma))$ instead of $\widehat{\mathbb{F}_p((t))^{1/p^\infty}}$, where $\Gamma = \frac{1}{p^\infty}\mathbb{Z}$, thereby recovering the above result unconditionally. Nevertheless, we do not have a working example at present.

7.2. *Reversing the direction.*

7.2.1. Given that our understanding of decidability problems in characteristic p is limited, our philosophy of reducing decidability questions from mixed characteristic to positive characteristic may seem impractical. Nevertheless, we have already seen two applications in Sections 5 and 6. We also mention another application in [Kartas 2023], which proves an *undecidability* result for the asymptotic theory of $\{K : [K : \mathbb{Q}_p] < \infty\}$ in the language L_{val} with a cross-section, again by transposing a result in positive characteristic.

7.2.2. We shall now demonstrate that the characteristic p difficulties in the language $L_{\text{val}}(t)$ are already encoded in the mixed characteristic setting, by showing a relative decidability result in the opposite direction:

Proposition 7.2.3. *If $\mathbb{Q}_p(p^{1/p^\infty})$ is $\forall^1\exists$-decidable in L_{val}, then $\mathbb{F}_p[\![t]\!]^{1/p^\infty}$ is $\exists^+$-decidable in $L_{\text{val}}(t)$.*

Proof. We may focus on $L_{\text{rings}}(t)$ sentences since $x \in \mathcal{O}$ is $\exists^+$-definable in $L_{\text{rings}}(t)$ (see note 1). Let $f_i(X_1, \dots, X_m, T) \in \mathbb{F}_p[X_1, \dots, X_m, T]$ for $i = 1, \dots, n$. We claim that

$$\mathbb{F}_p[\![t]\!]^{1/p^\infty} \models \exists x_1, \dots, x_m\Bigg(\bigwedge_{1\leq i\leq n} f_i(x_1, \dots, x_m, t) = 0\Bigg)$$

$$\iff \mathbb{F}_p[t^{1/p^\infty}]/(t) \models \forall y \in \mathfrak{m}\exists x_1, \dots, x_m\Bigg(\bigwedge_{1\leq i\leq n} f_i(x_1, \dots, x_m, y) = 0\Bigg).$$

It is enough to prove the claim since $\mathbb{Z}_p[p^{1/p^\infty}]/(p) \cong \mathbb{F}_p[t^{1/p^\infty}]/(t)$ by Lemma 4.4.2(a). We leave it to the reader to write down the $\forall^1\exists$-statement about $\mathbb{Q}_p(p^{1/p^\infty})$ which is equivalent to the one about $\mathbb{F}_p[t^{1/p^\infty}]/(t)$ written above;

$\Rightarrow$: Let $(\alpha_1, \dots, \alpha_m) \in (\mathbb{F}_p[\![t]\!]^{1/p^\infty})^m$ be such that

$$f_1(\alpha_1, \dots, \alpha_m, t) = f_2(\alpha_1, \dots, \alpha_m, t) = \dots = f_n(\alpha_1, \dots, \alpha_m, t) = 0.$$

Let $y \in \mathfrak{m} \subset \mathbb{F}_p[\![t]\!]^{1/p^\infty}$ and $\kappa \in \mathbb{N}$ be such that $y^{p^\kappa} \in \mathbb{F}_p[\![t]\!]$. Then there exists a ring endomorphism ρ on $\mathbb{F}_p[\![t]\!]$ mapping $t \mapsto y^{p^\kappa}$, which extends uniquely to $\mathbb{F}_p[\![t]\!]^{1/p^\infty}$. Let $\beta_i := \rho(\alpha_i)$ for $i = 1, \dots, m$. Since $f_i(X_1, \dots, X_m, T) \in \mathbb{F}_p[X, T]$, we get

$$f_1(\beta_1, \dots, \beta_m, y^{p^\kappa}) = f_2(\beta_1, \dots, \beta_m, y^{p^\kappa}) = \dots = f_n(\beta_1, \dots, \beta_m, y^{p^\kappa}) = 0$$

and thus

$$f_1(\beta_1^{1/p^\kappa}, \dots, \beta_m^{1/p^\kappa}, y) = f_2(\beta_1^{1/p^\kappa}, \dots, \beta_m^{1/p^\kappa}, y) = \dots = f_n(\beta_1^{1/p^\kappa}, \dots, \beta_m^{1/p^\kappa}, y) = 0.$$

In particular, the tuple $(x_1, \dots, x_m) := (\beta_1^{1/p^\kappa}, \dots, \beta_m^{1/p^\kappa})$ is a solution modulo (t) to the above system of equations.

$\Leftarrow$: A generalized version of Greenberg's Theorem due to Moret-Bailly [2012, Corollary 1.2.2] shows that

$$f_1(x_1, \dots, x_m, t) = f_2(x_1, \dots, x_m, t) = \dots = f_n(x_1, \dots, x_m, t) = 0$$

has a solution in $\mathbb{F}_p[\![t]\!]^{1/p^\infty}$ if and only if it has a solution modulo (t^N), for all $N \in \mathbb{N}$. Equivalently, if and only if it has a solution modulo (t^{p^N}) for all $N \in \mathbb{N}$. Using the N-th iterated Frobenius, we see that for any $N \in \mathbb{N}$ we have

$$\mathbb{F}_p[\![t]\!]^{1/p^\infty} \models \exists x_1, \dots, x_m \Big(\bigwedge_{1 \le i \le n} f_i(x_1, \dots, x_m, t) = 0 \bmod t^{p^N} \Big)$$
$$\iff \mathbb{F}_p[\![t]\!]^{1/p^\infty} \models \exists x_1, \dots, x_m \Big(\bigwedge_{1 \le i \le n} f_i(x_1, \dots, x_m, t^{1/p^N}) = 0 \bmod t \Big)$$

and the latter is true by assumption, for any $N \in \mathbb{N}$. □

Remark 7.2.4. By an identical argument, one can prove a similar result for $\mathbb{Q}_p(\zeta_{p^\infty})$ or $\mathbb{Q}_p^{ab}$. In the case of the latter, one gets that $\bar{\mathbb{F}}_p[\![t]\!]^{1/p^\infty}$ is $\exists^+$-decidable in $L_{\text{val}}(t)$, provided that $\mathbb{Q}_p^{ab}$ is $\forall^1\exists$-decidable in L_{val}.

It would be nice to have a version of Proposition 7.2.3 for the full theories. Together with Corollary A, this would yield a Turing equivalence between the theories of $\mathbb{Q}_p(p^{1/p^\infty})$ and $\mathbb{F}_p((t))^{1/p^\infty}$. Nevertheless, Proposition 7.2.3 still suggests that if we eventually want to understand the theories of $\mathbb{Q}_p(p^{1/p^\infty})$, $\mathbb{Q}_p(\zeta_{p^\infty})$ and $\mathbb{Q}_p^{ab}$ (even modest parts of their theories), we would have to face certain characteristic p difficulties, posed in Question 7.2.5 below:

Question 7.2.5. (a) Is $\mathrm{Th}_{\exists^+}(\mathbb{F}_p[[t]]^{1/p^\infty})$ decidable in $L_{\mathrm{val}}(t)$?

(b) Is $\mathrm{Th}_{\exists^+}(\bar{\mathbb{F}}_p[[t]]^{1/p^\infty})$ decidable in $L_{\mathrm{val}}(t)$?

Acknowledgements

A great mathematical debt is owed to E. Hrushovski from whom I learned many of the crucial ideas in this work. I would like to thank J. Koenigsmann for insightful suggestions and his encouragement throughout. Many thanks to T. Scanlon for his hospitality while I was a visitor at UC Berkeley and for many inspiring discussions. I also thank all participants in a study group that took place at Fields Institute in Fall 2021, for their meticulous readings of earlier versions of this work and for pointing out several local corrections. I finally wish to thank two anonymous referees for their thorough reviews.

References

[Anscombe and Fehm 2016] S. Anscombe and A. Fehm, "The existential theory of equicharacteristic henselian valued fields", *Algebra Number Theory* **10**:3 (2016), 665–683. MR Zbl

[Anscombe and Jahnke 2022] S. Anscombe and F. Jahnke, "The model theory of Cohen rings", *Confluentes Math.* **14**:2 (2022), 1–28. MR Zbl

[Anscombe and Kuhlmann 2016] S. Anscombe and F.-V. Kuhlmann, "Notes on extremal and tame valued fields", *J. Symb. Log.* **81**:2 (2016), 400–416. MR Zbl

[Ax and Kochen 1965] J. Ax and S. Kochen, "Diophantine problems over local fields, II: A complete set of axioms for p-adic number theory", *Amer. J. Math.* **87**:3 (1965), 631–648. MR Zbl

[Basarab 1978] S. A. Basarab, "Some model theory for Henselian valued fields", *J. Algebra* **55**:2 (1978), 191–212. MR Zbl

[Bélair 1999] L. Bélair, "Types dans les corps valués munis d'applications coefficients", *Illinois J. Math.* **43**:2 (1999), 410–425. MR Zbl

[Deligne 1984] P. Deligne, "Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0", pp. 119–157 in *Représentations des groupes réductifs sur un corps local*, edited by J.-N. Bernstein et al., Travaux en Cours **8**, Hermann, Paris, 1984. MR Zbl

[Denef and Schoutens 2003] J. Denef and H. Schoutens, "On the decidability of the existential theory of $\mathbb{F}_p[[t]]$", pp. 43–60 in *Valuation theory and its applications* (Saskatoon, SK, 1999), vol. 2, edited by F.-V. Kuhlmann et al., Fields Inst. Commun. **33**, Amer. Math. Soc., Providence, RI, 2003. MR Zbl

[Dittmann 2022] P. Dittmann, "Two examples concerning existential undecidability in fields", preprint, 2022. arXiv 2211.01775

[van den Dries 1999] L. van den Dries, "On the elementary theory of rings of Witt vectors with a multiplicative set of representatives for the residue field", *Manuscripta Math.* **98**:2 (1999), 133–137. MR Zbl

[van den Dries 2014] L. van den Dries, "Lectures on the model theory of valued fields", pp. 55–157 in *Model theory in algebra, analysis and arithmetic* (Cetraro, 2012), edited by H. D. Macpherson and C. Toffalori, Lecture Notes in Math. **2111**, Springer, 2014. MR Zbl

[Eršov 1965] J. L. Eršov, "On elementary theories of local fields", *Algebra i Logika Sem.* **4**:2 (1965), 5–30. In Russian. MR

[Fargues and Fontaine 2014] L. Fargues and J.-M. Fontaine, "Vector bundles on curves and p-adic Hodge theory", pp. 17–104 in *Automorphic forms and Galois representations* (Durham, 2011), vol. 2, edited by F. Diamond et al., London Math. Soc. Lecture Note Ser. **415**, Cambridge Univ. Press, 2014. MR Zbl

[Fargues and Fontaine 2018] L. Fargues and J.-M. Fontaine, *Courbes et fibrés vectoriels en théorie de Hodge p-adique*, Astérisque **406**, Soc. Math. de France, Paris, 2018. MR Zbl

[Hodges 1993] W. Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications **42**, Cambridge University Press, 1993. MR Zbl

[Kartas 2023] K. Kartas, "An undecidability result for the asymptotic theory of p-adic fields", *Ann. Pure Appl. Logic* **174**:2 (2023), art. id. 103203. MR Zbl

[Kazhdan 1986] D. Kazhdan, "Representations of groups over close local fields", *J. Analyse Math.* **47** (1986), 175–179. MR Zbl

[Kedlaya 2006] K. S. Kedlaya, "Finite automata and algebraic extensions of function fields", *J. Théor. Nombres Bordeaux* **18**:2 (2006), 379–420. MR Zbl

[Kedlaya and Liu 2015] K. S. Kedlaya and R. Liu, *Relative p-adic Hodge theory: foundations*, Astérisque **371**, Soc. Math. de France, Paris, 2015. MR Zbl

[Kedlaya and Temkin 2018] K. S. Kedlaya and M. Temkin, "Endomorphisms of power series fields and residue fields of Fargues–Fontaine curves", *Proc. Amer. Math. Soc.* **146**:2 (2018), 489–495. MR Zbl

[Kochen 1975] S. Kochen, "The model theory of local fields", pp. 384–425 in *ISILC Logic Conference* (Kiel, 1974), edited by G. H. Müller et al., Lecture Notes in Math. **499**, Springer, 1975. MR Zbl

[Koenigsmann 2018] J. Koenigsmann, "Decidability in local and global fields", pp. 45–59 in *Proceedings of the International Congress of Mathematicians* (Rio de Janeiro, 2018), vol. 2: Invited lectures, edited by B. Sirakov et al., World Sci. Publ., 2018. MR Zbl

[Krasner 1957] M. Krasner, "Approximation des corps valués complets de caractéristique $p \neq 0$ par ceux de caractéristique 0", pp. 129–206 in *Colloque d'algèbre supérieure* (Brussels, 1956), Établissements Ceuterick, Louvain, 1957. MR Zbl

[Kuhlmann 2016] F.-V. Kuhlmann, "The algebra and model theory of tame valued fields", *J. Reine Angew. Math.* **719** (2016), 1–43. MR Zbl

[Kuhlmann and Rzepka 2023] F.-V. Kuhlmann and A. Rzepka, "The valuation theory of deeply ramified fields and its connection with defect extensions", *Trans. Amer. Math. Soc.* **376**:4 (2023), 2693–2738. MR Zbl

[Lee 2020] J. Lee, "Hyperfields, truncated DVRs, and valued fields", *J. Number Theory* **212** (2020), 40–71. MR Zbl

[Lee and Lee 2021] J. Lee and W. Lee, "On the structure of certain valued fields", *Ann. Pure Appl. Logic* **172**:4 (2021), art. id. 102927. MR Zbl

[Lisinski 2021] V. Lisinski, "Decidability of positive characteristic tame Hahn fields in $\mathcal{L}_t$", preprint, 2021. arXiv 2108.04132

[Lurie 2018] J. Lurie, "The Fargues–Fontaine curve", online notes, 2018, available at https://www.math.ias.edu/~lurie/205.html.

[Macintyre 1986] A. Macintyre, "Twenty years of p-adic model theory", pp. 121–153 in *Logic colloquium* '84 (Manchester, 1984), edited by J. B. Paris et al., Stud. Logic Found. Math. **120**, North-Holland, Amsterdam, 1986. MR Zbl

[Marker 2002] D. Marker, *Model theory: an introduction*, Graduate Texts in Mathematics **217**, Springer, 2002. MR Zbl

[Moret-Bailly 2012] L. Moret-Bailly, "An extension of Greenberg's theorem to general valuation rings", *Manuscripta Math.* **139**:1-2 (2012), 153–166. MR Zbl

[Morrow 2019] M. Morrow, "The Fargues–Fontaine curve and diamonds", exposé 1150, pp. 533–571 in *Séminaire Bourbaki* 1978/79, Astérisque **414**, Soc. Math. de France, Paris, 2019. MR Zbl

[Acosta de Orozco and Vélez 1982] M. Acosta de Orozco and W. Y. Vélez, "The lattice of subfields of a radical extension", *J. Number Theory* **15**:3 (1982), 388–405. MR Zbl

[Robinson and Zakon 1960] A. Robinson and E. Zakon, "Elementary properties of ordered abelian groups", *Trans. Amer. Math. Soc.* **96** (1960), 222–236. MR Zbl

[Scanlon 2003] T. Scanlon, "Quantifier elimination for the relative Frobenius", pp. 323–352 in *Valuation theory and its applications* (Saskatoon, SK, 1999), vol. 2, edited by F.-V. Kuhlmann et al., Fields Inst. Commun. **33**, Amer. Math. Soc., Providence, RI, 2003. MR Zbl

[Scholze 2012] P. Scholze, "Perfectoid spaces", *Publ. Math. Inst. Hautes Études Sci.* **116** (2012), 245–313. MR Zbl

[Scholze 2013] P. Scholze, "Perfectoid spaces: a survey", pp. 193–227 in *Current developments in mathematics* (Cambridge, MA, 2012), edited by D. Jerison et al., Int. Press, Somerville, MA, 2013. MR Zbl

[Scholze 2014] P. Scholze, "Perfectoid spaces and their applications", pp. 461–486 in *Proceedings of the International Congress of Mathematicians* (Seoul, 2014), vol. 2, edited by S. Y. Jang et al., Kyung Moon Sa, Seoul, 2014. MR Zbl

[Scholze 2021] P. Scholze, "How many untilts?", MathOverflow post, 2021, available at https://mathoverflow.net/q/390522.

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, 1979. MR Zbl

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, 1997. MR Zbl

[Ziegler 1972] M. Ziegler, *Die elementare Theorie der henselschen Körper*, Ph.D. thesis, Universität zu Köln, 1972, available at https://tinyurl.com/3ez4sb2a.

Communicated by Anand Pillay
Received 2020-02-14 Revised 2022-12-16 Accepted 2023-04-13

kartas@imj-prg.fr *Institut Mathématique de Jussieu, CNRS/IMJ-PRG, Paris, France*

ALGEBRA AND NUMBER THEORY 18:2 (2024)
https://doi.org/10.2140/ant.2024.18.249

Differentially large fields

Omar León Sánchez and Marcus Tressl

We introduce the notion of *differential largeness* for fields equipped with several commuting derivations (as an analogue to largeness of fields). We lay out the foundations of this new class of “tame” differential fields. We state several characterizations and exhibit plenty of examples and applications. Our results strongly indicate that differentially large fields will play a key role in differential field arithmetic. For instance, we characterize differential largeness in terms of being existentially closed in their power series field (furnished with natural derivations), we give explicit constructions of differentially large fields in terms of iterated powers series, we prove that the class of differentially large fields is elementary, and we show that differential largeness is preserved under algebraic extensions, therefore showing that their algebraic closure is differentially closed.

1. Introduction

Recall that a field K is called *large* (or *ample*) if every irreducible variety defined over K with a smooth K-rational point has a Zariski-dense set of K-rational points. Equivalently, every variety defined over K that has a $K((t))$-rational point also has a K-rational point. Large fields constitute one of the widest classes of *tame fields*: namely, every class of fields that serves as a *locality*, in the sense that universal local-global principles hold, consists entirely of large fields; see [3; 28]. For example, all local fields are large and so are pseudoclassically closed fields (like PAC or PRC fields), the field of totally real numbers, as well as the quotient field of any local Henselian domain [27]. On the other hand, number fields and algebraic function fields are not large by Faltings’ theorem and its function field version.

One of the most remarkable Galois-theoretic applications of large fields, due to Pop [26], states every finite split embedding problem over large fields has proper regular solutions. In particular, the regular

León Sánchez was partially supported by EPSRC grant EP/V03619X/1.
MSC2020: primary 12E99, 12H05; secondary 03C60, 34M25.
Keywords: differential fields, large fields, Taylor morphism, Picard–Vessiot theory, elimination theory, existentially closed structures.

inverse Galois problem is solvable over all large fields. Pop's work (and the work of many others) demonstrates that "over large fields one can do a lot of interesting mathematics". For instance, large fields have been widely used to tackle long-standing problems in field arithmetic: inverse Galois theory, torsors of finite groups, elementary theory of function fields, extremal-valued fields, to name a few. We refer the reader to Pop's survey [28] for earlier and current developments on the subject, and to [3] for a list of open problems.

In this paper we introduce the notion of *differential largeness* in the class of differential fields of characteristic zero in several commuting derivations. We lay out the foundations of this new and exciting class of "tame" differential fields, prove several characterizations (see Theorem 4.3, Proposition 4.7), and exhibit many examples (see Proposition 4.7, Corollary 4.8(ii), Theorems 5.12 and 5.18, and 5.2) and applications (see Corollaries 4.8(iii) and 5.13, Theorems 5.7 and 5.12, Lemma 5.9, Proposition 5.16, and 5.14 and 5.19). An outline of these is given in the rest of the introduction.

In order to give the definition of a differentially large field we need one piece of terminology. We say that a field K is *existentially closed* (e.c.) in L if every variety defined over K that has an L-rational point also has a K-rational point. Hence, a field is large just if it is e.c. in its Laurent series field. Similarly, a differential field K (of characteristic zero throughout, in $m \geq 1$ commuting derivations) is e.c. in a differential field extension L if every differential variety defined over K that has an L-rational differential point also has a K-rational differential point. (See Proposition 2.2 for other characterizations of this property.)

A differential field is *differentially large* if it is large as a pure field, and for every differential field extension L/K, if K is e.c. in L as a field, then it is e.c. in L as a differential field. For example differentially closed fields (a.k.a. *constrainedly closed* in Kolchin terminology) and closed ordered differential fields in the sense of [32] are differentially large.

In Theorem 4.3, we establish several equivalent formulations of differential largeness that justify why indeed this is the right differential analogue of largeness. For instance, we characterize them in terms of differential varieties having a Kolchin-dense set of rational points as long as they have suitable "smooth" rational points. In addition, we prove (in analogy to the characterization of largeness in terms of being e.c. in its Laurent series field) that a differential field K is differentially large just if it is e.c. in its power series field $K((t_1, \dots, t_m))$ as differential fields. The derivations on the power series field are given by the unique commuting derivations $\delta_1, \dots, \delta_m$ extending the ones on K that are compatible with infinite sums and satisfy $\delta_i(t_j) = dt_j/dt_i$.

A key tool in establishing our formulations of differential largeness (and further results) is the introduction of a twisted version of the classical Taylor morphism associated to a ring homomorphism $\varphi : A \to B$ for a given differential ring A. We explain this briefly in the case of one derivation δ. Recall that the Taylor morphism $T_\varphi(a) = \sum_{k\geq 0}\big(\varphi(\delta^k(a))/k!\big)\,t^k$ defines a differential ring homomorphism $(A, \delta) \to (B[\![t]\!], \mathrm{d}/\mathrm{d}t)$. Typically this is applied when A is a differential K-algebra for a differential field K and φ is a (not necessarily differential) K-algebra homomorphism $A \to K$ (so $B = K$). If the derivation on K is trivial, then T_φ is in fact a (differential) K-algebra homomorphism and in this context it was used by Seidenberg, for example, to establish his embedding theorem for differential fields into meromorphic functions. However, if the derivation on K is not trivial, then T_φ is not a K-algebra homomorphism, i.e, it is not an extension of φ. On the other hand, T_φ can be "twisted" in order to obtain a natural differential K-algebra homomorphism $T_\varphi^* : (A, \delta) \to (K[\![t]\!], \partial)$, where ∂ is the natural derivation extending the given one on K and satisfying $\partial(t) = 1$. This is established in Proposition 3.5, where we use it to derive the following result that is of independent interest (for instance, in the analysis of formal solutions to PDEs; see [30]), and is deployed in most parts of this article (in the more general form Corollary 3.6).

Theorem. *Let (K, δ) be a differential field of characteristic zero that is large as a field and let (S, δ) be a differentially finitely generated K-algebra. If there is a K-algebra homomorphism $S \to L$ for some field extension L/K in which K is e.c.* (*as a field*), *then there is a differential K-algebra homomorphism $(S, \delta) \to (K[\![\boldsymbol{t}]\!], \partial)$.*

Differentially large fields will play a very similar role in differential field arithmetic to that played by large fields in field arithmetic (of characteristic zero). The principal indicators for this are established in this paper (in Sections 4 and 5). We show that:

(a) A differential field K is differentially large if and only if it is existentially closed in its power series field $K((t_1, \dots, t_m))$ furnished with m natural derivations extending those on K satisfying $\partial_i(t_j) = dt_j/dt_i$; see Theorem 4.3.

(b) Every large field equipped with commuting derivations has an extension to a differentially large field L such that K is e.c. in L as a pure field; see Corollary 4.8.

(c) Differentially large fields are first-order axiomatizable (see Proposition 4.7 and also Theorem 6.4 for a concrete algebro-geometric description), and the elimination theory of the underlying field transfers to the differential field; see Corollary 4.8.

(d) Differential largeness is preserved under algebraic extensions. Thus, the algebraic closure of a differentially large field is differentially closed. This provides many new differential fields with minimal differential closures; see Theorem 5.12.

(e) Differentially large fields (and differentially closed fields) can be produced by iterated power series constructions; see 5.2.

(f) The existential theory of the class of differentially large fields is the existential theory of the differential field $\mathbb{Q}((\boldsymbol{t}_1))((\boldsymbol{t}_2))$ equipped with its natural derivations; see Theorem 5.7.

(g) Differentially large fields are Picard–Vessiot closed; see Lemma 5.9.

(h) Connected differential algebraic groups defined over differentially large fields have a Kolchin-dense set of rational points; see 5.15.

(i) A differentially large field is PAC (at the field level) if and only if it is pseudodifferentially closed; see Theorem 5.18.

Large fields have also made an appearance in the (inverse) Picard–Vessiot theory of linear ordinary differential equations. In [2], it is shown that if K is a large field of infinite transcendence degree, then every linear algebraic group over K is a Picard–Vessiot group over $(K(x), \mathrm{d}/\mathrm{d}x)$. We envisage that differentially large fields will make a similar appearance in the parameterized Picard–Vessiot theory and its differential (constrained) coholomogy. The first application in this direction already appears in a paper of the first author with A. Pillay [18] using an earlier draft of the present paper. They show that if an ordinary differential field (K, δ) is differentially large and bounded as a field (that is, has finitely many extensions of degree n, for each $n \in \mathbb{N}$), then for any linear differential algebraic group G over K the differential Galois cohomology $H^1_\delta(K, G)$ is finite. This can be thought of as a differential analogue of the classical result of Serre stating that if a field K is bounded then the Galois cohomology $H^1(K, G)$ is finite for any linear algebraic group over K.

2. Preliminaries

All rings and algebras in this article are assumed to be commutative and unital. We also assume that all our fields are of characteristic zero.

We briefly summarize the key notions and terminology, mostly from differential algebra, that we will freely use throughout the paper (especially in Section 4 where we give several equivalent formulations of differential largeness). We make a few remarks on the notion of existentially closed differential ring extensions, we recall the structure theorem for finitely generated differential algebras, and give a quick review of jets and prolongation spaces.

Recall that a derivation on a ring R is an additive map $\delta : R \to R$ satisfying the Leibniz rule

$$\delta(rs) = \delta(r)s + r\delta(s) \quad \text{for all } r, s \in R.$$

Throughout, a differential ring $R = (R, \Delta)$ is a ring R equipped with a distinguished set of *commuting* derivations $\Delta = \{\delta_1, \dots, \delta_m\}$. Usually the order of the derivations does matter, but it will either be clear from the context or we will make it explicit. We also allow the case when $m = 0$, in which case we are simply talking of rings with no additional structure.

Given a differential ring R, a differential R-algebra A is an R-algebra equipped with derivations $\Delta = \{\delta_1, \dots, \delta_m\}$ such that the structure map $R \to A$ is a differential ring homomorphism. If L is another differential R-algebra which is also a field, then an *L-rational point* of A is a differential R-algebra homomorphism $A \to L$. This terminology is in line with the standard language of algebraic geometry, where A is thought of as $R\{x_1, \dots, x_n\}/I$, with I a differential ideal of the differential polynomial ring $R\{x_1, \dots, x_n\}$, and the differential R-algebra homomorphisms $A \to L$ are coordinate free descriptions of the common differential zeroes $a \in L^n$ of the polynomials from I (via evaluation at a).

For the basics in differential algebra, such as differential field extensions and differentially closed fields (also called constrainedly closed which is the differential analogue of algebraically closed), we refer the reader to the excellent book of Kolchin [12].

2.1. Definition (existentially closed extensions). Fix $m \geq 0$. Let $B = (B, \delta_1, \dots, \delta_m)$ be a differential ring and let A be a differential subring of B. (If $m = 0$, B is just a ring and A is a subring.) Then A is said to be *existentially closed (e.c.) in B* if for every $n \in \mathbb{N}$ and all finite collections $\Sigma, \Gamma \subseteq A\{x_1, \dots, x_n\}$ of differential polynomials in m derivations and n differential variables, if there is a common solution in B^n of $P = 0$ and $Q \neq 0$ ($P \in \Sigma$, $Q \in \Gamma$), then such a solution may also be found in A^n.

We are mainly interested in the case when $A = K$ is a differential field and in this case we will use the following properties (in the case $m = 0$, differentially finitely generated, differential field, etc. should be understood as finitely generated, field, etc., and differentially closed field should be understood as algebraically closed field and Kolchin topology should be understood as Zariski topology). We make heavy use of the following properties.

2.2. Proposition. *In the notation of Definition 2.1*:

(i) *If K is e.c. in B, then one easily checks that B is a domain and that K is also e.c. in* $\mathrm{qf}(B)$.

(ii) *If B is also a differential field, then K is e.c. in B if and only if every differentially finitely generated K-algebra S that possesses a differential point $S \to B$, also possesses a differential point $S \to K$. The reason is that if B is a field then the inequalities $Q \neq 0$ in the definition of existentially closed above may be replaced by the equality $y \cdot Q(x) - 1 = 0$, where y is a new variable.*

(iii) *If B is a differentially finitely generated K-algebra then the following are equivalent*:

(a) *K is e.c. in B.*

(b) *B is a domain and for each $b \in B$, if $f(b) = 0$ for every differential K-rational point $f : B \to K$, then $b = 0$.*[1] (*In particular B has a differential K-rational point.*) *We refer to this property as* ***B has a Kolchin-dense set of differential K-rational points***.

(c) *For all $n \in \mathbb{N}$, each differential prime ideal $\mathfrak{p}$ of $K\{x\}$, $x = (x_1, \dots, x_n)$, with $B \cong_K K\{x\}/\mathfrak{p}$ and each differential field L containing K, the set $V_K = \{a \in K^n \mid \mathfrak{p}(a) = 0\}$ is dense in $V_L = \{a \in L^n \mid \mathfrak{p}(a) = 0\}$ for the* ***Kolchin topology*** *of L^n* (*having zero sets of differential polynomials from $L\{x\}$ as a basis of closed sets*).

(d) *There is some $n \in \mathbb{N}$, a differential prime ideal $\mathfrak{p}$ of $K\{x\}$, $x = (x_1, \dots, x_n)$, with $B \cong_K K\{x\}/\mathfrak{p}$ and a differentially closed field M containing K such that the set V_K is dense in V_M for the K-Kolchin topology of M^n* (*having the zero sets in M^n of differential polynomials from $K\{x\}$ as a basis of closed sets*).

(iv) *If $m = 0$ and B is a finitely generated K-algebra then K is e.c. in B if and only if B is a domain and the set of smooth K-rational points of B is Zariski dense in the L-rational points for any field L containing K. This is a statement in classical algebraic geometry* (*using the formulation* (*c*) *of e.c. in* (iii)). *If in addition K is a large field, then K is e.c. in B if and only if B is a domain that has a smooth K-rational point.*

Proof of (iii). We may assume that B is a domain throughout and write $B = K\{x\}/\mathfrak{p}$, $x = (x_1, \dots, x_n)$. The arguments below go through for any choice of these data. By the differential basis theorem there is

[1] In other words, in the subspace of $\mathrm{Spec}(B)$ consisting of differential prime ideals, the set of maximal and differential ideals with residue field K, is dense.

some finite $\Phi \subseteq K\{x\}$ such that $\mathfrak{p}$ is the radical differential ideal $\sqrt[d]{\Phi}$ generated by Φ. For a differential field L containing K we write $V_L = \{a \in L^n \mid \mathfrak{p}(a) = 0\}$ and $I_L = \{Q \in L\{x\} \mid Q|_{V_L} = 0\}$. If L is differentially closed, then the differential Nullstellensatz [12, Chapter IV, section 3, Theorem 2, p. 147] says $I_L = \sqrt[d]{\mathfrak{p}}$ (in $L\{x\}$).

(a) $\Rightarrow$ (b). If K is e.c. in B and $b \in B \setminus \{0\}$, then take $Q \in K\{x\}$ with $b = Q(x+\mathfrak{p})$. Since in B we have a solution of $\Phi = 0$ and $Q \neq 0$, there is also a solution $a \in K^n$ and evaluation $K\{x\} \to K$ at a factors through a differential K-rational point $B \to K$ that is nonzero at b.

(b) $\Rightarrow$ (c). Let M be a differentially closed field containing L such that the fixed field of the group of differential K-automorphisms of M is K (for example, M could be a sufficiently saturated differentially closed field or, in Kolchin's terminology, a universal differential extension of K). It suffices to show that V_K is dense in V_M for the Kolchin topology of M^n. Let W be the closure of V_K in M^n for the Kolchin topology of M^n and let $J = \{Q \in M\{x\} \mid Q|_W = 0\}$. Then every differential K-automorphism of M fixes W setwise and so also fixes J setwise. Using our assumption on M we see that the differential field of definition of J is contained in K; hence, the differential ideal J is generated as an ideal by $J \cap K\{x\}$. On the other hand, we have $I_M \cap K\{x\} = \mathfrak{p}$. As $W \subseteq V_M$ we get $\mathfrak{p} \subseteq I_M \subseteq J$ and we claim that $\mathfrak{p} = J \cap K\{x\}$. Take $P \in J \cap K\{x\}$. Then P vanishes on V_K, which says that the element $P + \mathfrak{p} \in B$ is mapped to 0 by all differential K-rational points of B. By (b), this implies $P + \mathfrak{p} = 0$ in B, in other words $P \in \mathfrak{p}$. We have shown that $\mathfrak{p} = I_M \cap K\{x\} = J \cap K\{x\}$, which implies $W = V_M$ as required.

(c) $\Rightarrow$ (d). This is trivial.

(d) $\Rightarrow$ (a). Let $\Sigma = \{P_1, \dots, P_s\}$, $\Gamma \subseteq K\{y\}$ be finite, $y = (y_1, \dots, y_r)$, and assume there is some $c \in B^r$ with $\Sigma(c) = 0$ and $\Gamma(c) \neq 0$. We need to find some $a \in K^r$ with $\Sigma(a) = 0$ and $\Gamma(a) \neq 0$. Since B is a domain we may assume that $\Gamma = \{Q(y)\}$ is a singleton. We write $c_i = H_i(x + \mathfrak{p})$ with $H_i \in K\{x\}$ and $H = (H_1, \dots, H_r)$. Then $\Sigma(c) = 0$ and $Q(c) \neq 0$ means $P_1(H), \dots, P_s(H) \in \mathfrak{p}$ and $Q(H) \notin \mathfrak{p}$. Since M is differentially closed and $Q(H) \notin \mathfrak{p} = K\{x\} = I_M \cap K\{x\}$ there is some $d \in V_M$ with $Q(H(d)) \neq 0$. By (d) and because $Q(H) \in K\{x\}$, there is some $b \in V_K$ with $Q(H(b)) \neq 0$. Since $P_i(H) \in \mathfrak{p}$ we also know $P_i(H(b)) = 0$. Hence, the tuple $a = (H_1(b), \dots, H_r(b)) \in K^r$ solves the given system. □

If B is a differential K-algebra we will say that K *is existentially closed in B as a field* if it is e.c. in B when we forget about the derivations; hence if the above condition holds true for systems Σ, Γ of ordinary (nondifferential) polynomials. If we want to emphasize that the derivations are to be taken into account we say K *is existentially closed in B as a differential field.*

2.3. Theorem (structure theorem for finitely generated differential algebras). *Let K be a differential field (of characteristic zero) and let S be a differential K-algebra that is differentially finitely generated and a domain. Then,* by [33], *there are K-subalgebras A, P of S and an element $h \in A \setminus \{0\}$ such that A is a finitely generated K-algebra, P is a polynomial K-algebra ($P \cong_K K[T]$ for some possibly infinite set T of indeterminates) and the natural homomorphism $A_h \otimes_K P \to S_h$ given by multiplication is an isomorphism. Note that in general neither A_h nor P is differential.*

2.4. Definition. Let K be a differential field and let S be a differentially finitely generated K-algebra that is a domain. A *decomposition* of S consists of (not necessarily differential) K-subalgebras A, P such that

(a) A is a finitely generated K-algebra and P is a polynomial K-algebra, and

(b) the natural map $A \otimes_K P \to S$ given by multiplication is an isomorphism.

If S possesses a decomposition we say that S is *composite* and we indicate the data of a decomposition by writing $S = A \otimes P$.

2.5. Corollary. *Let K be a differential field and let S be a differentially finitely generated K-algebra. Let $f : S \to L$ be a differential K-algebra homomorphism to some differential field extension L of K.*

(i) *There is a differential K-subalgebra $S_0 \subseteq L$ that is composite and contains the image of f.*

(ii) *If K is e.c. in L as a field, then there is a K-algebra homomorphism $S \to K$.*

Proof. (i). Let $\mathfrak{p}$ be the kernel of f. Then $S/\mathfrak{p}$ is again a differentially finitely generated K-algebra and so we may assume that $\mathfrak{p} = 0$ and $S \subseteq L$. By Theorem 2.3, $S_h \cong_K A_h \otimes_K P$ where A is a finitely generated K-subalgebra of S, $h \in A$, and P is a polynomial K-algebra, $P \subseteq S$. As $S \subseteq L$, we have $A_h \subseteq L$. Hence, we may take $S_0 = S_h$.

(ii). Take S_0 as in (i) and A, P for S_0 as in Definition 2.4. Since A is a finitely generated K-subalgebra of L and K is e.c. in L as a field, there is a K-algebra homomorphism $A \to K$. Since P is a polynomial K-algebra there is also a K-algebra homomorphism $P \to K$. Hence, by the universal property of the tensor product there is a K-algebra homomorphism $S \to K$. □

We recall the basic objects of differential algebraic geometry in the sense of Kolchin [12], and the constructions of jets and prolongations. Some parts are notationally heavy but we try to only introduce those that we will need (and freely use) in coming sections.

2.6. Definition (differential varieties, jets and prolongations). We work inside a (sufficiently saturated or universal) differentially closed field $(\mathbb{U}, \Delta)$, and K denotes a differential subfield of $\mathbb{U}$. A *Kolchin-closed* subset of $\mathbb{U}^n$ is the common zero set of a set of differential polynomials over $\mathbb{U}$ in n differential variables; such sets are also called *affine differential varieties*. If the defining polynomials can be chosen with coefficients in K we say the set is *defined over K*.

By a *differential variety V* we mean a topological space which has as finite open cover $V_1, \dots, V_s$ with each V_i homeomorphic to an affine differential variety (inside some power of $\mathbb{U}$) such that the transition maps are regular as differential morphisms; see [15, Chapter 1, section 7]. We will say that the differential variety is over K when all objects and morphisms can be defined over K. This definition also applies to our use of algebraic varieties, replacing Kolchin-closed with Zariski-closed in powers of $\mathbb{U}$ (recall that $\mathbb{U}$ is algebraically closed and a universal domain for algebraic geometry in Weil's "foundations" sense).

2.7. Notation. We fix integers $n > 0$ and $r \geq 0$, and set

$$\Gamma_n(r) = \left\{ (\xi, i) \in \mathbb{N}^m \times \{1, \dots, n\} \mid \sum_{i=1}^{m} \xi_i \leq r \right\}.$$

The *r-th nabla map* $\nabla_r : \mathbb{U}^n \to \mathbb{U}^{\alpha(n,r)}$ with $\alpha(n,r) := |\Gamma_n(r)| = n \cdot \binom{r+m}{m}$ is defined by

$$\nabla_r(x) = (\delta^\xi x_i : (\xi, i) \in \Gamma_n(r)),$$

where $x = (x_1, \dots, x_n)$ and $\delta^\xi = \delta_1^{\xi_1} \cdots \delta_m^{\xi_m}$. We order the elements of the tuple $(\delta^\xi x_i : (\xi, i) \in \Gamma_n(r))$ according to the canonical orderly ranking of the indeterminates $\delta^\xi x_i$; that is,

$$\delta^\xi x_i < \delta^\zeta x_j \iff \left(\sum \xi_k, i, \xi_1, \dots, \xi_m\right) <_{\text{lex}} \left(\sum \zeta_k, j, \zeta_1, \dots, \zeta_m\right). \tag{2-1}$$

Let $\mathbb{U}_r := \mathbb{U}[\epsilon_1, \dots, \epsilon_m]/(\epsilon_1, \dots, \epsilon_m)^{r+1}$ where the ϵ_i's are indeterminates, and let $e : \mathbb{U} \to \mathbb{U}_r$ denote the ring homomorphism

$$x \mapsto \sum_{\xi \in \Gamma_1(r)} \frac{1}{\xi_1! \cdots \xi_m!} \, \delta^\xi(x) \, \epsilon_1^{\xi_1} \cdots \epsilon_m^{\xi_m}.$$

We call e the exponential $\mathbb{U}$-algebra structure of $\mathbb{U}_r$. To distinguish between the standard and the exponential algebra structure on $\mathbb{U}_r$, we denote the latter by $\mathbb{U}_r^e$.

2.8. Definition. Given an algebraic variety X the r-th *prolongation* τX is the algebraic variety given by taking the $\mathbb{U}$-rational points of the classical Weil descent (or Weil restriction) of $X \times_{\mathbb{U}} \mathbb{U}_r^e$ from $\mathbb{U}_r$ to $\mathbb{U}$. Note that the base change $V \times_{\mathbb{U}} \mathbb{U}_r^e$ is with respect to the exponential structure while the Weil descent is with respect to the standard $\mathbb{U}$-algebra structure.

For details and properties of prolongation spaces we refer to [21, §2]; for a more general presentation, see [20]. In particular, it is pointed out there that the prolongation $\tau_r X$ always exist when X is quasiprojective (an assumption that we will adhere to later on). A characterizing feature of the prolongation is that for each point $a \in X = X(\mathbb{U})$ we have $\nabla_r(a) \in \tau_r X$. Thus, the map $\nabla_r : X \to \tau_r X$ is a differential regular section of $\pi_r : \tau_r X \to X$ the canonical projection induced from the residue map $\mathbb{U}_r \to \mathbb{U}$. We note that if X is defined over the differential field K then $\tau_r X$ is defined over K as well.

In fact, τ_r as defined above is a functor from the category of algebraic varieties over K to itself, and the maps $\pi_r : \tau_r X \to X$ and $\nabla_r : X \to \tau_r X$ are natural. The latter means that for any morphism of algebraic varieties $f : X \to Y$ we get

$$f \circ \pi_{r,X} = \pi_{r,Y} \circ \tau_r f \quad \text{and} \quad \tau_r f \circ \nabla_{r,X} = \nabla_{r,Y} \circ f. \tag{2-2}$$

If G is an algebraic group, then $\tau_r G$ also has the structure of an algebraic group. Indeed, since τ_r commutes with products, the group structure is given by

$$\tau_r(*) : \tau_r G \times \tau_r G \to \tau_r G,$$

where $*$ denotes multiplication in G. By the right-most equality in (2-2), the map $\nabla_r : G \to \tau_r G$ is an injective group homomorphism. Hence, $\nabla_r(G)$ is a differential algebraic subgroup of $\tau_r G$. We will use this in 5.15 below.

Assume that V is a differential variety which is given as a differential subvariety of a quasiprojective algebraic variety X. We define the r-th jet of V to be the Zariski-closure of the image of V under the r-th nabla map $\nabla_r : X \to \tau_r X$; that is,

$$\mathrm{Jet}_r\, V = \overline{\nabla_r(V)}^{\mathrm{Zar}} \subseteq \tau_r X.$$[2]

The jet sequence of V is defined as $(\mathrm{Jet}_r\, V : r \geq 0)$. Note that this sequence determines V. Indeed,

$$V = \{a \in X : \nabla_r(a) \in \mathrm{Jet}_r\, V \text{ for all } r \geq 0\}.$$

2.9. General Assumption. Throughout we assume, whenever necessary for the existence of jets, that our differential varieties are given as differential subvarieties of quasiprojective algebraic varieties. Of course, in the affine case this is always the case. It is worth noting, as it will be used in 5.15, that for connected differential algebraic groups this is also true. Indeed, by [23, Corollary 4.2(ii)] every such group embeds into a connected algebraic group and the latter is quasiprojective by Chevalley's theorem.

3. The Taylor morphism

In parallel to the characterization of large fields in terms of being e.c. in Laurent series, we will prove in Theorem 4.3 that differential largeness can be characterized similarly. For this, we will make use of a *twisted* Taylor morphism. In this section, we give a description of this morphism and use it to construct solutions in power series to systems of differential equations (see Corollary 3.6).

3.1. Setup. Let (A, Δ) be a differential ring with commuting derivations $\Delta = \{\delta_1, \dots, \delta_m\}$. Recall that given a ring homomorphism $\varphi : A \to B$ (where B is a $\mathbb{Q}$-algebra), the Taylor morphism. $T^{\varphi}_{\Delta} : A \to B[\![\boldsymbol{t}]\!]$, where $\boldsymbol{t} = (t_1, \dots, t_m)$, is defined as

$$a \mapsto \sum_{\alpha} \frac{\varphi(\delta^{\alpha} a)}{\alpha!}\, \boldsymbol{t}^{\alpha},$$

where we make use of multi-index notation. Namely, $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{N}^m$, $\alpha! = \alpha_1! \cdots \alpha_m!$, $\delta^{\alpha} = \delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m}$, and $\boldsymbol{t}^{\alpha} = t_1^{\alpha} \cdots t_m^{\alpha_m}$. It is a straightforward computation to check that T^{φ}_{Δ} is a differential ring homomorphism

$$(A, \Delta) \to \left(B[\![\boldsymbol{t}]\!], \frac{\mathrm{d}}{\mathrm{d}t_1}, \dots, \frac{\mathrm{d}}{\mathrm{d}t_m} \right).$$

For every such family of commuting derivations Δ on A, there is a unique extension to $A[\![\boldsymbol{t}]\!]$ such that the derivations commute with meaningful sums[3] and map all t_i's to 0. We continue to denote these derivations on $A[\![\boldsymbol{t}]\!]$ by $\Delta = \{\delta_1, \dots, \delta_m\}$; note that they still commute with each other. We work with the derivations $\delta_i + \mathrm{d}/\mathrm{d}t_i$, for $i = 1, \dots, m$, on $A[\![\boldsymbol{t}]\!]$; again these commute with each other. Assuming that A is

[2] Notice that $\mathrm{Jet}_r\, V$ is not the jet space defined in [20, 5.3].

[3] In the sense of [12, Chapter 0, section 13, p. 30]; specifically, if $(f_i)_{i \in \mathbb{N}}$ is a sequence that converges to 0 in the $(\boldsymbol{t})$-adic topology of $K[\![\boldsymbol{t}]\!]$, then $\sum_i f_i$ is meaningful.

a $\mathbb{Q}$-algebra, we now study the algebraic properties of the Taylor morphism associated to the evaluation map

$$\mathrm{ev} : A[\![\boldsymbol{t}]\!] \to A[\![\boldsymbol{t}]\!], \quad f \mapsto f(0, \dots, 0).$$

For instance, we show that the map from $\mathrm{Der}(A)$ to ring endomorphisms of $A[\![t]\!]$ given by $\delta \mapsto T^{\mathrm{ev}}_{\delta+\mathrm{d}/\mathrm{d}t}$ is a monoid homomorphism when restricted to any submonoid of commuting derivations. Here the monoid structure on $\mathrm{Der}(A)$ is just addition of derivations (and so is indeed a group), while the monoid structure on ring endomorphisms is composition. Note that as a consequence $T^{\mathrm{ev}}_{\delta+\mathrm{d}/\mathrm{d}t}$ is a differential ring isomorphism, because $T^{\mathrm{ev}}_{\delta+\mathrm{d}/\mathrm{d}t}$ has compositional inverse $T^{\mathrm{ev}}_{-\delta+\mathrm{d}/\mathrm{d}t}$ and $T^{\mathrm{ev}}_{\mathrm{d}/\mathrm{d}t}$ is the identity map on $A[\![t]\!]$. We state all this more generally below.

We first introduce some convenient notation and terminology. Let $\Delta = \{\delta_1, \dots, \delta_m\}$ and $\Omega = \{\partial_1, \dots, \partial_m\}$ be families of commuting derivations on A. We say that these families commute if δ_i commutes with ∂_j for all $1 \le i, j \le m$; when this is the case, we denote by $\Delta + \Omega$ the family of commuting derivations on A given by $\{\delta_1 + \partial_1, \dots, \delta_m + \partial_m\}$. Note that the natural extensions of Δ and Ω to $A[\![\boldsymbol{t}]\!]$, as discussed above, commute with the family

$$\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}} := \left\{\frac{\mathrm{d}}{\mathrm{d}t_1}, \dots, \frac{\mathrm{d}}{\mathrm{d}t_m}\right\}.$$

Therefore, the family of derivations $\Delta + \Omega + \mathrm{d}/\mathrm{d}\boldsymbol{t}$ on $A[\![\boldsymbol{t}]\!]$ is a commuting family.

3.2. Theorem. *Let A be a $\mathbb{Q}$-algebra, and let Δ and Ω be families of m-many commuting derivations on A. If Δ and Ω commute, then*

$$T^{\mathrm{ev}}_{\Delta+\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}} = T^{\mathrm{ev}}_{\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ T^{\mathrm{ev}}_{\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}}. \tag{3-1}$$

Proof. For $\alpha \in \mathbb{N}^m$ we use the multi-index notation

$$(\delta + \partial)^\alpha = (\delta_1 + \partial_1)^{\alpha_1} \cdots (\delta_m + \partial_m)^{\alpha_m},$$
$$\left(\delta + \partial + \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right)^\alpha = \left(\delta_1 + \partial_1 + \frac{\mathrm{d}}{\mathrm{d}t_1}\right)^{\alpha_1} \cdots \left(\delta_m + \partial_m + \frac{\mathrm{d}}{\mathrm{d}t_m}\right)^{\alpha_m}.$$

We use the product order $\le$ on $\mathbb{N}^m$ given by $\beta \le \alpha$ if and only if $\beta_i \le \alpha_i$ for $1 \le i \le m$. As the derivations commute, we have the usual binomial identities

$$(\delta + \partial)^\alpha = \sum_{\beta \le \alpha} \binom{\alpha}{\beta} \delta^\beta \partial^{\alpha-\beta} = \sum_{\beta+\gamma=\alpha} \binom{\alpha}{\beta} \delta^\beta \partial^\gamma,$$
$$\begin{aligned}\left(\delta + \partial + \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right)^\alpha &= \sum_{\xi \le \alpha} \sum_{\beta+\gamma=\xi} \binom{\alpha}{\xi}\binom{\xi}{\beta} \delta^\beta \partial^\gamma \frac{\mathrm{d}^{\alpha-\xi}}{\mathrm{d}\boldsymbol{t}} \\ &= \sum_{\beta+\gamma \le \alpha} \binom{\alpha}{\beta+\gamma}\binom{\beta+\gamma}{\beta} \delta^\beta \partial^\gamma \frac{\mathrm{d}^{\alpha-\beta-\gamma}}{\mathrm{d}\boldsymbol{t}}.\end{aligned}$$

Now take $f = \sum_\xi a_\xi \boldsymbol{t}^\xi \in A[\![\boldsymbol{t}]\!]$. We show that both sides of (3-1) applied to f are equal to

$$\sum_\alpha \Big(\sum_{\beta+\gamma \le \alpha} \frac{1}{\beta! \cdot \gamma!}\, \delta^\beta \partial^\gamma (a_{\alpha-\beta-\gamma}) \Big) \boldsymbol{t}^\alpha. \tag{3-2}$$

We begin with the left-hand-side. By definition, the coefficient at $\boldsymbol{t}^\alpha$ of $T^{\mathrm{ev}}_{\Delta+\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}}\big(\sum_\xi a_\xi \boldsymbol{t}^\xi\big)$ is given by

$$\begin{aligned}
\frac{1}{\alpha!}\,\mathrm{ev}\Big[\Big(\delta+\partial+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)^{\alpha}\Big(\sum_{\xi} a_\xi \boldsymbol{t}^\xi\Big)\Big] &= \frac{1}{\alpha!}\mathrm{ev}\Big[\sum_{\beta+\gamma\le\alpha}\binom{\alpha}{\beta+\gamma}\binom{\beta+\gamma}{\beta}\delta^\beta\partial^\gamma\frac{\mathrm{d}^{\alpha-\beta-\gamma}}{\mathrm{d}\boldsymbol{t}}\Big(\sum_{\xi} a_\xi \boldsymbol{t}^\xi\Big)\Big] \\
&= \frac{1}{\alpha!}\mathrm{ev}\Big[\sum_{\beta+\gamma\le\alpha}\sum_{\xi}\binom{\alpha}{\beta+\gamma}\binom{\beta+\gamma}{\beta}\delta^\beta\partial\gamma(a_\xi)\frac{\mathrm{d}^{\alpha-\beta-\gamma}}{\mathrm{d}\boldsymbol{t}}(\boldsymbol{t}^\xi)\Big] \\
&= \frac{1}{\alpha!}\sum_{\beta+\gamma\le\alpha}\binom{\alpha}{\beta+\gamma}\binom{\beta+\gamma}{\beta}\delta^\beta\partial^\gamma(a_{\alpha-\beta-\gamma})\cdot(\alpha-\beta-\gamma)! \\
&= \sum_{\beta+\gamma\le\alpha}\frac{1}{\beta!\cdot\gamma!}\delta^\beta\partial^\gamma(a_{\alpha-\beta-\gamma}),
\end{aligned}$$

which is the term in (3-2). We now compute the right-hand-side of (3-1), when applied to f. The coefficient at $\boldsymbol{t}^\alpha$ is

$$\begin{aligned}
\frac{1}{\alpha!}\,\mathrm{ev}\Big[\Big(\delta+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)^{\alpha}\Big(T^{\mathrm{ev}}_{\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}}\Big(\sum_{\xi} a_\xi \boldsymbol{t}^\xi\Big)\Big)\Big] &= \frac{1}{\alpha!}\,\mathrm{ev}\Big[\Big(\delta+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)^{\alpha}\Big(\sum_{\zeta}\frac{1}{\zeta!}\mathrm{ev}\Big(\Big(\partial+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)^{\zeta}\Big(\sum_{\xi} a_\xi \boldsymbol{t}^\xi\Big)\Big)\boldsymbol{t}^\zeta\Big)\Big] \\
&= \frac{1}{\alpha!}\,\mathrm{ev}\Big[\Big(\delta+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)^{\alpha}\Big(\sum_{\zeta}\frac{1}{\zeta!}\mathrm{ev}\Big(\sum_{\gamma\le\zeta}\binom{\zeta}{\gamma}\partial^\gamma\frac{\mathrm{d}^{\zeta-\gamma}}{\mathrm{d}\boldsymbol{t}}\Big(\sum_{\xi} a_\xi \boldsymbol{t}^\xi\Big)\Big)\boldsymbol{t}^\zeta\Big)\Big] \\
&= \frac{1}{\alpha!}\,\mathrm{ev}\Big[\Big(\delta+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)^{\alpha}\Big(\sum_{\zeta}\frac{1}{\zeta!}(\sum_{\gamma\le\zeta}\binom{\zeta}{\gamma}\partial^\gamma(a_{\zeta-\gamma})\cdot(\zeta-\gamma)!)\boldsymbol{t}^\zeta\Big)\Big] \\
&= \frac{1}{\alpha!}\,\mathrm{ev}\Big[\Big(\delta+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)^{\alpha}\Big(\sum_{\zeta}\sum_{\gamma\le\zeta}\frac{1}{\gamma!}\partial^\gamma(a_{\zeta-\gamma})\boldsymbol{t}^\zeta\Big)\Big] \\
&= \frac{1}{\alpha!}\,\mathrm{ev}\Big[\sum_{\zeta}\sum_{\beta\le\alpha}\sum_{\gamma\le\zeta}\frac{1}{\gamma!}\binom{\alpha}{\beta}\delta^\beta\partial^\gamma(a_{\zeta-\gamma})\frac{\mathrm{d}^{\alpha-\beta}}{\mathrm{d}\boldsymbol{t}}(\boldsymbol{t}^\zeta)\Big] \\
&= \frac{1}{\alpha!}\sum_{\beta\le\alpha}\sum_{\gamma\le\alpha-\beta}\frac{1}{\gamma!}\binom{\alpha}{\beta}\delta^\beta\partial^\gamma(a_{\alpha-\beta-\gamma})\cdot(\alpha-\beta)! \\
&= \sum_{\beta\le\alpha}\sum_{\gamma\le\alpha-\beta}\frac{1}{\beta!\cdot\gamma!}\delta^\beta\partial^\gamma(a_{\alpha-\beta-\gamma}) \\
&= \sum_{\beta+\gamma\le\alpha}\frac{1}{\beta!\cdot\gamma!}\delta^\beta\partial^\gamma(a_{\alpha-\beta-\gamma}),
\end{aligned}$$

which is the term in (3-2), as required. □

What will be important to us is the following consequence.

3.3. Corollary. *For any family of commuting derivations $\Delta=\{\delta_1,\dots,\delta_m\}$ on a $\mathbb{Q}$-algebra A, the Taylor morphism of the evaluation map* $\mathrm{ev}: A[\![\boldsymbol{t}]\!]\to A$ *at* 0 *is an isomorphism of differential rings*

$$T^{\mathrm{ev}}_{\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}:\Big(A[\![\boldsymbol{t}]\!],\,\Delta+\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big)\to\Big(A[\![\boldsymbol{t}]\!],\,\frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\Big).$$

Its compositional inverse is $T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$, *where* $-\Delta$ *is the family of commuting derivations* $\{-\delta_1, \dots, -\delta_m\}$. *Furthermore*, $T^{\mathrm{ev}}_{\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$ *is a differential isomorphism*

$$(A[\![\boldsymbol{t}]\!], \Delta) \to (A[\![\boldsymbol{t}]\!], \Delta).$$

Proof. We recall that $T^{\mathrm{ev}}_{\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$ is a differential homomorphism $(A[\![\boldsymbol{t}]\!], \Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}) \to (A[\![\boldsymbol{t}]\!], \mathrm{d}/\mathrm{d}\boldsymbol{t})$. By Theorem 3.2, we have

$$T^{\mathrm{ev}}_{\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} = T^{\mathrm{ev}}_{\mathrm{d}/\mathrm{d}\boldsymbol{t}} = T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ T^{\mathrm{ev}}_{\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}.$$

It is easy to check that $T^{\mathrm{ev}}_{\mathrm{d}/\mathrm{d}\boldsymbol{t}}$ is the identity on $A[\![\boldsymbol{t}]\!]$. Hence, $T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$ is the compositional inverse of $T^{\mathrm{ev}}_{\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$.

It follows that $T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$ is also a differential isomorphism $(A[\![\boldsymbol{t}]\!], \mathrm{d}/\mathrm{d}\boldsymbol{t}) \to (A[\![\boldsymbol{t}]\!], \Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t})$ — in other words, that $T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ \mathrm{d}/\mathrm{d}t_i = (\delta_i + \mathrm{d}/\mathrm{d}t_i) \circ T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$. Now $\mathrm{d}/\mathrm{d}t_i \circ T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} = T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ (-\delta_i + \mathrm{d}/\mathrm{d}t_i)$, because $T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$ is a differential isomorphism $(A[\![\boldsymbol{t}]\!], -\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}) \to (A[\![\boldsymbol{t}]\!], \mathrm{d}/\mathrm{d}\boldsymbol{t})$. It follows that

$$T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ \frac{\mathrm{d}}{\mathrm{d}t_i} = \delta_i \circ T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} + T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ \left(-\delta_i + \frac{\mathrm{d}}{\mathrm{d}t_i}\right),$$

which implies $T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ \delta_i = \delta_i \circ T^{\mathrm{ev}}_{-\Delta+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$, as claimed in the "furthermore" part. □

We now use Corollary 3.3 to introduce a twisting of the Taylor morphism.

3.4. Definition (the twisted Taylor morphism). We assume all derivations commute. Let A be a differential ring with derivations $\Delta = \{\delta_1, \dots, \delta_m\}$ and let B be a $\mathbb{Q}$-algebra and a differential ring with derivations $\Omega = \{\partial_1, \dots, \partial_m\}$. Let $\varphi : A \to B$ be a (not necessarily differential) ring homomorphism. We write ∂_i again for the extension of ∂_i to $B[\![\boldsymbol{t}]\!]$, $\boldsymbol{t} = (t_1, \dots, t_m)$, obtained from differentiating coefficients as explained in Setup 3.1. Let $\mathrm{ev} : B[\![\boldsymbol{t}]\!] \to B$ be the evaluation map at 0. If we equip $B[\![\boldsymbol{t}]\!]$ with the derivations $\Omega + \mathrm{d}/\mathrm{d}\boldsymbol{t}$ as in Setup 3.1 and apply Corollary 3.3 for (B, Ω), we get a differential ring isomorphism

$$T^{\mathrm{ev}}_{\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}} : \left(B[\![\boldsymbol{t}]\!], \Omega + \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right) \to \left(B[\![\boldsymbol{t}]\!], \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right)$$

with compositional inverse $T^{\mathrm{ev}}_{-\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}}$. Consequently, the map

$$T^{*}_{\varphi} := T^{\mathrm{ev}}_{-\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}} \circ T^{\varphi}_{\Delta} : (A, \Delta) \xrightarrow{T^{\varphi}_{\Delta}} \left(B[\![\boldsymbol{t}]\!], \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right) \xrightarrow{T^{\mathrm{ev}}_{-\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}}} \left(B[\![\boldsymbol{t}]\!], \Omega + \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right)$$

is a differential ring homomorphism $(A, \Delta) \to (B[\![\boldsymbol{t}]\!], \Omega + \mathrm{d}/\mathrm{d}\boldsymbol{t})$, called the *twisted Taylor morphism* of φ. Writing $T^{*}_{\varphi}(a) = \sum_{\alpha} b_{\alpha} \boldsymbol{t}^{\alpha}$, the b_{α}'s are explicitly computed as

$$b_{\alpha} = \frac{1}{\alpha!} \sum_{\beta \le \alpha} (-1)^{\alpha-\beta} \binom{\alpha}{\beta} \partial^{\alpha-\beta}\bigl(\varphi(\delta^{\beta}(a))\bigr).$$

3.5. Proposition. *We use the same assumptions and notation as in Definition 3.4. If* $a \in A$ *and* $\mathbb{Z}\{a\}$ *denotes the differential subring generated by* a *in* A, *one checks readily that*:

(i) $T^{\varphi}_{\Delta}(a) = \varphi(a) \iff \delta^{\alpha}(a) \in \ker(\varphi)$ *for all nonzero* $\alpha \in \mathbb{N}^m$.

(ii) $T^*_\varphi(a) = T^\varphi_\Delta(a) \iff \varphi(\mathbb{Z}\{a\})$ *is contained in the ring of* Ω*-constants of* B.

(iii) $T^*_\varphi(a) = \varphi(a) \iff$ *the restriction of* φ *to* $\mathbb{Z}\{a\}$ *is a differential homomorphism.*

Hence, by the implication $\Leftarrow$ *in* (iii), *if* R *is a differential subring of* A *such that the restriction* $\varphi|_R$ *is a differential ring homomorphism* $(R, \Delta|_R) \to (B, \Omega)$, *then* T^*_φ *extends* φ *and the part showing solid arrows in the following diagram commutes*:

$$\begin{tikzcd}
 & & \left(B\llbracket \boldsymbol{t} \rrbracket, \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right) & \left(B\llbracket \boldsymbol{t} \rrbracket, \Omega + \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{t}}\right) \arrow[l, "T^{\mathrm{ev}}_{\Omega+\mathrm{d}/\mathrm{d}\boldsymbol{t}}"', "\cong"] \arrow[dl, dashed, "\mathrm{ev}"] \\
(A, \Delta) \arrow[urr, "T^\varphi_\Delta"] \arrow[urrr, bend left, "T^*_\varphi"] \arrow[rr, dashed, "\varphi"] & & (B, \Omega) \arrow[u, hook, dashed] \arrow[ur, hook, bend right] & \\
 & (R, \Delta|_R) \arrow[ul, hook] \arrow[ur, "\varphi|_R"'] & &
\end{tikzcd}$$

Notice that all solid arrows in this diagram are differential homomorphisms. The main case for us is when $R = K$ *is a field and* B *is a* K*-algebra such that* φ *is a* K*-algebra homomorphism. In this case the twisted Taylor morphism* T^*_φ *is in fact a differential* K*-algebra homomorphism.*

3.6. Corollary. *Let* (K, Δ) *be a differential field that is large as a field and let* S *be a differentially finitely generated* K*-algebra. If there is a* K*-algebra homomorphism* $S \to L$ *for some field extension* L/K *in which* K *is e.c.* (*as a field, there are no derivations on* L *given*), *then there is a differential* K*-algebra homomorphism* $S \to K\llbracket \boldsymbol{t} \rrbracket$, *where the derivations on* $K\llbracket \boldsymbol{t} \rrbracket$ *are* $\Delta + \mathrm{d}/\mathrm{d}\boldsymbol{t}$ *as described above.*

Proof. Since K as a field is e.c. in L, there is a field extension L' of L which is an elementary extension of the field K. We replace L by L' if necessary and assume that L is an elementary extension of the field underlying K. As K is large, also L is large. We equip L with a set of commuting derivations extending those on K (this is chosen arbitrarily and can always be done).

By Proposition 3.5, there is a differential K-algebra homomorphism $S \to L((\boldsymbol{t}))$. As L is large and also an elementary extension of the field K, we know that K is e.c. as a field in $L((\boldsymbol{t}))$. Hence, by Corollary 2.5(ii) there is a K-algebra homomorphism $S \to K$. By Proposition 3.5 there is a differential K-algebra homomorphism $S \to K\llbracket \boldsymbol{t} \rrbracket$. □

4. Differentially large fields and algebraic characterizations

We introduce the notion of differential largeness and characterize it in multiple ways; see Theorem 4.3 and Proposition 4.7. First we recall the notion of largeness of fields.

4.1. Definition. A field K is said to be *large* (or *ample* in [6, Remark 16.12.3]) if every irreducible affine algebraic variety V over K with a smooth K-point has a Zariski-dense set of K-points (equivalently, K is e.c. in the function field $K(V)$).

Another equivalent formulation of largeness is that K is e.c. in the formal Laurent series field $K((t))$. Examples of large fields are pseudoalgebraically closed fields, pseudoreal closed fields and pseudo p-adically closed fields. By [27] the fraction field of any Henselian local ring is large; in particular, for every field K and all $n \geq 1$, the power series field $K((t_1, \dots, t_n))$ is large.

Convention. Recall that for us a differential field always means a differential field in m commuting derivations $\Delta = \{\delta_1, \dots, \delta_m\}$ and of characteristic zero. For a differential field (K, Δ), we equip the Laurent series field $K((\boldsymbol{t}))$ with the natural derivations extending those on K; namely, $\Delta + \mathrm{d}/\mathrm{d}\boldsymbol{t}$ as described in the previous section.

4.2. Definition. A differential field K is said to be *differentially large* if it is large as a pure field and for every differential field extension L of K the following implication holds:

If K is e.c. in L as a field, then K is e.c. in L as a differential field.

We now provide several algebraic characterizations of differential largeness. These characterizations resemble to some extent the characterizations of largeness of a field and serve as justification for the terminology "differentially large". A further characterization will be given in Proposition 4.7.

4.3. Theorem (characterizations of differential largeness). *Let $K = (K, \Delta)$ be a differential field. The following conditions are equivalent*:

(i) *K is differentially large.*

(ii) *K is e.c. in $K((\boldsymbol{t}))$ as a differential field, where the derivations on $K((\boldsymbol{t}))$ are the natural ones extending those on K.*

(iii) *K is e.c. in $K((\boldsymbol{t}_1)) \dots ((\boldsymbol{t}_k))$ as a differential field for every $k \geq 1$.*

(iv) *K is large as a field and every differentially finitely generated K-algebra that has a K-rational point also has a differential K-rational point.*

(v) *K is large and every composite K-algebra in which K is e.c. as a field has a differential K-rational point.*

(vi) *Every composite differential K-subalgebra S of $K((\boldsymbol{t}))$ has a differential K-rational point.*

(vii) *K is large as a field and for every composite K-algebra $S = A \otimes_K P$, if A has a K-rational point, then S has a differential K-rational point.*

(viii) *K is large as a field and for every composite K-algebra $S = A \otimes_K P$, if the variety defined by A is smooth and if A has a K-rational point $A \to K$, then S has a differential K-rational point.*

(ix) *K is large as a field and for every composite K-algebra $S = A \otimes_K P$, if A has a smooth K-rational point, then S has a Kolchin-dense set of differential K-rational points* (*see Proposition* 2.2(*iii*)(*b*)).

(x) *K is large as a field and for every irreducible differential variety V over K such that for infinitely many $r \geq 0$ the algebraic variety* $\mathrm{Jet}_r(V)$ *has a smooth K-point, the set of differential K-rational points of V is Kolchin dense in V; in other words, for every proper closed differential subvariety $W \subseteq V$ there is a differential K-point in $V \setminus W$.*

Proof. (i) $\Rightarrow$ (iii). In the tower $K \subseteq K((\boldsymbol{t}_1)) \subseteq K((\boldsymbol{t}_1))((\boldsymbol{t}_2)) \subseteq \cdots \subseteq K((\boldsymbol{t}_1)) \ldots ((\boldsymbol{t}_k))$ all fields are large and therefore K is e.c. in $K((\boldsymbol{t}_1)) \ldots ((\boldsymbol{t}_k))$ as a field. So by definition of differential largeness, K is e.c. in $K((\boldsymbol{t}_1)) \ldots ((\boldsymbol{t}_k))$ as a differential field.

(iii) $\Rightarrow$ (ii). This is trivial.

(ii) $\Rightarrow$ (iv). Since K is e.c. in $K((\boldsymbol{t}))$ as a differential field it is also e.c. in $K((\boldsymbol{t}))$ as a field and so K is large as a field. Let S be a differentially finitely generated K-algebra and assume there is a point $S \to K$. Then by Proposition 3.5, there is a differential K-algebra homomorphism $S \to K[\![\boldsymbol{t}]\!]$. By Proposition 2.2(ii) applied to $K \subseteq K((\boldsymbol{t}))$, (ii) entails a differential K-algebra homomorphism $S \to K$.

(iv) $\Rightarrow$ (v). Take A, P for S as in Definition 2.4. Since K is also e.c. in A as a field and A is a finitely generated K-algebra, there is a K-algebra homomorphism $g : A \to K$. Since $S \cong_K A \otimes_K P$ and P is a polynomial K-algebra, g can be extended to a K-algebra homomorphism $S \to K$. Hence, (iv) applies.

(v) $\Rightarrow$ (i). Let L be a differential field extension of K and suppose K is e.c. in L as a field. Let S be a differentially finitely generated K-algebra, which has a differential point $f : S \to L$. By Proposition 2.2(ii) it suffices to find a differential point $S \to K$. By Corollary 2.5(i) we may replace S by a composite K-algebra contained in L and assume that f is the inclusion map $S \hookrightarrow L$. Now (v) applies.

Hence we know that conditions (i)–(v) are equivalent.

(iv) $\Rightarrow$ (vii). If $S = A \otimes_K P$ is composite and A has a K-rational point, then as P is a polynomial K-algebra we may extend this point to a point $S \to K$. By (iv), S has a differential K-rational point.

(vii) $\Rightarrow$ (vi). If $S = A \otimes_K P$ is a composite K-subalgebra of $K((\boldsymbol{t}))$, then as K is a large field, K is e.c. in A as a field and thus A has a K-rational point. Now (vii) applies.

(vi) $\Rightarrow$ (ii). This follows from Corollary 2.5(i) using the characterization Proposition 2.2(ii) of e.c.

Hence we know that conditions (i)–(vii) are equivalent.

(i) $\Rightarrow$ (ix). If $S = A \otimes_K P$ is composite and A has a smooth K-rational point, then as a large field, K is e.c. in A as a field. Since P is a polynomial K-algebra we know that S is a polynomial A-algebra and so A is e.c. in S as a ring. It follows that K is e.c. in S as a field and by (i) (invoke Proposition 2.2(i)) it is then also e.c. in S as a differential field. By Proposition 2.2(iii) we see that S has a Kolchin-dense set of differential K-rational points.

(ix) $\Rightarrow$ (viii). This is trivial.

(viii) $\Rightarrow$ (v). Let $S = A \otimes_K P$ be a composite K-algebra in which K is e.c. as a field. Then K is also e.c. in A as a field and therefore it possesses a smooth K-rational point $f : A \to K$ (see Proposition 2.2(iv)).

Pick $h \in A$ with $f(h) \neq 0$ such that the variety defined by the localization A_h is smooth. We may now apply (viii) to the composite algebra $S_h = A_h \otimes_K P$.

Hence we know that (i)–(ix) are equivalent. Property (x) is just a reformulation of the definition of differential largeness in geometric form as follows. Let $S = K\{x\}/\mathfrak{p}$, $x = (x_1, \dots, x_n)$, be a differentially finitely generated K-algebra and a domain with quotient map $\pi : K\{x\} \to S$. Let V be the differential variety defined by S. Hence, $V = \{a \in M^n \mid \mathfrak{p}(a) = 0\}$, where M is the differential closure of K. Then V is a K-irreducible differential variety defined over K. Now for $r \in \mathbb{N}$, the variety $\mathrm{Jet}_r(V)$ has coordinate ring $A_r := \pi(K\{x\}_{\leq r})$ and S is the union of the chain $(A_r)_r$ of K-subalgebras of S.[4] Clearly K is e.c. in S as a field if and only if K is e.c. in A_r as a field for all (or infinitely many) r. Since K is large, this is equivalent to saying that $\mathrm{Jet}_r(V)$ has a smooth K-point for all (or infinitely many) r. Hence, the assumption about V in (x) precisely says that K is e.c. in S as a field.

On the other hand, the conclusion about V in (x) precisely says that K is e.c. in S as a differential field (use Proposition 2.2(iii)).

This shows that differential largeness is equivalent to (x) formulated for affine differential varieties. But obviously the affine case implies (x) in full. □

4.4. Corollary. *If $K = (K, \delta_1, \dots, \delta_m, \partial_1, \dots, \partial_k)$ is a differentially large field, $m, k \geq 0$, then also $K = (K, \delta_1, \dots, \delta_m)$ is differentially large.*

Proof. This is immediate from the power series characterization in Theorem 4.3(ii). □

4.5. Corollary. *Let $K = (K, \delta_1, \dots, \delta_m, \partial_1, \dots, \partial_k)$ be a differentially large field, $m \geq 0$, $k \geq 1$ and let $C = \{a \in K \mid \partial_1(a) = \cdots = \partial_k(a) = 0\}$ be the constant field of $(\partial_1, \dots, \partial_k)$.*

(i) *C is closed under the derivations $\delta_1, \dots, \delta_m$ and $(C, \delta_1, \dots, \delta_m)$ is e.c. in $(K, \delta_1, \dots, \delta_m)$.*

(ii) *$(C, \delta_1, \dots, \delta_m)$ is differentially large; when $m = 0$, this just says that C is a large field.*

Proof. We write $\delta = (\delta_1, \dots, \delta_m)$ and by a trivial induction we may assume that $k = 1$. Set $\partial = \partial_1$.

(i). Since all derivations commute, C is closed under all derivations. Let $(S, \hat{\delta})$ be a (C, δ)-algebra that is finitely generated as such. Suppose we are given a differential K-rational point $\lambda : (S, \hat{\delta}) \to (K, \delta)$ (in fact we will only need that S has a K-rational point). It suffices to find a differential C-algebra homomorphism $(S, \hat{\delta}) \to (C, \delta)$. We expand $(S, \hat{\delta})$ by the trivial derivation and obtain a differentially finitely generated (C, δ, ∂)-algebra $(S, \hat{\delta}, 0)$ (note that ∂ is trivial on C).

A straightforward calculation shows that $(S, \hat{\delta}, 0) \otimes_C (K, \delta, \partial)$ is a differential (K, δ, ∂)-algebra (the derivations are given by $\hat{\delta}_i \otimes \delta_i$ and $0 \otimes \partial$) that is finitely generated as such, and $\lambda \otimes \mathrm{id} : S \otimes_C K \to K$ is a (not necessarily differential) K-algebra homomorphism; also see [19, §3.1] for generalities on derivations and tensor products.

Since (K, δ, ∂) is differentially large, there is a differential point $\mu : (S, \hat{\delta}, 0) \otimes_C (K, \delta, \partial) \to (K, \delta, \partial)$ by Theorem 4.3(iv), and we get a C-algebra homomorphism $\mu_0 : S \to S \otimes_C K \xrightarrow{\mu} K$. Since the natural map $S \to S \otimes_C K$ is differential for δ, also μ_0 is a differential homomorphism $(S, \hat{\delta}) \to (K, \delta)$. But

[4] Here $K\{x\}_{\leq r}$ denotes the subring of $K\{x\}$ of all polynomials in θx_i, where $\mathrm{ord}(\theta) \leq r$.

μ_0 has values in C because for $s \in S$ we have $\partial(\mu_0(s)) = \partial(\mu(s \otimes 1)) = \mu((0 \otimes \partial)(s \otimes 1)) = \mu(0) = 0$. Hence, indeed, $\mu_0(s) \in C$ as required.

(ii) Since (K, δ, ∂) is differentially large, it is e.c. in $K((t_1, \dots, t_{m+1}))$ when the latter is furnished with the natural derivations; see Theorem 4.3(ii). By (i), (C, δ) is e.c. in (K, δ). If $m = 0$ it follows that C is e.c. as a field in $K((t_1))$, hence C is a large field. If $m \geq 1$, we see that (C, δ) is e.c. in $C((t_1, \dots, t_m))$, which shows that it is differentially large by Theorem 4.3(ii). □

At the end of this section we show that differentially large fields are first-order axiomatizable; in other words, the class of differentially large fields is an elementary class in the language of differential rings. We show this implicitly in Proposition 4.7, by proving that differentially large fields are precisely those large and differential fields satisfying the axiom scheme UC in [34, 4.5]; thus, we refer to this paper for explicit axioms. The proof of Proposition 4.7 only uses properties of models of UC and results from this paper.

4.6. Remark. It is worth mentioning (for the nonlogician) the benefits of knowing that a class of structures is elementary (first-order axiomatizable). In our context this means that two properties hold: (1) ultraproducts of differentially large fields are again differentially large, and (2) differential fields that are existentially closed in some differentially large field are themselves differentially large. Property (2) is obvious from the characterization Theorem 4.3(ii). So it is only property (1) that needs to be established. Being an elementary class opens up the model theoretic toolbox to the analysis of differentially large fields, and it implies, for example, the following transfer principle (phrased in technical terms in Corollary 4.8 below):

> If K is a differentially large field and K as a pure field has "good" elimination theory, then the differential field K also has good elimination theory.

To illustrate what "good" elimination theory means, we look at classical examples of "good" elementary classes of fields. Algebraically closed fields have good elimination theory; this is due to Chevalley's theorem which says that the projection of a variety is constructible. If K is a real closed field or a p-adically closed field, then projections of K-varieties (by which we mean here Zariski closed subset of some K^n) are generally not constructible; however, the following weaker statement holds: the complement of a projection of a K-variety is again the projection of a K-variety (this property of a field is called "model-completeness"; see [10, section 8.3]). So then the transfer principle above says that for a differentially large field K the following holds: if K is algebraically closed as a field, then the projection of a differential variety is differentially constructible (a finite Boolean combination of Kolchin closed sets); if K is real closed or p-adically closed, then the complement of a projection of a differential variety is again the projection of a differential variety.

4.7. Proposition. *Let K be a differential field that is large as a field. Then K is differentially large if and only if it satisfies the axiom scheme* UC *from* [34, 4.5].

Proof. First assume that K is differentially large. By [34, Theorem 6.2(II)], there is a differential field extension L of K such that $L \models \mathrm{UC}$ and such that K is elementary in L as a field. In particular K is e.c. in

L as a field. Since K is differentially large, K is e.c. in L as a differential field. By [34, Proposition 6.3], UC has an inductive axiom system in the language of differential rings. But then K also satisfies these axioms. Hence $K \models \text{UC}$.

For the converse assume that K is a model of UC. We verify the definition of differentially large. Let L be a differential field extension of K such that K is e.c. in L as a field. Then there is a field M extending L such that K is elementary in M as a field. In particular M is a large field. We may now extend the derivations of L arbitrarily to commuting derivations of M. Hence, we may replace L by M furnished with these derivations and assume that L is large as a field. By [34, Theorem 6.2(II)] again, there is a differential field extension F of L such that $F \models \text{UC}$ and such that L is elementary in F as a field. Then K is e.c. in F as a field and $K, F \models \text{UC}$. By [34, Theorem 6.2(I)], this shows that K is e.c. in F (as a differential field), showing the assertion. □

By Proposition 4.7 we may now record important properties of differentially large fields (that follow from being models of UC; see [34]).

4.8. Corollary. (i) *If L and M are differentially large fields and K is a common differential subfield, then L and M have the same existential theory over K (meaning they solve the same systems of differential equations with coefficients in K) if and only if they have the same existential theory over K as fields.*

(ii) *If K is a differential field that is large as a field, then there is a differential field extension L of K such that L is differentially large and an elementary extension of K as a field.*

(iii) *Let K be a differentially large field and let $A \subseteq K$. Suppose K is model complete as a field in the language $\mathscr{L}_{\text{ri}}(A)$ of rings extended by constant symbols naming the elements of A.*

Then also K is model complete in the language $\mathscr{L}_{\text{diff}}(A)$ of differential rings extended by all constant symbols naming the elements of A. If $\hat{\mathscr{L}}$ is a language extending $\mathscr{L}_{\text{ri}}$ and $\hat{K}$ is an expansion of K to $\hat{\mathscr{L}}_{\text{diff}}$ such that the new symbols are A-definable in the field K and such that the restriction of $\hat{K}$ to $\mathscr{L}^*(A)$ has quantifier elimination[5]*, then $\hat{K}$ has quantifier elimination in the language $\hat{\mathscr{L}}_{\text{diff}}(A)$.*

5. Fundamental properties, constructions and applications

We show that algebraic extensions of differentially large fields are again differentially large by invoking the differential Weil descent in 5.12. Specifically differentially closed fields are identified as precisely the algebraic closures of differentially large fields; in a similar way, M. Singer's closed ordered differential fields are characterized; see 5.13. We show that a differentially large field is pseudoalgebraically closed just if it is pseudodifferentially closed; see 5.18. We characterize the existential theory of differentially large fields in 5.7. We show that differentially large fields are Picard–Vessiot closed in 5.9. In 5.15 we establish Kolchin-denseness of rational points in differential algebraic groups.

[5] An example of $\hat{\mathscr{L}}$ is the language $\mathscr{L}_{\text{ri}}(\leq)$ of ordered rings, $K = (K, \delta)$ is a real closed field furnished with commuting derivations, $A = \varnothing$ and $\hat{K} = (K, \leq, \delta)$. The restriction of $\hat{K}$ to $\mathscr{L}_{\text{ri}}(A)$ then is the ordered field $(K, \leq)$.

We start with a concrete method to construct differentially large fields. This is deployed in 5.14 to obtain concrete constructions of differentially closed fields.

5.1. Proposition. *Let $(K_i, f_{ij})_{i,j\in I}$ be a directed system of differential fields and differential embeddings with the following properties*:

(a) *All K_i are large as fields.*

(b) *All embeddings $f_{ij} : K_i \to K_j$ are isomorphisms onto a subfield of K_j that is e.c. in K_j as a field.*

(c) *For all $i \in I$ there exist $j \geq i$ and a differential homomorphism $K_i[\![\boldsymbol{t}]\!] \to K_j$ extending f_{ij}.*

Then the direct limit L of the directed system is a differentially large field.

Proof. We write $f_i : K_i \to L$ for the natural map into the limit, which obviously is a differential homomorphism between differential fields. We use the characterization Theorem 4.3(vii) to show that L is differentially large. Firstly, L is large as a field, because if C is a curve defined over L that has a smooth L-rational point then take $i \in I$ such that C is defined over K_i (via f_i) and such that C has a smooth K_i-rational point. By (a), the curve C has infinitely many K_i-rational points and so it also has infinitely many L-rational points.

Now let S be a differentially finitely generated L-algebra and a domain that has a point $S \to L$. Pick $r \in \mathbb{N}$ and a differential prime ideal $\mathfrak{p}$ of $L\{x\}$, $x = (x_1, \ldots, x_r)$, such that $S = L\{x\}/\mathfrak{p}$. By the Ritt–Raudenbusch basis theorem there is a finite $\Sigma \subseteq \mathfrak{p}$ whose differential radical is $\mathfrak{p}$. By Theorem 4.3(vii) it suffices to find a differential zero of Σ in L. Take $i \in I$ with $\Sigma \subseteq f_i(K_i)\{x\}$ and let $S_0 := K_i\{x\}/f_i^{-1}(\mathfrak{p})$. Then S_0 is a differentially finitely generated K_i-algebra and the composition of the natural embedding $S_0 \to S$ with a point $S \to L$ is a homomorphism $S_0 \to L$ extending f_i. We now want to invoke Corollary 3.6 and here we need (b). Namely, with this condition one readily verifies Proposition 2.2 and checks that K_i is existentially closed in L as a field (via f_i).

Hence, we may apply Corollary 3.6 to obtain a differential K-algebra homomorphism $S_0 \to K_i[\![\boldsymbol{t}]\!]$. Finally (c) gives us a differential K_i-algebra homomorphism $S_0 \to K_j$ for some $j \geq i$. This yields a differential solution of Σ in L. □

Concretely, Proposition 5.1 may be used to produce differentially large fields via iterated power series constructions using standard power series, Puiseux series or generalized power series. Here are a few instances; see 5.14 for applications.

5.2. Differentially large power series fields. Let K be a differential field. We write $K_0 = K$.

(i) We define by induction on $n \geq 0$, the differential field extension K_{n+1} of K_n as $K_{n+1} = K_n((\boldsymbol{t}_n))$, where $\boldsymbol{t}_n = (t_{n1}, \ldots, t_{nm})$; the derivations on K_{n+1} are the natural ones, extending those on K_n and satisfying $\delta_j(t_{nk}) = (\mathrm{d}/\mathrm{d}t_{nj})(t_{nk})$. Then $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$ is differentially large. If K is large as a field, then K is e.c. in K_∞ as a field.

To see this we apply Proposition 5.1 to the family of all K_n, $n > 0$ together with the inclusion maps $K_i \hookrightarrow K_j$ for $i \leq j$. Hence, K_∞ is differentially large. Since all K_n are large fields we know that they are e.c. in K_∞ as a field. Hence, if K happens to be large as a field, then K is also e.c. in K_∞ as a field.

This construction is discussed further in 5.14.

(ii) Assume here that the number m of derivations is 1. Then the generalized power series field $K((t^{\mathbb{Q}}))$ carries a derivation defined by $(\mathrm{d}/\mathrm{d}t)\big(\sum a_\gamma t^\gamma\big) = \sum a_\gamma \cdot \gamma \cdot t^{\gamma-1}$ and the given derivation δ on K can be extended to a derivation ∂ by $\partial\big(\sum a_\gamma t^\gamma\big) = \sum \delta(a_\gamma) t^\gamma$. We consider $K((t^{\mathbb{Q}}))$ as a differential field extension of $K((t))$, equipped with the derivation $\mathrm{d}/\mathrm{d}t + \partial$.

Now define $K_{n+1} = K_n((t_n^{\mathbb{Q}}))$. Since K_n carries a Henselian valuation for $n > 0$ we know that K_n is a large field. Hence, Proposition 5.1(a) and (c) hold for the family of all K_n, $n > 0$, and the inclusion maps $K_i \hookrightarrow K_j$ when $i \le j$.

If K is algebraically closed, real closed or p-adically closed, then so are all K_n and by standard theorems from model theory, Proposition 5.1(b) holds in each case. Thus $K_\infty = \bigcup_n K_n$ is a differentially large field. Also, $K_\infty = \bigcup_n K_n$ is again algebraically closed, real closed or p-adically closed, respectively. To be precise: if K is algebraically closed, then K_∞ is a differentially closed field; if K is real closed, then K_∞ is a closed ordered differential field in the sense of [32]; and if K is p-adically closed, then K_∞ is an existentially closed differential field in the class of p-adically valued and differential fields as considered in [8].

(iii) The differentially large field K_∞ in (ii) has various interesting differentially large subfields: for example, in each step of the construction we can work with Puiseux series only. More precisely, if P_{n+1} is defined to be the Puiseux series field over P_n, namely

$$P_{n+1} = P_n((t^{1/\infty})) = \bigcup_{k\in\mathbb{N}} P_n((t^{1/k})),$$

then $P_\infty = \bigcup_n P_n$ is a differentially large subfield of K_∞. Another example is given by working with completions of Puiseux series. More precisely, if C_{n+1} is defined to be the completion of the Puiseux series field over C_n, namely

$$C_{n+1} = \{f \in C_n((t^{\mathbb{Q}})) \mid \mathrm{supp}(f) \text{ is finite, or } \mathrm{supp}(f) \text{ is unbounded in } \mathbb{Q} \text{ and of order type } \omega\},$$

then $C_\infty = \bigcup_n C_n$ is a differentially large subfield of K_∞.

Again the fields P_∞ and C_∞ as pure fields, are algebraically closed, real closed, or p-adically closed if K has this property. By applying Corollary 4.8(iii) and model completeness of algebraically closed, real closed, and p-adically closed fields, we see that the differential fields P_∞ and C_∞ are elementary substructures of K_∞ in these cases.

5.3. Counterexample. Let L be the differential subfield $K((\boldsymbol{t}_1, \boldsymbol{t}_2, \ldots))$ of the differential field K_∞ from 5.2(i) and let L^{alg} be its algebraic closure. Then none of the t_{nj}^{-1} has an integral in L^{alg}, and hence L^{alg} is not differentially large and so obviously neither is $K((\boldsymbol{t}_1, \boldsymbol{t}_2, \ldots))$. Notice that the latter is large as a pure field by [27].

For the proof we may restrict to the case of one derivation. For $k \in \mathbb{N}$, the derivation δ of K_∞ restricts to a derivation of $L_0 = K((t_1, \ldots, t_k))$. The definition of the derivation, restricted to $K[\![t_1, \ldots, t_k]\!]$, shows that the K-automorphism of this ring permuting the variables is differential; obviously such an automorphism extends uniquely to a differential automorphism of L_0^{alg}. Hence, in order to show that none of the t_n^{-1}, $n \le k$, has an integral in L_0^{alg} we may assume that $n = k$. We write $t = t_k$ and let F be the algebraic closure of the differential subfield $K((t_1, \dots, t_{k-1}))$. Then L_0^{alg} is a differential subfield of the Puiseux series field $P = F((t^{1/\infty}))$, the latter being equipped with the natural derivation extending the one on F and mapping t to 1. It remains to show that t^{-1} has no integral in P. Suppose for a contradiction that $\delta(f) = t^{-1}$ for some $f \in P$. Then the order of f is $-q$ for some $q \in \mathbb{Q}$, $q > 0$. Hence, $t^q \cdot f$ has order 0 and so by definition of the derivation of P we see that the order of $\delta(t^q \cdot f)$ is > -1. On the other hand $\delta(t^q \cdot f) = q \cdot t^{q-1} \cdot f + t^q \cdot t^{-1} = t^{q-1} \cdot (q \cdot f + 1)$ has order -1, a contradiction.

5.4. Remark. In view of Counterexample 5.3 it is of interest to see integrals of t_1^{-1} in the differential field K_∞ from 5.2(i) in the ordinary case: take $k \ge 2$ and let $f_k = \sum_{n \ge 1} (1/nt_1^n) \cdot t_k^n$ (resembling $-\log(1 - (t_k/t_1))$). One readily checks that $\delta(f_k) = t_1^{-1}$.

5.5. Iterating algebraic power series. A further natural question related to the field K_∞ of 5.2(i) asks what type of differential equations can be solved when we iterate only algebraic Laurent series instead of all Laurent series. Let K be an ordinary differential field and let $L = \bigcup_n K((t_1))_{\text{alg}} \dots ((t_n))_{\text{alg}}$, where the derivation is chosen as in 5.2(i). Thus L is a differential subfield of $K(t_1, t_2, \dots)^{\text{alg}}$, where $\delta(t_i) = 1$ for all i. Notice that L is large as a pure field, because algebraic power series are a local henselian domain and so [27] applies again. Since L is a differential subfield of the algebraic closure of $K((t_1, t_2, \dots))$ we already know from Counterexample 5.3 that L is not differentially large. Here we show that L is not even Picard–Vessiot closed in general.

If L were Picard–Vessiot closed, then L has nontrivial solutions of the differential equation $\delta x = x$. However, we show that this is in general not the case even for $M = K(t_1, t_2, \dots)^{\text{alg}}$. To see this, consider the following property of a differential field F:

$$(\dagger) \qquad \forall x \in F, n \in \mathbb{N} : \delta(x) = n \cdot x \Rightarrow x = 0.$$

Then, if F has property (†) so does its algebraic closure F^{alg} and its function field $F(t)$, where $\delta(t) = 1$. Hence, if we start with K being a differential field with trivial derivation, then by induction, property (†) passes to $K(t_1, \dots, t_n)^{\text{alg}}$ and so also passes to M.

For the proof that (†) passes to $F(t)$, assume that $\delta(f/g) = n \cdot f/g$ with g monic and f with leading coefficient a. Then $nfg = \delta(f)g - f\delta(g) = (f^\delta + f')g - f(g^\delta + g')$ and comparing leading coefficients shows that $n \cdot a = \delta(a)$. Hence, by (†) for F we get $a = 0$ as required.

For the proof that (†) passes to F^{alg}, one first checks that it passes to $F(C)$, where C is the constant field of F^{alg}. Hence, we may replace F by $F(C)$ and assume that F and F^{alg} have the same constant field. Let α be algebraic over F with minimal polynomial f and assume $\delta(\alpha) = n \cdot \alpha$. Then any other root β of f also satisfies this equation, which implies that $\delta(\alpha/\beta)$ is a constant; thus it is in F. Hence, $F(\alpha)$ is the splitting field of f and so $F(\alpha)/F$ is Galois. Let d be the order of the Galois group and let $\sigma \in \text{Gal}(F(\alpha)/F)$. As we have seen, $\sigma(\alpha) = c \cdot \alpha$ for some constant c. Hence, $\alpha = \sigma^d(\alpha) = c^d \cdot \alpha$ and so

$c^d = 1$. But then $\sigma(\alpha^d) = (c\alpha)^d = \alpha^d$, which shows that α^d is in the fixed field F. Since $\delta(\alpha^d) = d{\cdot}n{\cdot}\alpha^d$, we get $\alpha = 0$ from (†) for F.

5.6. The existential theory of differentially large fields. The existential theory of the class of all large fields of characteristic zero is the existential theory of the field $\mathbb{Q}((t))$ (see [29, Proposition 2.25]). This follows essentially from the fact that $\mathbb{Q}((t))$ is itself a large field. Since the existential theory of a differentially large field is uniquely determined by its existential theory of its field structure — in the sense of Corollary 4.8(i) — one is led to the question on whether the existential theory of the class of differentially large fields is the existential theory of $\mathbb{Q}((\boldsymbol{t}))$, equipped with its natural derivations.

However, $\mathbb{Q}((\boldsymbol{t}))$ does not satisfy the existential theory of the class of differentially large fields (and so it is not differentially large either). To see an example, let C be the curve defined by $x^3 + y^3 = 1$. Then $(1, 0)$ and $(0, 1)$ are the only rational points on C (and they are regular points). Hence, the sentence φ saying that there is a point (x, y) on C with $x \neq 0$, $y \neq 0$ and $x' = y' = 0$ fails in the differential field $\mathbb{Q}((t))$ (we work with $m = 1$ here). On the other hand φ is true in every differentially large field K, because the constants of K are large as a field by Corollary 4.5.

On the positive side we now show:

5.7. Theorem. *The existential theory of the class of differentially large fields is the existential theory of* $\mathbb{Q}((\boldsymbol{t}_1))((\boldsymbol{t}_2))$.

Proof. Let $\Sigma \subseteq \mathbb{Z}\{x_1, \dots, x_n\}$ be a system of differential polynomials in n variables and m commuting derivations. If Σ has a solutions in $\mathbb{Q}((\boldsymbol{t}_1))((\boldsymbol{t}_2))$ and K is a differentially field, then Σ also has a solution in $K((\boldsymbol{t}_1))((\boldsymbol{t}_2))$. Hence, if K is differentially large, then by Theorem 4.3(iii), Σ also has a solution in K.

Conversely, suppose Σ has a solution in every differentially large field. By Corollary 4.8(ii) there is a differentially large field K containing $\mathbb{Q}((\boldsymbol{t}_1))$ as a differential subfield such that the extension $K/\mathbb{Q}((\boldsymbol{t}_1))$ of fields is elementary. Let $S_0 = \mathbb{Q}\{x_1, \dots, x_n\}/\sqrt[d]{\Sigma}$ and let $f : S_0 \to K$ be a differential point of S_0. Let $\mathfrak{p} = \mathrm{Ker}(f)$ and let $S = S_0/\mathfrak{p}$. It suffices to find a differential point $S \to \mathbb{Q}((\boldsymbol{t}_1))((\boldsymbol{t}_2))$. Write $S = A_h \otimes_{\mathbb{Q}} P$ as in Theorem 2.3. The restriction $f|_{A_h}$ is a K-rational point of A_h. Since A_h is a finitely generated $\mathbb{Q}$-algebra and $\mathbb{Q}((\boldsymbol{t}_1))$ is e.c. in K as a field, there is also a point $g_0 : A_h \to \mathbb{Q}((\boldsymbol{t}_1))$. Since P is a polynomial $\mathbb{Q}$-algebra, g_0 can be extended to a point $g : S \to \mathbb{Q}((\boldsymbol{t}_1))$. By Corollary 3.6, there is a differential point $S \to \mathbb{Q}((\boldsymbol{t}_1))[[\boldsymbol{t}_2]]$. □

5.8. Differentially large fields are PV-closed. We prove that differentially large fields solve plenty of algebraic differential equations. Namely, we prove that they solve all consistent systems of linear differential equations. We first show that they are Picard–Vessiot closed (or PV-closed).

Let $(K, \delta_1, \dots, \delta_m)$ be a differential field, and let $A_i \in \mathrm{Mat}_n(K)$, for $i = 1, \dots, m$, satisfying what is called the *integrability condition*; namely

$$\delta_i A_j - \delta_j A_i = [A_i, A_j],$$

where $\delta_j A_j$ denotes the $n \times n$ matrix obtained by applying δ_i to A_j entrywise. The differential field K is said to be PV-closed if for each such tuple $(A_1, \dots, A_m)$ of matrices there is a $Z \in GL_n(K)$ such that

$$\delta_i Z = A_i Z_i \quad \text{for } i = 1, \dots, m.$$

5.9. Lemma. *Every differentially large field is PV-closed.*

Proof. Suppose K is a differentially large field. Suppose $A_1, \dots, A_m$ are elements in $\mathrm{Mat}_n(K)$ satisfying the integrability condition. Let X be an $n \times n$ matrix of variables and define derivations on $K(X)$ that extend the ones in K and satisfy

$$\delta_i X = A_i X.$$

Then, by the integrability condition, these derivations commute in all of $K(X)$. Since K is e.c. in $K(X)$ as fields, by differential largeness, it is also e.c. as differential fields. This yields the desired (fundamental) solution in K. □

In differentially large fields, Lemma 5.9 is a special case of a stronger property:

5.10. Proposition. *Let Σ and Γ be finite collections of differential polynomials in $K\{x_1, \dots, x_n\}$. Assume that the system*

$$P = 0 \quad \textit{and} \quad Q \neq 0 \qquad \textit{for } P \in \Sigma \textit{ and } Q \in \Gamma$$

is consistent (i.e., it has a solution in some differential field extension of K). If Σ consists of linear differential polynomials and K is differentially large, then the system has a solution in K.

Proof. Since the system is assumed to be consistent, the differential ideal generated by Σ in $K\{x_1, \dots, x_n\}$, denoted by $[\Sigma]$, is prime. Thus, the differential field extension $L = \mathrm{qf}(K\{x_1, \dots, x_n\}/[\Sigma])$ has a solution to the system. Since $[\Sigma]$ is generated, as an ideal of $K\{x_1, \dots, x_n\}$, by linear terms, we get that K is e.c. in L as fields, and, by differential largeness, also as differential fields. The result follows. □

5.11. A glimpse on the differential Weil descent. If K is a large field, then every algebraic field extension of K is again large. This follows from an argument involving Weil descent in the case when L/K is finite; see [29, Theorem 2.14; 26, Proposition 1.2]. For differentially large fields, this can also be carried out. We will explain a special case of the differential Weil descent suitable for our purpose and refer to [19, Theorem 3.4] for the general assertion and for proofs.

We will be working with a finite extension L/K of differential fields and a differential L-algebra S. Then the classical Weil descent $W(S)$ of the underlying L-algebra of S is a K-algebra and there is a "natural" bijection

$$\mathrm{Hom}_{K\text{-}\mathtt{Alg}}(W(S), K) \to \mathrm{Hom}_{L\text{-}\mathtt{Alg}}(S, L).$$

Here homomorphisms are algebra homomorphisms over K and L, respectively. Now in [19, Theorem 3.4] it is shown that the ring $W(S)$ can be naturally expanded to a differential K-algebra $W^{\text{diff}}(S)$ such that the bijection above restricts to a bijection

$$\mathrm{Hom}_{\text{diff. } K\text{-}\mathtt{Alg}}(W^{\text{diff}}(S), K) \to \mathrm{Hom}_{\text{diff. } L\text{-}\mathtt{Alg}}(S, L).$$

This time, homomorphisms are differential algebra homomorphisms over K and L, respectively. The terminology "natural" in both bijections refers to the fact that W and W^{diff} are indeed functors defined on categories of algebras and differential algebras, respectively. However for our application below only the existence of the bijections above are needed. We refer to [19, Section 3] for a self contained exposition of the matter, where all data are constructed explicitly. In particular the construction there shows that $W^{\mathrm{diff}}(S)$ is a differentially finitely generated K-algebra if S is a differentially finitely generated L-algebra.

5.12. Theorem. *If K is differentially large, then so is every algebraic extension* (*equipped with the induced derivations*).

Proof. Let L/K be an algebraic extension. We first deal with the case when L/K is finite. We verify Theorem 4.3(iv) for L. So let S be a differentially finitely generated L-algebra that has an L-rational point. Let $W^{\mathrm{diff}}(S)$ be the differential Weil descent as explained in 5.11. Thus, $W^{\mathrm{diff}}(S)$ is a differentially finitely generated K-algebra and we have a bijection

$$\mathrm{Hom}_{K\text{-}\mathtt{Alg}}(W(S),K)\to\mathrm{Hom}_{L\text{-}\mathtt{Alg}}(S,L),$$

which restricts to a bijection

$$\mathrm{Hom}_{\mathrm{diff.}\ K\text{-}\mathtt{Alg}}(W^{\mathrm{diff}}(S),K)\to\mathrm{Hom}_{\mathrm{diff.}\ L\text{-}\mathtt{Alg}}(S,L).$$

Since S has an L-rational point we may use the first bijection and see that $W(S)$ has a K-rational point. Since K is differentially large there is a differential K-rational point $W^{\mathrm{diff}}(S)\to K$. Using the second bijection we see that S has a differential L-rational point.

Hence, we know the assertion when L/K is finite. In general, let $S=A\otimes P$ be a composite L-algebra such that the affine variety defined by A is smooth. Suppose there is an L-rational point $A\to L$. By Theorem 4.3(viii) it suffices to show that there is a differential point $S\to L$. Write $S=L\{x\}/\mathfrak{p}$, $x=(x_1,\dots,x_r)$, for a prime differential ideal $\mathfrak{p}$ of $L\{x\}$ and let $\Sigma\subseteq\mathfrak{p}$ be finite with $\mathfrak{p}=\sqrt[d]{\Sigma}$. It suffices to find a differential solution of $\Sigma=0$ in L. Choose a finite extension K_0/K in L with $\Sigma\subseteq K_0\{x\}$. Let $S_0=K_0\{x\}/\mathfrak{p}\cap K_0\{x\}$, which we consider as a subring of S. By Theorem 2.3 there are a finitely generated K_0-subalgebra A_0 of S_0, a polynomial K_0-subalgebra P_0 of S_0 and an element $h\in A_0$ such that $(S_0)_h\cong(A_0)_h\otimes_{K_0}P_0$.

Since $A_0\subseteq S$ is finitely generated we may write $P=P_1\otimes_L P_2$ for some polynomial L-algebras P_i, P_1 finitely generated such that $A_0\subseteq A\otimes_L P_1$. Then $A\otimes_L P_1$ is again finitely generated, the affine variety defined by $A\otimes_L P_1$ is again smooth and still has an L-rational point. Since L is large, there is also an L-rational point $(A\otimes_L P_1)_h\to L$. Via restriction we get an L-rational point $f:(A_0)_h\to L$. Since $(A_0)_h$ is finitely generated as a K_0-algebra, there is a finite extension K_1/K_0 contained in L such that f has values in K_1. Since P_0 is a polynomial K_0-algebra, f can be extended to a K_1-rational point $(S_0)_h\to K_1$. Tensoring with K_1 gives a K_1-rational point of $(S_0)_h\otimes_{K_0}K_1$. The latter is a differentially finitely generated K_1-algebra. By what we have shown, K_1 is differentially large. By Theorem 4.3(iv) there is a differential point $(S_0)_h\otimes_{K_0}K_1\to K_1$. Since $\Sigma\subseteq K_1\{x\}$ this gives rise to a differential solution of $\Sigma=0$ in $K_1\subseteq L$. □

As an application, we see from 5.12 and Corollary 4.8(iii) that the algebraic closure of a differentially large field is differentially closed. Hence, differentially large fields have minimal differential closures:

5.13. Corollary. *The algebraic closure of a differentially large field is differentially closed. In particular, if $K \models \mathrm{CODF}_m$, the theory of closed ordered differential fields in m commuting derivations, then $K(i) \models \mathrm{DCF}_{0,m}$.*

The result above has already been deployed in [1] making reference to an earlier draft of this paper. Previously known examples of differential fields with minimal differential closures are models of CODF (which we denote as CODF_1), see [31], and fixed fields of models of $\mathrm{DCF}_{0,m}$ A, the theory differentially closed fields with a generic differential automorphism; see [16]. The corollary delivers a vast variety of new differential fields with this property, namely all differentially large fields; see also Corollary 4.8(ii).

We also get new and explicit models of $\mathrm{DCF}_{0,m}$ and CODF_m:

5.14. Construction of differentially closed fields. We continue with the constructions in 5.2(i). If K is a differential field, then the algebraic closure of the differentially large field $K_\infty = \bigcup_{n\in\mathbb{N}} K((\boldsymbol{t}_1))\dots((\boldsymbol{t}_n))$ from 5.2(i) is differentially closed. If K is an ordered field and the order is extended to L in some way, then the real closure of L is a model of CODF_m.

Observe that these models are different from those obtained using iterated Puiseux series or generalized power series constructions in 5.2(ii) and (iii).

5.15. Kolchin-denseness of rational points in differential algebraic groups. In the classical case of a connected linear algebraic group G over any field F of characteristic zero, the unirationality theorem implies that the F-rational points of G are Zariski-dense. In the differential situation the corresponding statement does not hold. For example, the linear differential algebraic group defined by $\delta x = x$ does in general not have a Kolchin-dense set of rational points. However, as a further application, we prove that in differentially large fields this is true again:

5.16. Proposition. *Assume K is differentially large. If G is a connected differential algebraic group over K, then the set of K-rational points of G, denoted $G(K)$, is Kolchin dense in $G = G(\mathbb{U})$.*

Proof. We verify Theorem 4.3(x), and hence it suffices to show that for infinitely many values of r the jet $\mathrm{Jet}_r\, G$ has a smooth K-rational point. By [23, Corollary 4.2(ii)], G embeds over K into a connected algebraic group H defined over K. As we saw in Definition 2.6, for each r, $\nabla_r G$ is a differential algebraic subgroup of $\tau_r H$. As a result, $\mathrm{Jet}_r\, G$ is an algebraic subgroup of $\tau_r H$, and so $\mathrm{Jet}_r\, G$ is smooth. If e denotes the identity of G, which is a K-point, then, for each r, the K-point $\nabla_r(e)$ is a smooth point of $\mathrm{Jet}_r\, G$. □

The result above has already been deployed in [18] making reference to an earlier draft of this paper.

5.17. Pseudodifferentially closed fields. Recall that a field K is pseudoalgebraically closed (PAC) if every absolutely irreducible algebraic variety over K has a K-point. It is easy to see and well known that PAC fields are large and that the PAC property is equivalent to saying that K is e.c. in every regular field extension L (meaning that K is algebraically closed in L). From model theoretic literature one can formulate several notions of pseudodifferentially closed fields; see [11; 24]. We show that they are all equivalent to the property "PAC + differentially large".

5.18. Theorem (pseudodifferentially closed fields). *Let K be a differential field. The following are equivalent*:

(i) *K is PAC* (*as a field*) *and K is differentially large.*

(ii) *Every absolutely irreducible differential variety over K has a differential K-point. Recall that a differential variety V over K is absolutely irreducible if it is irreducible in the Kolchin topology of a differential closure K^{diff} and this is equivalent to saying that V is irreducible over K^{alg}.*

(iii) *K is e.c. in every differential field extension L in which K is R-regular* (*that is*, $\text{tp}(a/K)$ *is stationary for every tuple a from L, where the type* $\text{tp}(a/K)$ *is with respect to the stable theory* $\text{DCF}_{0,m}$).

(iv) *K is e.c. in every differential field extension L in which K is H-regular* (*that is*, $K^{\text{alg}} \cap L = K$).

If these equivalent conditions hold we call K pseudodifferentially closed.

Proof. We use [11, Lemma 3.35], which says in our situation that for a tuple a from $\mathcal{U}$ (the monster model of $\text{DCF}_{0,m}$), the type $\text{tp}(a/K)$ is stationary if and only if the differential field extension $K\langle a\rangle$ over K is H-regular. Clearly this characterization implies that H-regularity and R-regularity are equivalent. In particular, (iii) is equivalent to (iv).

(i) $\Rightarrow$ (iv). Let K be PAC and differentially large. Let L/K be an H-regular extension of K. Then K is algebraically closed in L as a field and because K is PAC, it is e.c. in L as a field. Since K is differentially large, it follows that it is e.c. in L as a differential field.

(iv) $\Rightarrow$ (ii). This follows from the fact that a type $\text{tp}(a/K)$ is stationary if and only if the Kolchin-locus of a over K is absolutely irreducible. Let V be an absolutely irreducible differential variety over K. Then the generic type $p = \text{tp}(a/K)$ of V over K is stationary, and hence, by the quoted characterization of stationarity, the differential field $L = K\langle a\rangle$ is an H-regular extension of K. By (iv), K is e.c. in L as a differential field and so there is a differential K-point in V, as required.

(ii) $\Rightarrow$ (i). Suppose V is a K-irreducible differential variety such that all jets of V have a smooth K-point. Then all these jets are absolutely Zariski irreducible (as they are Zariski K-irreducible and contain a smooth K-point). It follows that V is absolutely irreducible. Hence, V has a K-point. In fact, V has Kolchin-dense many K-points; indeed, we can take any open differential subvariety O of V and argue similarly (using the fact that K is large, as it is PAC, to produce smooth K-points in the jets of O). This shows (i) using the equivalence (i) $\iff$ (x) of Theorem 4.3. □

5.19. Pseudodifferentially closed fields are axiomatizable. An application of Theorem 5.18 is that the class of pseudodifferentially closed fields is first-order axiomatizable (so far this had only been established in the case of one derivation in [24, Proposition 5.6]). Indeed, being a PAC field is a first-order condition (see [6, 11.3.2]) and we have seen in Proposition 4.7 that differential largeness is too. The fact that being pseudodifferentially closed is a first-order property has very interesting model-theoretic consequences: (i) by [25, §3] it implies that the theory of a bounded pseudodifferentially closed field is supersimple, and (ii) by [5, Theorem 5.11] it implies that the elementary equivalence theorem holds for pseudodifferentially closed fields.

6. Algebraic-geometric axioms

We present algebraic-geometric axioms for differentially large fields in the spirit of the classical Pierce–Pillay axioms for differentially closed fields in one derivation [22] (see Remark 6.6(i) below). While this section might seem mostly of interest to model theorists, the general reader should keep in mind that Theorem 6.4 is a general statement on systems of algebraic PDEs that have solutions in differentially large fields.

Our presentation here follows the recent algebraic-geometric axiomatization of differentially closed fields in several commuting derivations established in [17]. In particular, we will use the recently developed theory of differential kernels for fields with several commuting derivations from [7]. One significant difference with the arguments in [17] is that theirs only requires the existence of regular realizations of differential kernels, while here we need the existence of principal realizations; see Remark 6.1 and Fact 6.2. We carry on the notation and conventions from previous sections.

We use two different orders $\leq$ and $\trianglelefteq$ on $\mathbb{N}^m \times \{1, \dots, n\}$. Given two elements (ξ, i) and (τ, j) of $\mathbb{N}^m \times \{1, \dots, n\}$, we set $(\xi, i) \leq (\tau, j)$ if and only if $i = j$ and $\xi \leq \tau$ in the product order of $\mathbb{N}^m$. We set $(\xi, i) \trianglelefteq (\tau, j)$ if and only if

$$\left(\sum \xi_k, i, \xi_1, \dots, \xi_m\right) \leq_{\text{lex}} \left(\sum \tau_k, j, \tau_1, \dots, \tau_m\right)$$

Note that if $x = (x_1, \dots, x_n)$ are differential indeterminates and we identify (ξ, i) with $\delta^\xi x_i := \delta_1^{\xi_1} \cdots \delta_m^{\xi_m} x_i$, then $\leq$ induces an order on the set of algebraic indeterminates given by $\delta^\xi x_i \leq \delta^\tau x_j$ if and only if $\delta^\tau x_j$ is a derivative of $\delta^\xi x_i$ (in particular this implies that $i = j$). On the other hand, the ordering $\trianglelefteq$ induces the canonical orderly ranking on the set of algebraic indeterminates.

We will look at field extensions of K of the form

$$L := K(a_i^\xi : (\xi, i) \in \Gamma_n(r)) \tag{6-1}$$

for some fixed $r \geq 0$. Here we use a_i^ξ as a way to index the generators of L over K. The element $(\tau, j) \in \mathbb{N}^m \times \{1, \dots, n\}$ is said to be a leader of L if there is $\eta \in \mathbb{N}^m$ with $\eta \leq \tau$ and $\sum \eta_k \leq r$ such that a_j^η is algebraic over $K(a_i^\xi : (\xi, i) \triangleleft (\eta, j))$. A leader (τ, j) is a minimal leader of L if there is no leader (ξ, i) with $(\xi, i) < (\tau, j)$. Observe that the notions of leader and minimal leader make sense even when $r = \infty$.

A (differential) kernel of length r over K is a field extension of the form

$$L = K(a_i^\xi : (\xi, i) \in \Gamma_n(r))$$

such that there exist derivations

$$D_k : K(a_i^\xi : (\xi, i) \in \Gamma_n(r-1)) \to L$$

for $k = 1, \dots, m$ extending δ_k and $D_k a_i^\xi = a_i^{\xi+\boldsymbol{k}}$ for all $(\xi, i) \in \Gamma_n(r-1)$, where $\boldsymbol{k}$ denotes the m-tuple whose k-th entry is one and zeroes elsewhere.

Given a kernel $(L, D_1, \dots, D_k)$ of length r, we say that it has a *prolongation of length* $s \geq r$ if there is a kernel $(L', D'_1, \dots, D'_k)$ of length s over K such that L' is a field extension of L and each D'_k extends D_k. We say that $(L, D_1, \dots, D_k)$ has a *regular realization* if there is a differential field extension $(M, \Delta' = \{\delta'_1, \dots, \delta'_m\})$ of $(K, \Delta = \{\delta_1, \dots, \delta_m\})$ such that M is a field extension of L and $\delta'_k a_i^\xi = a_i^{\xi+\boldsymbol{k}}$ for all $(\xi, i) \in \Gamma_n(r-1)$ and $k = 1, \dots, m$. In this case we say that $g := (a_1^{\boldsymbol{0}}, \dots, a_n^{\boldsymbol{0}})$ is a regular realization of L. If in addition the minimal leaders of L and those of the differential field $K\langle g\rangle$ coincide we say that g is a *principal realization* of L.

6.1. Remark. If g is a principal realization of the differential kernel L, then L is existentially closed in $K\langle g\rangle$ as fields. Indeed, since the minimal leaders of L and $K\langle g\rangle$ coincide, for every $(\xi, i) \in \mathbb{N}^m \times \{1, \dots, n\}$ we have that either $\delta^\xi g_i$ is in L or it is algebraically independent from $K(\delta^\eta g_j : (\eta, j) \lhd (\xi, i))$. In other words, the differential ring generated by g over L, namely $L\{g\}$, is a polynomial ring over L. The claim follows.

In general, it is not the case that every kernel has a principal realization (not even regular). In [7], an upper bound $C^n_{r,m}$ was obtained for the length of a prolongation of a kernel that guarantees the existence of a principal realization. This bound depends only on the data (r, m, n) and is constructed recursively as

$$C^1_{0,m} = 0, \quad C^1_{r,m} = A(m-1, C^1_{r-1,m}), \qquad \text{and} \qquad C^n_{r,m} = C^1_{C^{n-1}_{r,m},m},$$

where $A(x, y)$ is the Ackermann function. For example,

$$C^n_{r,1} = r, \quad C^n_{r,2} = 2^n r \qquad \text{and} \qquad C^1_{r,3} = 3(2^r - 1).$$

6.2. Fact [7, Theorem 18]. If a differential kernel $L = K(a_i^\xi : (\xi, i) \in \Gamma_n(r))$ of length r has a prolongation of length $C^n_{r,m}$, then there is $r \leq h \leq C^n_{r,m}$ such that the differential kernel $K(a_i^\xi : (\xi, i) \in \Gamma_n(h))$ has a principal realization.

6.3. Remark. Note that in the ordinary case $\Delta = \{\delta\}$ (i.e., $m = 1$), we have $C^n_{r,1} = r$ by definition, and so the fact above shows that in this case every differential kernel has a principal realization (this is a classical result of Lando [13]).

The fact above is the key to our algebraic-geometric axiomatization of differential largeness. We need some additional notation. For a given positive integer n, we set

$$\alpha(n) = n \cdot \binom{C^n_{1,m} + m}{m} \quad \text{and} \quad \beta(n) = n \cdot \binom{C^n_{1,m} - 1 + m}{m}.$$

We write $\pi : \mathbb{U}^{\alpha(n)} \to \mathbb{U}^{\beta(n)}$ for the projection onto the first $\beta(n)$ coordinates; i.e., setting $(x_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m})}$ to be coordinates for $\mathbb{U}^{\alpha(n)}$ then π is the map

$$(x_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m})} \mapsto (x_i^\xi)_{(\xi,i)\in\Gamma(C^n_{1,m}-1)}.$$

It is worth noting here that $\alpha(n) = |\Gamma_n(C^n_{1,m})|$ and $\beta(n) = |\Gamma_n(C^n_{1,m} - 1)|$. We also use the projection $\psi : \mathbb{U}^{\alpha(n)} \to \mathbb{U}^{n\cdot(m+1)}$ onto the first $n \cdot (m + 1)$ coordinates, that is,

$$(x_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m})} \mapsto (x_i^\xi)_{(\xi,i)\in\Gamma_n(1)}.$$

Finally, we use the embedding $\varphi : \mathbb{U}^{\alpha(n)} \to \mathbb{U}^{\beta(n)\cdot(m+1)}$ given by

$$(x_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m})} \mapsto \big((x_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m}-1)}, (x_i^{\xi+\mathbf{1}})_{(\xi,i)\in\Gamma_n(C^n_{1,m}-1)}, \dots\dots, (x_i^{\xi+\boldsymbol{m}})_{(\xi,i)\in\Gamma_n(C^n_{1,m}-1)}\big).$$

Recall from Definition 2.6 that for a Zariski-constructible set X of $\mathbb{U}^n$, the first prolongation of X is denoted by $\tau X = \tau_1 X \subseteq \mathbb{U}^{n(m+1)}$. For the first prolongation it is easy to give the defining equations: $\tau(X)$ is the Zariski-constructible set given by the conditions

$$x \in X \qquad \text{and} \qquad \sum_{i=1}^{n} \frac{\partial f_j}{\partial x_i}(x) \cdot y_{i,k} + f_j^{\delta_k}(x) = 0 \quad \text{for } 1 \le j \le s,\ 1 \le k \le m,$$

where $f_1, \dots, f_s$ are generators of the ideal of polynomials over $\mathbb{U}$ vanishing at X, and each $f_j^{\delta_k}$ is obtained by applying δ_k to the coefficients of f_j. Note that $(a, \delta_1 a, \dots, \delta_m a) \in \tau X$ for all $a \in X$. Further, if X is defined over the differential field K then so is τX.

6.4. Theorem. *Assume K is a differential field that is large as a field. Then, K is differentially large if and only if*

($\Diamond$) *for every K-irreducible Zariski-closed set W of $\mathbb{U}^{\alpha(n)}$ with a smooth K-point such that $\varphi(W) \subseteq \tau(\pi(W))$, the set of K-points of $\psi(W)$ of the form $(a, \delta_1 a, \dots, \delta_m a)$ is Zariski-dense in $\psi(W)$.*

Proof. The proof follows the strategy of [17], but here regular realizations are replaced by principal realizations with the appropriate adaptations. As the set up is technically somewhat intricate we give details.

Assume K is differentially large. Let W be as in condition ($\Diamond$), we must find Zariski-dense many K-points in $\psi(W)$ of the form $(a, \delta_1 a, \dots, \delta_m a)$. Let $b = (b_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m})}$ be a Zariski-generic point of W over K. Then $(b_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m}-1)}$ is a Zariski-generic point of $\pi(W)$ over K, and

$$\begin{aligned}\varphi(b) = \big((b_i^\xi)_{(\xi,i)\in\Gamma_n(C^n_{1,m}-1)}, (b_i^{\xi+\mathbf{1}})_{(\xi,i)\in\Gamma_n(C^n_{1,m}-1)}, \dots, (b_i^{\xi+\boldsymbol{m}})_{(\xi,i)\in\Gamma_n(C^n_{1,m}-1)}\big)&\\ \in \tau(\pi(W)).&\end{aligned}$$

By the standard argument for extending derivations (see [14, Chapter 7, Theorem 5.1], for instance), there are derivations

$$D'_k : K(b_i^\xi : (\xi, i) \in \Gamma_n(C^n_{1,m} - 1)) \to K(b_i^\xi : (\xi, i) \in \Gamma_n(C^n_{1,m}))$$

for $k = 1, \dots, m$ extending δ_k and such that $D'_k b_i^\xi = b_i^{\xi+\mathbf{k}}$ for all $(\xi, i) \in \Gamma_n(C^n_{1,m} - 1)$. Thus, $L' = K(b_i^\xi : (\xi, i) \in \Gamma_n(C^n_{1,m}))$ is a differential kernel over K and, also, it is a prolongation of length $C^n_{1,m}$ of the differential kernel $L = K(b_i^\xi : (\xi, i) \in \Gamma_n(1))$ of length 1 with $D_k = D'_k|_L$. By Fact 6.2, there is $r \le h \le C^n_{1,m}$ such that $L'' = K(b_i^\xi : (\xi, i) \in \Gamma_n(h))$ has a principal realization; in particular, there is a differential field extension (M, Δ') of (K, Δ) containing L'' such that $\delta'_k b^{\mathbf{0}} = b^{\mathbf{k}}$, where $b^{\mathbf{0}} = (b_1^{\mathbf{0}}, \dots, b_n^{\mathbf{0}})$ and similarly for $b^{\mathbf{k}}$. Then

$$(*) \qquad (b^{\mathbf{0}}, \delta'_1 b^{\mathbf{0}}, \dots, \delta'_m b^{\mathbf{0}}) \text{ is a generic point of } \psi(W) \text{ over } K.$$

Now, since W has a smooth K-point and K is large, K is e.c. in L' as fields; in particular, K is e.c. in L'' as fields. By Remark 6.1, L'' is e.c. in the differential field $K\langle b^{\mathbf{0}}\rangle$ as fields, and so K is e.c. in $K\langle b^{\mathbf{0}}\rangle$ as fields. Since K is differentially large, the latter implies that K is e.c. in $K\langle b^{\mathbf{0}}\rangle$ as differential fields as well. The conclusion now follows using $(*)$.

For the converse, assume K is e.c. as a field in a differential field extension F. We must show that K is also e.c. in F as differential field. Let $\rho(x)$ be a quantifier-free formula over K (in the language of differential rings with m derivations) in variables $x = (x_1, \dots, x_t)$ with a realization c in F. We may write

$$\rho(x) = \gamma(\delta^\xi x_i : (\xi, i) \in \Gamma_t(r)),$$

where $\gamma((x^\xi)_{(\xi,i)\in\Gamma_t(r)})$ is a quantifier-free formula in the language of rings over K for some r. If $r = 0$, then ρ is a formula in the language of rings, and so $\rho(x)$ has a realization in K since K is e.c. in F as a field. Now assume $r > 0$. Let $n := t \cdot \binom{r-1+m}{m}$, $d := (\delta^\xi c_i)_{(\xi,i)\in\Gamma_t(r-1)}$, and

$$W := \text{Zar-loc}_K(\delta^\xi d_i : (\xi, i) \in \Gamma_n(C^n_{1,m})) \subseteq \mathbb{U}^{\alpha(n)}.$$

We have that $\varphi(W) \subseteq \tau(\pi(W))$. Since W has a smooth F-point (namely $(\delta^\xi d_i)_{(\xi,i)\in\Gamma_n(C^n_{1,m})}$) and K is e.c. in F as fields, W has a smooth K-point. By $(\diamondsuit)$, there is $a = (a_i^\xi)_{(\xi,i)\in\Gamma_t(r-1)} \in K^n$ such that $(a, \delta_1 a, \dots, \delta_m a) \in \psi(W)$. This implies that $a_i^\xi = \delta^\xi a_i^{\mathbf{0}}$ for all $(\xi, i) \in \Gamma_t(r-1)$. Thus,

$$(\delta^\xi a_i^{\mathbf{0}})_{(\xi,i)\in\Gamma_t(r)} \in \text{Zar-loc}_K((\delta^\xi c_i)_{(\xi,i)\in\Gamma_t(r)}) \subseteq \mathbb{U}^{t\cdot\binom{r+m}{m}},$$

and so, since $(\delta^\xi c_i)_{(\xi,i)\in\Gamma_t(r)}$ realizes γ, the point $(\delta^\xi a_i^{\mathbf{0}})_{(\xi,i)\in\Gamma_t(r)}$ also realizes γ. Consequently, $K \models \rho(a^{\mathbf{0}})$, as desired. □

In the ordinary case ($m = 1$) we get the values $\alpha(n) = 2n$ and $\beta(n) = n$. Also, in this case, $\pi : \mathbb{U}^{2n} \to \mathbb{U}^n$ is just the projection onto the first n coordinates, and $\psi, \varphi : \mathbb{U}^{2n} \to \mathbb{U}^{2n}$ are both the identity map. We thus get the following:

6.5. Corollary. *Assume that (K, δ) is an ordinary differential field of characteristic zero which is large as a field. Then, (K, δ) is differentially large if and only if*

$(\diamondsuit')$ *for every K-irreducible Zariski-closed set W of $\mathbb{U}^{2n}$ with a smooth K-point such that $W \subseteq \tau_\delta(\pi(W))$, the set of K-points of W of the form $(a, \delta a)$ is Zariski dense in W.*

6.6. Remark. (i) If K is algebraically closed of characteristic zero, then Corollary 6.5 yields the classical algebraic-geometric axiomatization of DCF_0 given by Pierce and Pillay in [22].

(ii) If K has a model complete theory T in the language of fields and if K is large, then Corollary 6.5 yields a slight variation of the geometric axiomatization of T_D given by Brouette, Cousins, Pillay and Point in [4, Lemma 1.6].

(iii) For large and topological fields with a single derivation, an alternative description of differentially large fields with reference to the topology may be found in [9].

References

[1] M. Aschenbrenner, A. Chernikov, A. Gehret, and M. Ziegler, "Distality in valued fields and related structures", *Trans. Amer. Math. Soc.* **375**:7 (2022), 4641–4710. MR Zbl

[2] A. Bachmayr, D. Harbater, J. Hartmann, and F. Pop, "Large fields in differential Galois theory", *J. Inst. Math. Jussieu* **20**:6 (2021), 1931–1946. MR Zbl

[3] L. Bary-Soroker and A. Fehm, "Open problems in the theory of ample fields", pp. 1–11 in *Geometric and differential Galois theories*, edited by D. Bertrand et al., Sémin. Congr. **27**, Soc. Math. France, Paris, 2013. MR

[4] Q. Brouette, G. Cousins, A. Pillay, and F. Point, "Embedded Picard–Vessiot extensions", *Comm. Algebra* **46**:11 (2018), 4609–4615. MR Zbl

[5] J. Dobrowolski, D. M. Hoffmann, and J. Lee, "Elementary equivalence theorem for PAC structures", *J. Symb. Log.* **85**:4 (2020), 1467–1498. MR Zbl

[6] M. D. Fried and M. Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Math. (3) **11**, Springer, 2008. MR Zbl

[7] R. Gustavson and O. L. Sánchez, "Effective bounds for the consistency of differential equations", *J. Symbolic Comput.* **89** (2018), 41–72. MR Zbl

[8] N. Guzy and F. Point, "Topological differential fields", *Ann. Pure Appl. Logic* **161**:4 (2010), 570–598. MR

[9] N. Guzy and C. Rivière, "Geometrical axiomatization for model complete theories of differential topological fields", *Notre Dame J. Formal Logic* **47**:3 (2006), 331–341. MR Zbl

[10] W. Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications **42**, Cambridge University Press, 1993. MR Zbl

[11] D. M. Hoffmann, "Model theoretic dynamics in Galois fashion", *Ann. Pure Appl. Logic* **170**:7 (2019), 755–804. MR Zbl

[12] E. R. Kolchin, *Differential algebra and algebraic groups*, Pure and Applied Mathematics **54**, Academic Press, New York, 1973. MR Zbl

[13] B. A. Lando, "Jacobi's bound for the order of systems of first order differential equations", *Trans. Amer. Math. Soc.* **152** (1970), 119–135. MR

[14] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, 2002. MR Zbl

[15] O. León Sánchez, *Contributions to the model theory of partial differential fields*, Ph.D. thesis, University of Waterloo, 2013, available at http://hdl.handle.net/10012/7752.

[16] O. León Sánchez, "On the model companion of partial differential fields with an automorphism", *Israel J. Math.* **212**:1 (2016), 419–442. MR Zbl

[17] O. León Sánchez, "Algebro-geometric axioms for $\mathrm{DCF}_{0,m}$", *Fund. Math.* **243**:1 (2018), 1–8. MR Zbl

[18] O. León Sánchez and A. Pillay, "Differential Galois cohomology and parameterized Picard–Vessiot extensions", *Commun. Contemp. Math.* **23**:8 (2021), 2050081. MR

[19] O. León Sánchez and M. Tressl, "Differential Weil descent", *Comm. Algebra* **50**:1 (2022), 104–114. MR Zbl

[20] R. Moosa and T. Scanlon, "Jet and prolongation spaces", *J. Inst. Math. Jussieu* **9**:2 (2010), 391–430. MR Zbl

[21] R. Moosa, A. Pillay, and T. Scanlon, "Differential arcs and regular types in differential fields", *J. Reine Angew. Math.* **620** (2008), 35–54. MR Zbl

[22] D. Pierce and A. Pillay, "A note on the axioms for differentially closed fields of characteristic zero", *J. Algebra* **204**:1 (1998), 108–115. MR

[23] A. Pillay, "Some foundational questions concerning differential algebraic groups", *Pacific J. Math.* **179**:1 (1997), 179–200. MR Zbl

[24] A. Pillay and D. Polkowska, "On PAC and bounded substructures of a stable structure", *J. Symbolic Logic* **71**:2 (2006), 460–472. MR Zbl

[25] N. M. Polkowska, "On simplicity of bounded pseudoalgebraically closed structures", *J. Math. Log.* **7**:2 (2007), 173–193. MR Zbl

[26] F. Pop, "Embedding problems over large fields", *Ann. of Math.* (2) **144**:1 (1996), 1–34. MR Zbl

[27] F. Pop, "Henselian implies large", *Ann. of Math.* (2) **172**:3 (2010), 2183–2195. MR Zbl

[28] F. Pop, "Little survey on large fields — old & new", pp. 432–463 in *Valuation theory in interaction*, edited by A. Campillo et al., Eur. Math. Soc., Zürich, 2014. MR Zbl

[29] T. Sander, "Aspects of algebraic geometry over non algebraically closed fields", ICSI technical report, 1996, available at http://www.icsi.berkeley.edu/icsi/publication_details?n=1063.

[30] J. Sanz, "Asymptotic analysis and summability of formal power series", pp. 199–262 in *Analytic, algebraic and geometric aspects of differential equations*, edited by G. Filipuk et al., Springer, 2017. MR Zbl

[31] M. F. Singer, "A class of differential fields with minimal differential closures", *Proc. Amer. Math. Soc.* **69**:2 (1978), 319–322. MR Zbl

[32] M. F. Singer, "The model theory of ordered differential fields", *J. Symbolic Logic* **43**:1 (1978), 82–91. MR Zbl

[33] M. Tressl, "A structure theorem for differential algebras", pp. 201–206 in *Differential Galois theory* (Będlewo, 2001), edited by T. Crespo and Z. Hajto, Banach Center Publ. **58**, Polish Acad. Sci. Inst. Math., Warsaw, 2002. MR Zbl

[34] M. Tressl, "The uniform companion for large differential fields of characteristic 0", *Trans. Amer. Math. Soc.* **357**:10 (2005), 3933–3951. MR Zbl

Communicated by Anand Pillay
Received 2021-04-21 Revised 2022-06-14 Accepted 2023-03-20

omar.sanchez@manchester.ac.uk *Department of Mathematics, University of Manchester, Manchester, United Kingdom*

marcus.tressl@manchester.ac.uk *Department of Mathematics, University of Manchester, Manchester, United Kingdom*

ALGEBRA AND NUMBER THEORY 18:2 (2024)
https://doi.org/10.2140/ant.2024.18.281

p-groups, p-rank, and semistable reduction of coverings of curves

Yu Yang

We prove various explicit formulas concerning p-rank of p-coverings of pointed semistable curves over discrete valuation rings. In particular, we obtain a full generalization of Raynaud's formula for p-rank of fibers over *nonmarked smooth* closed points in the case of *arbitrary* closed points. As an application, for abelian p-coverings, we give an affirmative answer to an open problem concerning boundedness of p-rank asked by Saïdi more than twenty years ago.

Introduction

Let R be a complete discrete valuation ring with algebraically closed residue field k of characteristic $p > 0$ and $S \overset{\text{def}}{=} \operatorname{Spec} R$. Write K for the quotient field of R, $\eta : \operatorname{Spec} K \to S$ for the generic point of S, and $s : \operatorname{Spec} k \to S$ for the closed point of S. Let $\mathscr{X} = (X, D_X)$ be a pointed semistable curve of genus g_X over S. Here, X denotes the underlying semistable curve of $\mathscr{X}$, and D_X denotes the finite (ordered) set of marked points of $\mathscr{X}$. Write $\mathscr{X}_\eta = (X_\eta, D_{X_\eta})$ and $\mathscr{X}_s = (X_s, D_{X_s})$ for the generic fiber and the special fiber of $\mathscr{X}$, respectively. Moreover, we suppose that $\mathscr{X}_\eta$ is a smooth pointed stable curve over η, i.e., D_X satisfies [Knudsen 1983, Definition 1.1(iv)].

MSC2020: primary 14E20, 14G17; secondary 14G20, 14H30.
Keywords: p-rank, semistable reduction, pointed semistable curve, pointed semistable covering.

0A. ***Raynaud's formula for p-rank of nonfinite fibers.***

0A1. Let G be a finite group, and let $\mathscr{Y}_\eta = (Y_\eta, D_{Y_\eta})$ be a smooth pointed stable curve over η and $f_\eta : \mathscr{Y}_\eta \to \mathscr{X}_\eta$ a morphism of pointed stable curves over η. Suppose that f_η is a Galois covering whose Galois group is isomorphic to G, that $f_\eta^{-1}(D_{X_\eta}) = D_{Y_\eta}$, and that the branch locus of f_η is contained in D_{X_η}. By replacing S by a finite extension of S (i.e., the spectrum of the normalization of R in a finite extension of K), f_η extends to a *G-pointed semistable covering*

$$f : \mathscr{Y} = (Y, D_Y) \to \mathscr{X}$$

over S (see Definition 1.5 and Proposition 1.6). We write $\mathscr{Y}_s = (Y_s, D_{Y_s})$ for the special fiber of $\mathscr{Y}$ and $f_s : \mathscr{Y}_s \to \mathscr{X}_s$ for the morphism of pointed semistable curves over s induced by f.

Suppose that the order of G is prime to p. Then f_s is a finite, generically étale morphism [SGA 1 1971; Vidal 2001]. On the other hand, suppose that $p \mid \#G$. Then the situation is quite different from that in the case of prime-to-p coverings. The geometry of $\mathscr{Y}_s$ is very complicated and the morphism f_s is not generically étale and, moreover, is *not finite* in general. This kind of phenomenon is called "resolution of nonsingularities" [Tamagawa 2004b] which has many important applications in the theory of arithmetic fundamental groups and anabelian geometry, e.g., [Mochizuki 1996; Lepage 2013; Pop and Stix 2017; Stix 2002].

0A2. M. Raynaud [1990] investigated the geometry of reduction of étale p-group schemes over $\mathscr{X}_\eta$ (i.e., G is a p-group), and proved an explicit formula for the p-rank (see Section 1B3 for the definition of p-rank) of nonfinite fibers of f_s. More precisely, we have the following famous result which is the main theorem of Raynaud.

Theorem 0.1 [Raynaud 1990, Théorèmes 1 et 2]. *Let G be a finite p-group, and let $f : \mathscr{Y} \to \mathscr{X}$ be a G-pointed semistable covering over S and x a closed point of $\mathscr{X}_s$. Suppose that x is a* ***nonmarked smooth*** *point (i.e., $x \notin X_s^{\mathrm{sing}} \cup D_{X_s}$, where X_s^{sing} denote the singular locus of X_s) of $\mathscr{X}_s$. Then we have the following formula for the p-rank of $f^{-1}(x)$:*

$$\sigma(f^{-1}(x)) = 0.$$

In particular, suppose that $\mathscr{X}$ is a smooth pointed stable curve (i.e., X is stable and $D_X = \varnothing$) over S. As a direct consequence of the above formula, the following statements hold:

(i) *The Jacobian of $\mathscr{Y}_\eta$ has potentially good reduction.*

(ii) *The dual semigraph (Section 1B2) of $\mathscr{Y}_s$ is a tree (Section 1A3).*

(iii) *The slopes of the crystalline cohomology of connected components of vertical fibers of f are in* $(0, 1)$.

Remark 0.1.1. If x is *not* a nonmarked smooth point of $\mathscr{X}_s$, $\sigma(f^{-1}(x))$ is not equal to 0 in general. For instance, if x is a singular point of $\mathscr{X}_s$, the dual semigraph of $f^{-1}(x)$ is no longer to be a tree even the simplest case where $G = \mathbb{Z}/p\mathbb{Z}$.

On the other hand, if G is not a p-group, the p-rank of irreducible components of $\mathscr{Y}_s$ cannot be calculated explicitly in general (see Remark 1.4.1).

0B. ***Main result.*** We maintain the notation introduced in Section 0A. In the present paper, we give a full generalization of Raynaud's formula. Namely, we will prove various formulas for $\sigma(f^{-1}(x))$ where x is an *arbitrary* closed point of $\mathscr{X}_s$. Note that if $f^{-1}(x)$ is finite, then $\sigma(f^{-1}(x)) = 0$ by the definition of p-rank. Moreover, since f is a Galois covering, to calculate $\sigma(f^{-1}(x)) = 0$, we only need to calculate the p-rank of a connected component of $f^{-1}(x)$. Thus, to calculate $\sigma(f^{-1}(x))$, we may assume that $f^{-1}(x)$ is *nonfinite* and *connected.*

0B1. Our main result is the following formulas for $\sigma(f^{-1}(x))$ in terms of the orders of inertia subgroups of irreducible components of $f^{-1}(x)$ which depend only on the action of G on $f^{-1}(x)$ (in the introduction, we do not give the list of definitions of the notation appeared in the main theorem, see Theorems 3.4 and 3.9 for more precise forms):

Theorem 0.2. *Let G be a finite p-group, and let $f : \mathscr{Y} \to \mathscr{X}$ be a G-pointed semistable covering over S and x an* ***arbitrary*** *closed point of $\mathscr{X}_s$. Suppose that $f^{-1}(x)$ is nonfinite and connected. Then we have* (*see Section 3B3 for $\Gamma_{\mathscr{E}_X}$, Section 3A5 for $\#I_v$, $\#I_e$, and Section 1A1 for $v(\Gamma_{\mathscr{E}_X})$, $e(v)$, $e^{\mathrm{cl}}(\Gamma_{\mathscr{E}_X})$*)

$$\sigma(f^{-1}(x)) = \sum_{v\in v(\Gamma_{\mathscr{E}_X})} \Bigl(1 - \#G/\#I_v + \sum_{e\in e(v)} (\#G/\#I_e)(\#I_e/\#I_v - 1)\Bigr) + \sum_{e\in e^{\mathrm{cl}}(\Gamma_{\mathscr{E}_X})} (\#G/\#I_e - 1).$$

Moreover, suppose that x is a ***singular*** *point of $\mathscr{X}_s$. Then we have a simpler form as follows*:

$$\sigma(f^{-1}(x)) = \sum_{\#I\in\mathcal{I}(x)} \#G/\#I - \sum_{\#J\in\mathcal{J}(x)} \#G/\#J + 1,$$

where $\mathcal{I}(x)$ and $\mathcal{J}(x)$ are the sets of minimal and maximal orders of inertia subgroups associated to x and f (*see Definition 3.5*(*b*)), *respectively.*

0B2. If x is a nonmarked smooth closed point of $\mathscr{X}_s$, Raynaud's formula (i.e., Theorem 0.1) can be deduced by the first formula of Theorem 0.2 (see Section 3B7). If x is a singular closed point of $\mathscr{X}_s$, the p-rank $\sigma(f^{-1}(x))$ had been studied by M. Saïdi [1998a; 1998b] under the assumption where G is a *cyclic* p-group, and his result can be deduced by the second formula of Theorem 0.2 (see Corollary 3.11). Moreover, as an application, in Section 4 of the present paper, by applying the "moreover" part of Theorem 0.2, we give an affirmative answer to an open problem posed by Saïdi (Section 4A) when G is an abelian p-group (see Theorem 4.3).

On the other hand, our approach to proving the formulas for $\sigma(f^{-1}(x))$ is *completely different* from that of Raynaud and Saïdi (Saïdi's method is close to the method of Raynaud), and we calculate $\sigma(f^{-1}(x))$ by introducing a kind of new object which we call *semigraphs with p-rank* (Section 2). Moreover, our method can be used not only for calculating the p-rank of a fiber $f^{-1}(x)$ of a closed point x, but also for *calculating the p-rank $\sigma(\mathscr{Y}_s)$ of the special fiber $\mathscr{Y}_s$* of $\mathscr{Y}$ (see Theorem 3.2 for a formula for $\sigma(\mathscr{Y}_s)$).

0C. ***Strategy of proof.*** We briefly explain the method of proving Theorem 0.2.

0C1. We maintain the notation introduced in Section 0B. To calculate the p-rank $\sigma(f^{-1}(x))$ of $f^{-1}(x)$, we need to calculate (i) the p-rank of the normalizations of irreducible components of $f^{-1}(x)$, and (ii) the Betti number γ_x 1A3 of the dual semigraph Γ_x 1B2 of $f^{-1}(x)$. By using the general theory of semistable curves, (i) can be obtained by using the Deuring–Shafarevich formula (Proposition 1.4).

The major difficulty is (ii). In the cases treated by Raynaud and Saïdi, the geometry of the fiber $f^{-1}(x)$ is well-managed (in fact, Γ_x is a tree when x is a nonmarked smooth point). On the other hand, in the general case (i.e., x is an arbitrary closed point and G is an arbitrary p-group), the geometry of $f^{-1}(x)$ is very complicated, and its dual semigraph is *far from being tree-like*.

0C2. The author observed that we can "avoid" to compute directly the Betti number γ_x of Γ_x if $f^{-1}(x)$ admits a good "deformation" such that the decomposition groups of irreducible components of the deformation are G, and that $\sigma(f^{-1}(x))$ is equal to the p-rank of the deformation. However, in general, such deformations *do not exist* in the theory of algebraic geometry (i.e., we cannot find such deformations in moduli spaces of curves, see Remark 2.4.1).

To overcome this difficulty, we introduce the so-called *semigraphs with p-rank* (Section 2), and define p-rank, coverings, and G-coverings for semigraphs with p-rank. Moreover, we can deform semigraphs with p-rank in a natural way, and prove that the deformations do not change the p-rank of semigraphs with p-rank (Proposition 2.6). Then we may obtain an explicit formula for the p-rank of G-coverings of semigraphs with p-rank (Theorem 2.7). Furthermore, by using the theory of semistable curves, we construct semigraphs with p-rank (Section 3) from G-pointed semistable coverings (in particular, we construct a semigraph with p-rank from $f^{-1}(x)$). Together with some precise analysis of inertia groups (Section 1) of singular points and irreducible components of G-pointed semistable coverings, we obtain Theorem 0.2.

0D. ***Structure of the present paper.*** The present paper is organized as follows. In Section 1, we introduce some notation concerning semigraphs, pointed semistable curves, and pointed semistable coverings. Moreover, we prove some results concerning inertia subgroups of singular points and irreducible components of pointed semistable coverings. In Section 2, we introduce semigraphs with p-rank, and study the p-rank of G-coverings of semigraphs with p-rank. In Section 3, we construct various G-coverings of semigraphs with p-rank from G-pointed semistable coverings. Moreover, by applying the results obtained in Section 2, we obtain various formulas for p-rank concerning G-pointed semistable coverings. In Section 4, we study bounds of p-rank of vertical fibers of G-pointed semistable coverings by using formulas obtained in Section 3.

1. Pointed semistable coverings

In this section, we introduce pointed semistable coverings of pointed semistable curves over discrete valuation rings.

1A. ***Semigraphs.*** We begin with some general remarks concerning semigraphs; see also [Mochizuki 2006, Section 1].

1A1. A *semigraph* $\mathbb{G}$ consists of the following data:

(i) A set $v(\mathbb{G})$ whose elements we refer to as vertices.

(ii) A set $e(\mathbb{G})$ whose elements we refer to as edges. Moreover, any element $e \in e(\mathbb{G})$ is a set of cardinality 2 satisfying the following property: for each $e \neq e' \in e(\mathbb{G})$, we have $e \cap e' = \varnothing$.

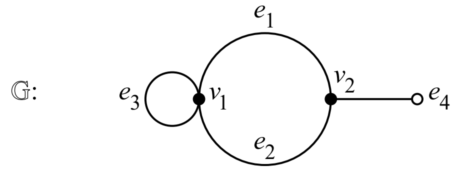
(iii) A set of maps $\{\zeta_e^{\mathbb{G}}\}_{e \in e(\mathbb{G})}$ such that $\zeta_e^{\mathbb{G}} : e \to v(\mathbb{G}) \cup \{v(\mathbb{G})\}$ is a map from the set e to the set $v(\mathbb{G}) \cup \{v(\mathbb{G})\}$, and that $\#((\zeta_e^{\mathbb{G}})^{-1}(\{v(\mathbb{G})\})) \in \{0, 1\}$, where $\#(-)$ denotes the cardinality of $(-)$.

Let $e \in e(\mathbb{G})$ be an edge of $\mathbb{G}$. We shall refer to an element $b \in e$ as a *branch* of the edge e. We shall call that $e \in e(\mathbb{G})$ is *closed* (resp. *open*) if $\#((\zeta_e^{\mathbb{G}})^{-1}(\{v(\mathbb{G})\})) = 0$ (resp. $\#((\zeta_e^{\mathbb{G}})^{-1}(\{v(\mathbb{G})\})) = 1$). Moreover, write $e^{\mathrm{cl}}(\mathbb{G})$ for the set of closed edges of $\mathbb{G}$ and $e^{\mathrm{op}}(\mathbb{G})$ for the set of open edges of $\mathbb{G}$. Note that we have $e(\mathbb{G}) = e^{\mathrm{cl}}(\mathbb{G}) \cup e^{\mathrm{op}}(\mathbb{G})$.

Let $v \in v(\mathbb{G})$ be a vertex of $\mathbb{G}$. Write $b(v)$ for the set of branches $\bigcup_{e \in e(\mathbb{G})} (\zeta_e^{\mathbb{G}})^{-1}(v)$, $e(v)$ for the set of edges which abut to v, and $v(e)$ for the set of vertices which are abutted by e. Note that we have $\#(v(e)) \leq 2$. We shall call a closed edge $e \in e^{\mathrm{cl}}(\mathbb{G})$ *loop* if $\#v(e) = 1$ (i.e., $\#(\zeta_e^{\mathbb{G}}(e)) = 1$). Moreover, we use the notation $e^{\mathrm{lp}}(v)$ to denote the set of loops which abut to v.

Example 1.1. Let us give an example of semigraph to explain the above definitions. We use the notation "•" and "∘ with a line segment" to denote a vertex and an open edge, respectively.

Let $\mathbb{G}$ be a semigraph as follows:



Then we have $v(\mathbb{G}) = \{v_1, v_2\}$, $e(\mathbb{G}) = \{e_1, e_2, e_3, e_4\}$, $e^{\mathrm{cl}}(\mathbb{G}) = \{e_1, e_2, e_3\}$, $e^{\mathrm{op}}(\mathbb{G}) = \{e_4\}$, $\zeta_{e_1}^{\mathbb{G}}(e_1) = \zeta_{e_2}^{\mathbb{G}}(e_2) = \{v_1, v_2\}$, $\zeta_{e_3}^{\mathbb{G}}(e_3) = \{v_1\}$, and $\zeta_{e_4}^{\mathbb{G}}(e_4) = \{v_2, \{v(\mathbb{G})\}\}$. Moreover, we have $e^{\mathrm{lp}}(\mathbb{G}) = e^{\mathrm{lp}}(v_1) = \{e_3\}$, $v(e_1) = v(e_2) = \{v_1, v_2\}$, $v(e_3) = \{v_1\}$, $v(e_4) = \{v_2\}$, $e(v_1) = \{e_1, e_2, e_3\}$, and $e(v_2) = \{e_1, e_2, e_4\}$.

1A2. Let $\mathbb{G}$ be a semigraph. We shall call $\mathbb{G}'$ a *subsemigraph* of $\mathbb{G}$ if $\mathbb{G}'$ is a semigraph satisfying the following conditions:

(i) $v(\mathbb{G}')$ (resp. $e(\mathbb{G}')$) is a subset of $v(\mathbb{G})$ (resp. $e(\mathbb{G})$).

(ii) If $e \in e^{\mathrm{cl}}(\mathbb{G}')$, then $\zeta_e^{\mathbb{G}'}(e) \overset{\mathrm{def}}{=} \zeta_e^{\mathbb{G}}(e)$.

(iii) If $e = \{b_1, b_2\} \in e^{\mathrm{op}}(\mathbb{G}')$ such that $\zeta_e^{\mathbb{G}}(b_1) \in v(\mathbb{G}')$ and $\zeta_e^{\mathbb{G}}(b_2) \notin v(\mathbb{G}')$, then $\zeta_e^{\mathbb{G}'}(b_1) \overset{\mathrm{def}}{=} \zeta_e^{\mathbb{G}}(b_1)$ and $\zeta_e^{\mathbb{G}'}(b_2) \overset{\mathrm{def}}{=} \{v(\mathbb{G}')\}$.

Moreover, we define a semigraph $\mathbb{G} \setminus \mathbb{G}'$ as follows:

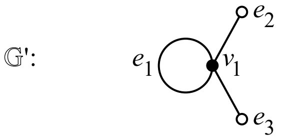
(i) $v(\mathbb{G} \setminus \mathbb{G}') \stackrel{\text{def}}{=} v(\mathbb{G}) \setminus v(\mathbb{G}')$.

(ii) $e^{\text{cl}}(\mathbb{G} \setminus \mathbb{G}') \stackrel{\text{def}}{=} \{e \in e^{\text{cl}}(\mathbb{G}) \mid v(e) \subseteq v(\mathbb{G} \setminus \mathbb{G}') \text{ in } \mathbb{G}\}$.

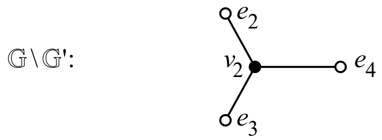
(iii) $e^{\text{op}}(\mathbb{G} \setminus \mathbb{G}') \stackrel{\text{def}}{=} \{e \in e^{\text{cl}}(\mathbb{G}) \mid v(e) \cap v(\mathbb{G}') \neq \varnothing \text{ in } \mathbb{G} \text{ and } v(e) \cap v(\mathbb{G} \setminus \mathbb{G}') \neq \varnothing \text{ in } \mathbb{G}\}$
$$\cup \{e \in e^{\text{op}}(\mathbb{G}) \mid v(e) \cap v(\mathbb{G} \setminus \mathbb{G}') \neq \varnothing \text{ in } \mathbb{G}\}.$$

(iv) For each $e = \{b_i\}_{i \in \{1,2\}} \in e^{\text{cl}}(\mathbb{G} \setminus \mathbb{G}') \cup e^{\text{op}}(\mathbb{G} \setminus \mathbb{G}')$, we put
$$\zeta_e^{\mathbb{G} \setminus \mathbb{G}'}(b_i) \stackrel{\text{def}}{=} \begin{cases} \zeta_e^{\mathbb{G}}(b_i) & \text{if } \zeta_e^{\mathbb{G}}(b_i) \notin v(\mathbb{G}') \text{ and } \zeta_e^{\mathbb{G}}(b_i) \neq \{v(\mathbb{G})\}, \\ \{v(\mathbb{G} \setminus \mathbb{G}')\} & \text{otherwise.} \end{cases}$$

Example 1.2. We give some examples to explain the above definition. Let $\mathbb{G}$ be the semigraph of Example 1.1 and $\mathbb{G}'$ be a subsemigraph as follows:



Moreover, the semigraph $\mathbb{G} \setminus \mathbb{G}'$ is the following:



Remark 1.2.1. We explain the motivation of the constructions of $\mathbb{G}'$ and $\mathbb{G} \setminus \mathbb{G}'$. Let $\mathscr{X} = (X, D_X)$ be a pointed semistable curve (Section 1B1) over an algebraically closed field such that the dual semigraph $\Gamma_{\mathscr{X}}$ (Section 1B1) is equal to $\mathbb{G}$ defined in Example 1.1. Write X_{v_1} and X_{v_2} for the irreducible components corresponding to v_1 and v_2, respectively. Then we have the following natural pointed semistable curves:
$$(X_{v_1}, D_{X_{v_1}} \stackrel{\text{def}}{=} X_{v_1} \cap X_{v_2}), \quad (X_{v_2}, D_{X_{v_2}} \stackrel{\text{def}}{=} (X_{v_1} \cap X_{v_2}) \cup D_X)$$
whose dual semigraphs are equal to $\mathbb{G}'$ and $\mathbb{G} \setminus \mathbb{G}'$ defined in Example 1.2, respectively.

1A3. A semigraph $\mathbb{G}$ will be called *finite* if $v(\mathbb{G})$ and $e(\mathbb{G})$ are finite. In the present paper, *we only consider finite semigraphs.* Since a semigraph can be regarded as a topological space (i.e., a subspace of $\mathbb{R}^2$), we shall call $\mathbb{G}$ *connected* if $\mathbb{G}$ is connected as a topological space. Moreover, we write
$$\gamma_{\mathbb{G}} \stackrel{\text{def}}{=} \dim_{\mathbb{C}}(H^1(\mathbb{G}, \mathbb{C}))$$
for the Betti number of $\mathbb{G}$, where $\mathbb{C}$ denotes the field of complex numbers. In particular, we shall call $\mathbb{G}$ a *tree* (or $\mathbb{G}$ *tree-like*) if $\gamma_{\mathbb{G}} = 0$.

Let $\mathbb{G}$ and $\mathbb{H}$ be two semigraphs. A *morphism* between semigraphs $\mathbb{G} \to \mathbb{H}$ is a collection of maps $v(\mathbb{G}) \to v(\mathbb{H})$, $e^{\text{cl}}(\mathbb{G}) \to e^{\text{cl}}(\mathbb{H})$, and $e^{\text{op}}(\mathbb{G}) \to e^{\text{op}}(\mathbb{H})$ satisfying the following: for each $e_{\mathbb{G}} \in e(\mathbb{G})$, write $e_{\mathbb{H}} \in e(\mathbb{H})$ for the image of $e_{\mathbb{G}}$; then the map $e_{\mathbb{G}} \xrightarrow{\sim} e_{\mathbb{H}}$ is a bijection, and is compatible with the $\{\zeta_e^{\mathbb{G}}\}_{e\in e(\mathbb{G})}$ and $\{\zeta_e^{\mathbb{H}}\}_{e\in e(\mathbb{H})}$.

1B. *Pointed semistable curves.*

1B1. Let $\mathscr{C} \overset{\text{def}}{=} (C, D_C)$ be a *pointed semistable curve* over a scheme A, namely, a marked curve over A such that every geometric fiber $C_{\bar{a}}$, $a \in A$, is a semistable curve, and that $D_{C_{\bar{a}}} \subseteq C_{\bar{a}}^{\text{sm}}$, where $C_{\bar{a}}^{\text{sm}}$ denotes the smooth locus of $C_{\bar{a}}$. We shall call C the underlying curve of $\mathscr{C}$ and the finite (ordered) set D_C the set of marked points of $\mathscr{C}$. In particular, we shall call that $\mathscr{C}$ is a *pointed stable curve* if D_C satisfies [Knudsen 1983, Definition 1.1 (iv)].

1B2. Suppose that A is the spectrum of an algebraically closed field. We write $\mathrm{Irr}(C)$ for the set of the irreducible components of C and C^{sing} for the set of singular points (or nodes) of C. We define the *dual semigraph* $\Gamma_{\mathscr{C}}$ of the pointed semistable curve $\mathscr{C}$ to be the following semigraph:

(i) $v(\Gamma_{\mathscr{C}}) \overset{\text{def}}{=} \{v_E\}_{E\in\mathrm{Irr}(C)}$.

(ii) $e^{\text{cl}}(\Gamma_{\mathscr{C}}) \overset{\text{def}}{=} \{e_s\}_{s\in C^{\text{sing}}}$ and $e^{\text{op}}(\Gamma_{\mathscr{C}}) \overset{\text{def}}{=} \{e_m\}_{m\in D_C}$.

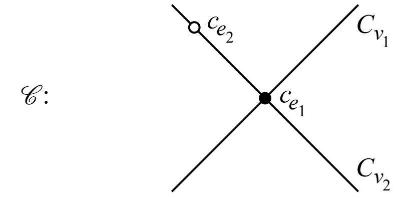
(iii) For each $e_s = \{b_s^1, b_s^2\} \in e^{\text{cl}}(\Gamma_{\mathscr{C}})$, $s \in C^{\text{sing}}$, we put
$$\zeta_{e_s}^{\Gamma_{\mathscr{C}}}(e_s) \overset{\text{def}}{=} \{v_E \in v(\Gamma_{\mathscr{C}}) \mid s \in E\}.$$

(iv) For each $e_m = \{b_m^1, b_m^2\} \in e^{\text{op}}(\Gamma_{\mathscr{C}})$, $m \in D_C$, we put
$$\zeta_{e_m}^{\Gamma_{\mathscr{C}}}(b_m^1) \overset{\text{def}}{=} v_E, \quad \zeta_{e_m}^{\Gamma_{\mathscr{C}}}(b_m^2) \overset{\text{def}}{=} \{v(\Gamma_{\mathscr{C}})\},$$
where E is the irreducible component of C satisfying $m \in E$.

Moreover, we put (see Section 1A3)
$$\gamma_{\mathscr{C}} \overset{\text{def}}{=} \gamma_{\Gamma_{\mathscr{C}}} = \dim_{\mathbb{C}}(H^1(\Gamma_{\mathscr{C}}, \mathbb{C})).$$

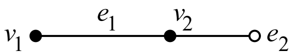
Let $v \in v(\Gamma_{\mathscr{C}})$ (resp. $e \in e^{\text{cl}}(\Gamma_{\mathscr{C}})$, $e \in e^{\text{op}}(\Gamma_{\mathscr{C}})$). We write C_v (resp. c_e, c_e) for the irreducible component of C corresponding to v (resp. the singular point of C corresponding to e, the marked point of $\mathscr{C}$ corresponding to e) and $\widetilde{C}_v$ for the normalization of C_v.

Example 1.3. We give an example to explain dual semigraphs of pointed semistable curves. Let $\mathscr{C} \overset{\text{def}}{=} (C, D_C)$ be a pointed semistable curve over k whose irreducible components are C_{v_1} and C_{v_2}, whose node is c_{e_1}, and whose marked point is $c_{e_2} \in C_{v_2}$. We use the notation "•" and "∘" to denote a node and a marked point, respectively. Then $\mathscr{C}$ is as follows:



We write v_1 and v_2 for the vertices of $\Gamma_{\mathscr{C}}$ corresponding to C_{v_1} and C_{v_2}, respectively, e_1 for the closed edge corresponding to c_{e_1}, and e_2 for the open edge corresponding to c_{e_2}. Moreover, we use the notation "•" and "○ with a line segment" to denote a vertex and an open edge, respectively. Then the dual semigraph $\Gamma_{\mathscr{C}}$ of $\mathscr{C}$ is as follows:

$\Gamma_{\mathscr{C}}$:



1B3. Let C be a disjoint union of projective curves over an algebraically closed field of characteristic $p > 0$. We define the *p-rank* (or *Hasse–Witt invariant*) $\sigma(C)$ of C to be

$$\sigma(C) \overset{\text{def}}{=} \dim_{\mathbb{F}_p}(H^1_{\text{ét}}(C, \mathbb{F}_p)).$$

Moreover, let $\mathscr{C} \overset{\text{def}}{=} (C, D_C)$ be a pointed semistable curve over an algebraically closed field of characteristic $p > 0$. Write $\Gamma_{\mathscr{C}}$ for the dual semigraph of $\mathscr{C}$. Then we put

$$\sigma(\mathscr{C}) \overset{\text{def}}{=} \sigma(C) = \gamma_{\mathscr{C}} + \sum_{v \in v(\Gamma_C)} \sigma(\widetilde{C}_v).$$

1B4. Let G be a finite p-group. The p-rank of a Galois covering whose Galois group is isomorphic to G can be calculated by the Deuring–Shafarevich formula (or Crew's formula) as follows:

Proposition 1.4 [Crew 1984, Corollary 1.8]. *Let $h : C' \to C$ be a (possibly ramified) Galois covering of smooth projective curves over an algebraically closed field of characteristic $p > 0$ whose Galois group is a finite p-group G. Then we have*

$$\sigma(C') - 1 = \#G(\sigma(C) - 1) + \sum_{c' \in (C')^{\text{cl}}} (e_{c'} - 1),$$

where $(C')^{\text{cl}}$ denotes the set of closed points of C' and $e_{c'}$ denotes the ramification index at c'.

Remark 1.4.1. We maintain the notation introduced in Proposition 1.4. Suppose that G is *not* a p-group. Then $\sigma(C')$ cannot be calculated explicitly in general. In fact, the p-rank (or more precisely, generalized Hasse–Witt invariants) of prime-to-p étale coverings can almost determine the isomorphism class of C, e.g., [Tamagawa 2004a; Yang 2018].

1C. *Pointed semistable coverings.*

1C1. *Settings.* We fix some notation of the present subsection. Let R be a complete discrete valuation ring with algebraically closed residue field k of characteristic $p > 0$ and K the quotient field. We put $S \overset{\text{def}}{=} \operatorname{Spec} R$. Write η and s for the generic point and the closed point corresponding to the natural morphisms $\operatorname{Spec} K \to S$ and $\operatorname{Spec} k \to S$, respectively. Let $\mathscr{X} \overset{\text{def}}{=} (X, D_X)$ be a pointed semistable curve over S. Write $\mathscr{X}_\eta \overset{\text{def}}{=} (X_\eta, D_{X_\eta})$ for the generic fiber of $\mathscr{X}$, $\mathscr{X}_s \overset{\text{def}}{=} (X_s, D_{X_s})$ for the special fiber of $\mathscr{X}$, and $\Gamma_{\mathscr{X}_s}$ for the dual semigraph of $\mathscr{X}_s$. Moreover, we suppose that $\mathscr{X}_\eta$ is a *smooth pointed stable curve* over η (note that $\mathscr{X}_s$ is not a pointed stable curve in general).

1C2. Let $l : \mathscr{W} \overset{\text{def}}{=} (W, D_W) \to \mathscr{X}$ be a morphism of pointed semistable curves over S and G a finite group. We define pointed semistable coverings as follows:

Definition 1.5. The morphism l is called a *pointed semistable covering* (resp. *G-pointed semistable covering*) over S if the morphism

$$l_\eta : \mathscr{W}_\eta \overset{\text{def}}{=} (W_\eta, D_{W_\eta}) \to \mathscr{X}_\eta = (X_\eta, D_{X_\eta})$$

over η induced by l on generic fibers is a finite generically étale morphism (resp. a Galois covering whose Galois group is isomorphic to G) such that the following conditions hold:

(i) The branch locus of l_η is contained in D_{X_η}.

(ii) $l_\eta^{-1}(D_{X_\eta}) = D_{W_\eta}$.

(iii) The following universal property holds: if $g : \mathscr{W}' \to \mathscr{X}$ is a morphism of pointed semistable curves over S such that the generic fiber $\mathscr{W}'_\eta$ of $\mathscr{W}'$ and the morphism $g_\eta : \mathscr{W}'_\eta \to \mathscr{X}_\eta$ induced by g on generic fibers are equal to $\mathscr{W}_\eta$ and l_η, respectively, then there exists a unique morphism $h : \mathscr{W}' \to \mathscr{W}$ such that $g = l \circ h$.

We shall call l a *pointed stable covering* (resp. *G-pointed stable covering*) over S if l is a pointed semistable covering (resp. G-pointed semistable covering) over S, and $\mathscr{X}$ is a pointed stable curve over S. We shall call l a *semistable covering* (resp. *stable covering*, *G-semistable covering*, *G-stable covering*) over S if l is a pointed semistable covering (resp. pointed stable covering, G-pointed semistable covering, G-pointed stable covering) over S, and D_X is empty.

1C3. We have the following proposition.

Proposition 1.6. *Let $f_\eta : \mathscr{Y}_\eta \overset{\text{def}}{=} (Y_\eta, D_{Y_\eta}) \to \mathscr{X}_\eta$ be a finite morphism of pointed smooth curves over η. Suppose that the branch locus of f_η is contained in D_{X_η} and that $f_\eta^{-1}(D_{X_\eta}) = D_{Y_\eta}$. Then, by replacing S by a finite extension of S, f_η extends to a pointed semistable covering $f : \mathscr{Y} = (Y, D_Y) \to \mathscr{X}$ over S such that the restriction of f to the generic fibers is f_η.*

Proof. The proposition follows from [Liu 2006, Theorem 0.2 and Remark 4.13]. □

Remark 1.6.1. We maintain the notation introduced in Proposition 1.6. In fact, we have that f_η extends *uniquely* to a pointed semistable covering f. Let us explain roughly in this remark.

By adding some marked points, we may obtain a pointed stable curve $\mathscr{X}^{\text{add}} \overset{\text{def}}{=} (X^{\text{add}}, D_{X^{\text{add}}})$ whose underlying curve X^{add} is X, and whose set of marked points contains D_X. Write $D_{X^{\text{add}}_\eta}$ for $D_{X^{\text{add}}}|_\eta$, and $D_{Y^{\text{add}}_\eta}$ for $f_\eta^{-1}(D_{X^{\text{add}}_\eta})$. Then $D_{Y^{\text{add}}_\eta}$ contains D_{Y_η}. Moreover, we have a finite morphism of pointed smooth curves

$$f_\eta^{\text{add}} : \mathscr{Y}_\eta^{\text{add}} \to \mathscr{X}_\eta^{\text{add}}$$

over η induced by f_η.

By applying Proposition 1.6 and by replacing S by a finite extension of S, f_{η}^{add} extends to a pointed semistable covering

$$f^{\mathrm{add}} : \mathscr{Y}^{\mathrm{add}} \overset{\mathrm{def}}{=} (Y^{\mathrm{add}}, D_{Y^{\mathrm{add}}}) \to \mathscr{X}^{\mathrm{add}}$$

over S. Since $\mathscr{X}^{\mathrm{add}}$ is a pointed stable curve over S, we see that $\mathscr{Y}^{\mathrm{add}}$ is a pointed stable model of $\mathscr{Y}_{\eta}^{\mathrm{add}}$. Then the uniqueness of f^{add} follows from the uniqueness of the pointed stable model $\mathscr{Y}^{\mathrm{add}}$.

We put $D_Y^{\mathrm{ss}} \overset{\mathrm{def}}{=} D_Y^{\mathrm{add}} \setminus D_Y$ and $D_{Y_s}^{\mathrm{ss}} \overset{\mathrm{def}}{=} D_Y^{\mathrm{ss}}|_s$. Let $\mathrm{Con}(Y_s^{\mathrm{add}})$ be the subset of the set of irreducible components of Y_s^{add} consisting of all irreducible components E of Y_s^{add} satisfying the following conditions:

(i) E is isomorphic to $\mathbb{P}_k^1$.

(ii) $E \cap D_{Y_s}^{\mathrm{ss}} \neq \varnothing$ and $E \cap D_Y = \varnothing$.

(iii) $f^{\mathrm{add}}(E)$ is a closed point of $\mathscr{X}^{\mathrm{add}}$.

Note that $\mathrm{Con}(Y_s^{\mathrm{add}})$ may be an empty set. Then by forgetting the marked points D_Y^{ss} and by contracting the irreducible components of $\mathrm{Con}(Y_s^{\mathrm{add}})$ [Bosch et al. 1990, 6.7 Proposition 4], we obtain a pointed semistable curve $\mathscr{Y}$ and a morphism of pointed semistable curves $f : \mathscr{Y} \to \mathscr{X}$ over S induced by f^{add}. We see that f is a pointed semistable covering over S, and that f does not depend on the choices of $D_{X^{\mathrm{add}}}$. Moreover, the uniqueness follows from the uniqueness of f^{add}.

1C4. If a G-pointed semistable covering over S is finite, then it induces a morphism of dual semigraphs of special fibers. More precisely, we have the following result:

Proposition 1.7. *Let G be a finite group, $f : \mathscr{Y} = (Y, D_Y) \to \mathscr{X}$ a **finite** G-pointed semistable covering over S, and $\Gamma_{\mathscr{Y}_s}$ the dual semigraph of $\mathscr{Y}_s$. Then the images of nodes (resp. smooth points) of the special fiber $\mathscr{Y}_s$ of $\mathscr{Y}$ are nodes (resp. smooth points) of $\mathscr{X}_s$. In particular, the map of dual semigraphs $\Gamma_{\mathscr{Y}_s} \to \Gamma_{\mathscr{X}_s}$ induced by the morphism of the special fibers $f_s : \mathscr{Y}_s \to \mathscr{X}_s$ over s induced by f is a morphism of semigraphs 1A3.*

Proof. Let y be a closed point of $\mathscr{Y}$. Write $I_y \subseteq G$ for the inertia subgroup of y. Thus, the natural morphism $\mathscr{Y}/I_y \to \mathscr{X}$ induced by f is étale at the image of y of the quotient morphism $\mathscr{Y} \to \mathscr{Y}/I_y$. Then to verify the proposition, we may assume that $G = I_y$.

If y is a smooth point, then x is a smooth point [Raynaud 1990, Proposition 5]. If y is a node, let Y_1 and Y_2 be the irreducible components (which may be equal) of the underlying curve of the special fiber $\mathscr{Y}_s$ of $\mathscr{Y}$ containing y. Write $D_1 \subseteq G$ and $D_2 \subseteq G$ for the decomposition subgroups of Y_1 and Y_2, respectively. The proof of [Raynaud 1990, Proposition 5] implies the following:

(i) If D_1 and D_2 are not equal to $I_y = G$, then x is a smooth point.

(ii) If $D_1 = D_2 = G$, then x is a node.

Next, we prove that the case (i) will not occur. If D_1 and D_2 are not equal to G, then, for each $\tau \in G \setminus D_1$ (or $\tau \in G \setminus D_2$), we have $\tau(Y_1) = Y_2$ and $\tau(Y_2) = Y_1$. Thus, we obtain $D \overset{\mathrm{def}}{=} D_1 = D_2$. Moreover, D is a normal subgroup of G. By replacing I_y by I_y/D and $\mathscr{Y}$ by $\mathscr{Y}/D$, and by applying the case (ii), we may assume that D is trivial. Then f_s is étale at the generic points of Y_1 and Y_2. Consider the local morphism $f_y : \operatorname{Spec} \mathcal{O}_{\mathscr{Y},y} \to \operatorname{Spec} \mathcal{O}_{\mathscr{X},f(y)}$ induced by f. Since f_y is étale at all the points of $\operatorname{Spec} \mathcal{O}_{\mathscr{Y},y}$ corresponding to the prime ideals of $\mathcal{O}_{\mathscr{Y},y}$ of height 1, the Zariski–Nagata purity theorem implies that f_y is étale. This means that if $f(y)$ is a smooth point, y is a smooth point too. This contradicts our assumption. We complete the proof of the proposition. □

1C5. On the other hand, pointed semistable coverings are not finite morphisms in general.

Definition 1.8. Let $f : \mathscr{Y} \to \mathscr{X}$ be a pointed semistable covering over S. A closed point $x \in \mathscr{X}$ is called a *vertical point associated to* f, or for simplicity, a *vertical point* when there is no fear of confusion, if $f^{-1}(x)$ is not a finite set. The inverse image $f^{-1}(x)$ is called the *vertical fiber associated to* f *and* x.

Remark 1.8.1. We maintain the notation introduced above. Then the specialization homomorphism of admissible fundamental groups of generic fiber and special fiber of $\mathscr{X}$ is not an isomorphism in general. When $\operatorname{char}(K) = 0$, this result follows from $\sigma(\mathscr{X}_s) \leq g_X$, where g_X denotes the genus of $\mathscr{X}$. On the other hand, when $\operatorname{char}(K) = p > 0$, this result is highly nontrivial [Tamagawa 2004a, Theorem 0.3; Yang 2020, Theorem 5.2 and Remark 5.2.1]. Then we may ask the following problem:

> By replacing S by a finite extension of S, does there exist a pointed semistable covering $f : \mathscr{Y} \to \mathscr{X}$ over S such that the set of vertical points associated to f is not empty?

Suppose $\operatorname{char}(K) = 0$. The problem was solved by A. Tamagawa [2004b, Theorem 0.2]. In fact, Tamagawa proved a very strong result as following:

> Suppose that $\operatorname{char}(K) = 0$, that k is an algebraic closure of a finite field, and that $\mathscr{X}$ is a pointed *stable* curve over S. Let $x \in \mathscr{X}$ be a closed point of $\mathscr{X}$. Then there exists a pointed stable covering $f : \mathscr{Y} \to \mathscr{X}$ over S such that x is a vertical point associated to f.

Moreover, the author generalized this result to the case where k is an arbitrary algebraically closed field [Yang 2019, Theorem 3.2]. On the other hand, suppose that $\operatorname{char}(K) = p > 0$. The problem was solved by the author when $\mathscr{X}_s$ is irreducible [Yang 2019, Theorem 0.2].

1C6. For the p-rank of vertical fibers of pointed semistable coverings, we have the following famous result proved by Raynaud, which is the main theorem of [Raynaud 1990].

Theorem 1.9 [Raynaud 1990, Théorème 2]. *Let G be a finite p-group, $f : \mathscr{Y} \to \mathscr{X}$ a G-pointed semistable covering over S, and x a vertical point associated to f. If x is a* ***nonmarked smooth*** *point of $\mathscr{X}_s$ (i.e., $x \notin X^{\mathrm{sing}} \cup D_{X_s}$), then we have $\sigma(f^{-1}(x)) = 0$.*

1C7. In the remainder of the present paper, we will generalize Theorem 1.9 to the case where x is an *arbitrary* (possibly singular) closed point of $\mathscr{X}$. Namely, we will give an explicit formula for p-rank of vertical fibers associated to arbitrary vertical points of G-pointed semistable coverings, where G is a finite p-group.

1D. ***Inertia subgroups and a criterion for vertical fibers.*** In this subsection, we study the relationship between the inertia subgroups of nodes and the inertia subgroups of irreducible components of special fibers of G-pointed semistable coverings. The main result of the present subsection is Proposition 1.12.

1D1. *Settings.* We maintain the settings introduced in Section 1C1.

1D2. Firstly, we have the following lemmas.

Lemma 1.10. *Let G be a finite group, $f : \mathscr{Y} = (Y, D_Y) \to \mathscr{X}$ a* ***finite*** *G-pointed semistable covering over S, $\mathscr{Y}_s = (Y_s, D_{Y_s})$ the special fiber of $\mathscr{Y}$, and $y \in \mathscr{Y}_s$ a node. Let Y_1 and Y_2 (which may be equal) be the irreducible components of $\mathscr{Y}_s$ containing y. Write $I_y \subseteq G$ (resp. $I_{Y_1} \subseteq G$, $I_{Y_2} \subseteq G$) for the inertia subgroup of y (resp. Y_1, Y_2). Suppose that G is a p-group. Then the inertia subgroup I_y is generated by I_{Y_1} and I_{Y_2}.*

Proof. Write I for the group generated by I_{Y_1} and I_{Y_2}. Then we have $I \subseteq I_y$. Consider the quotient $\mathscr{Y}/I$. We obtain morphisms of pointed semistable curves $\mu_1 : \mathscr{Y} \to \mathscr{Y}/I$ and $\mu_2 : \mathscr{Y}/I \to \mathscr{X}$ over S such that $\mu_2 \circ \mu_1 = f$. Note that $\mathscr{Y}/I$ is a pointed semistable curve over S [Raynaud 1990, Appendice, Corollaire], and that $\mu_1(y)$ is a node of the special fiber $(\mathscr{Y}/I)_s$ of $\mathscr{Y}/I$ (Proposition 1.7). Moreover, μ_2 is generically étale at the generic points of $\mu_1(Y_1)$ and $\mu_1(Y_2)$. Then by applying the well-known result concerning the structures of étale fundamental groups of nodes of pointed stable curves, e.g., [Tamagawa 2004b, Lemma 2.1(iii)], to the local morphism $\operatorname{Spec} \mathcal{O}_{\mathscr{Y}/I,\mu_1(y)} \to \operatorname{Spec} \mathcal{O}_{\mathscr{X},f(y)}$ induced by μ_2, we obtain that μ_2 is tamely ramified at $\mu_1(y)$. Moreover, since G is a p-group, μ_2 is étale at $\mu_1(y)$. This means $I_y \subseteq I$. Namely, we have $I_y = I$. We complete the proof of the lemma. □

Lemma 1.11 [Tamagawa 2004b, Propoisiton 4.3(ii)]. *Let G be a finite group, $f : \mathscr{Y} \to \mathscr{X}$ a G-pointed semistable covering over S, and x a node of $\mathscr{X}_s$. Suppose that, for each irreducible component $Z \overset{\text{def}}{=} \overline{\{z\}}$ of $\operatorname{Spec} \widehat{\mathcal{O}}_{\mathscr{X}_s,x}$ and each point w of the fiber $\mathscr{Y} \times_{\mathscr{X}} z$, the natural morphism from the integral closure W^s of Z in $k(w)^s$ to Z is wildly ramified, where $k(w)^s$ denotes the maximal separable subextension of $k(z)$ in $k(w)$. Then x is a vertical point associated to f (i.e., $f^{-1}(x)$ is not finite).*

Remark 1.11.1. Tamagawa [2004b] only treated the case where f is a stable covering. It is easy to see that Tamagawa's proof also holds for pointed semistable coverings.

1D3. Next, we prove a criterion for existence of vertical fibers over nodes as follows:

Proposition 1.12. *Let G be a finite group, $f : \mathscr{Y} = (Y, D_Y) \to \mathscr{X}$ a G-pointed semistable covering over S, $\mathscr{Y}_\eta = (Y_\eta, D_{Y_\eta})$ the generic fiber of $\mathscr{Y}$ over η, $\mathscr{Y}_s = (Y_s, D_{Y_s})$ the special fiber of $\mathscr{Y}$ over s, and x a node of $\mathscr{X}_s$. Write $\psi_2 : \mathscr{Y}' \to \mathscr{X}$ for the normalization morphism of $\mathscr{X}$ in the function field $K(Y)$ induced by the natural injection $K(X) \hookrightarrow K(Y)$ induced by f. We obtain a natural morphism of fiber surfaces $\psi_1 : \mathscr{Y} \to \mathscr{Y}'$ induced by f such that $\psi_2 \circ \psi_1 = f$. Write X_1 and X_2 (which may be equal) for the irreducible components of $\mathscr{X}_s$ containing x. Let $y' \in \psi_2^{-1}(x)_{\text{red}}$, and let Y_1 and Y_2 be the irreducible components of $\mathscr{Y}_s$ such that $y' \in \psi_1(Y_1) \cap \psi_1(Y_2)$. Write $I_{Y_1} \subseteq G$ and $I_{Y_2} \subseteq G$ for the inertia subgroups of Y_1 and Y_2, respectively. Suppose that neither $I_{Y_1} \subseteq I_{Y_2}$ nor $I_{Y_1} \supseteq I_{Y_2}$ holds. Then x is a vertical point associated to f (i.e., $f^{-1}(x)$ is not finite).*

Proof. To verify the proposition, we may assume that x is not a vertical point associated to f. Then $f^{-1}(x)$ is a finite set. Let $a \in \psi_2^{-1}(x)$ and $b \in \psi_1^{-1}(a)$. Thus, ψ_1 induces an isomorphism $\operatorname{Spec} \mathcal{O}_{\mathscr{Y},b} \to \operatorname{Spec} \mathcal{O}_{\mathscr{Y}',a}$. Write y for $\psi_1^{-1}(y')_{\mathrm{red}}$. By replacing $\mathscr{X}$ by the quotient $\mathscr{Y}/D_y$ and G by $D_y \subseteq G$, respectively, where $D_y \subseteq G$ denotes the decomposition group of y, we may assume $f^{-1}(x)_{\mathrm{red}} = \{y\} \subseteq Y_1 \cap Y_2$.

Consider the quotient curve $\mathscr{Y}/I_{Y_1}$ (resp. $\mathscr{Y}/I_{Y_2}$) over S. Note that $\mathscr{Y}/I_{Y_1}$ (resp. $\mathscr{Y}/I_{Y_2}$) is a pointed semistable curve over S. We obtain the following morphisms of pointed semistable curves

$$\lambda_1 : \mathscr{Y} \to \mathscr{Y}/I_{Y_1} \quad (\text{resp. } \lambda_2 : \mathscr{Y} \to \mathscr{Y}/I_{Y_2}),$$
$$\mu_1 : \mathscr{Y}/I_{Y_1} \to \mathscr{X} \quad (\text{resp. } \mu_2 : \mathscr{Y}/I_{Y_2} \to \mathscr{X})$$

over S such that $\mu_1 \circ \lambda_1 = f$ (resp. $\mu_2 \circ \lambda_2 = f$). Note that μ_1 (resp. μ_2) is étale at the generic point of $\lambda_1(Y_1)$ (resp. $\lambda_2(Y_2)$) of degree $\#G/\#I_{Y_1}$ (resp. $\#G/\#I_{Y_2}$).

If μ_1 (resp. μ_2) is also generically étale at the generic point of $\lambda_1(Y_2)$ (resp. $\lambda_2(Y_1)$), then, by applying [Tamagawa 2004b, Lemma 2.1(iii)] to

$$\operatorname{Spec} \widehat{\mathcal{O}}_{\mathscr{Y}/I_{Y_1},\lambda_1(y)} \to \operatorname{Spec} \widehat{\mathcal{O}}_{\mathscr{X},x} \quad (\text{resp. } \operatorname{Spec} \widehat{\mathcal{O}}_{\mathscr{Y}/I_{Y_2},\lambda_2(y)} \to \operatorname{Spec} \widehat{\mathcal{O}}_{\mathscr{X},x}),$$

we obtain that $\operatorname{Spec} \widehat{\mathcal{O}}_{\lambda_1(Y_1),\lambda_1(y)} \to \operatorname{Spec} \widehat{\mathcal{O}}_{X_1,x}$ (resp. $\operatorname{Spec} \widehat{\mathcal{O}}_{\lambda_2(Y_2),\lambda_2(y)} \to \operatorname{Spec} \widehat{\mathcal{O}}_{X_2,x}$) induced by μ_1 (resp. μ_2) is tamely ramified with ramification index t_1 (resp. t_2). Thus, we have $(t_1, p) = 1$ (resp. $(t_2, p) = 1$). On the other hand, since I_{Y_1} (resp. I_{Y_2}) does not contain I_{Y_2} (resp. I_{Y_1}), and I_{Y_2} (resp. I_{Y_1}) is a p-group, we have $p \mid t_1$ (resp. $p \mid t_2$). This is a contradiction. Thus, μ_1 (resp. μ_2) is not generically étale at the generic point of $\lambda_1(Y_2)$ (resp. $\lambda_2(Y_1)$). Thus, the morphism $\operatorname{Spec} \widehat{\mathcal{O}}_{\lambda_1(Y_1),\lambda_1(y)} \to \operatorname{Spec} \widehat{\mathcal{O}}_{X_1,x}$ (resp. $\operatorname{Spec} \widehat{\mathcal{O}}_{\lambda_2(Y_2),\lambda_2(y)} \to \operatorname{Spec} \widehat{\mathcal{O}}_{X_2,x}$) induced by μ_1 (resp. μ_2) is wildly ramified. Lemma 1.11 implies that x is a vertical point associated to f. This contradicts our assumptions. We complete the proof of the proposition. □

The following corollary follows immediately from Lemma 1.10 and Proposition 1.12.

Corollary 1.13. *Let G be a finite group, $f : \mathscr{Y} = (Y, D_Y) \to \mathscr{X}$ a G-pointed semistable covering over S, $\mathscr{Y}_s = (Y_s, D_{Y_s})$ the special fiber of $\mathscr{Y}$, and $y \in \mathscr{Y}_s$ a node. Let Y_1 and Y_2 (which may be equal) be the irreducible components of $\mathscr{Y}_s$ containing y. Write $I_y \subseteq G$ (resp. $I_{Y_1} \subseteq G$, $I_{Y_2} \subseteq G$) for the inertia subgroup of y (resp. Y_1, Y_2). Suppose that f is a **finite** morphism. Then either $I_{Y_1} \subseteq I_{Y_2}$ or $I_{Y_1} \supseteq I_{Y_2}$ holds. Moreover, if G is a p-group, then the inertia subgroup I_y is equal to either I_{Y_1} or I_{Y_2}.*

2. Semigraphs with p-rank

In this section, we develop the theory of semigraphs with p-rank. The main result of the present section is Theorem 2.7.

2A. *Semigraphs with p-rank and their coverings.*

2A1. We define semigraphs with p-rank as follows:

Definition 2.1. Let $\mathbb{G}$ be a semigraph (Section 1A1) and $\sigma_{\mathfrak{G}} : v(\mathbb{G}) \to \mathbb{Z}$ a map. We shall call the pair $\mathfrak{G} \overset{\text{def}}{=} (\mathbb{G}, \sigma_{\mathfrak{G}})$ a *semigraph with p-rank*. Moreover, we call that the semigraph $\mathbb{G}$ is the underlying semigraph of $\mathfrak{G}$, and that the map $\sigma_{\mathfrak{G}}$ is the p-rank map of $\mathfrak{G}$. We define the *p-rank* $\sigma(\mathfrak{G})$ of $\mathfrak{G}$ to be

$$\sigma(\mathfrak{G}) \overset{\text{def}}{=} \sum_{v \in v(\mathbb{G})} \sigma_{\mathfrak{G}}(v) + \gamma_{\mathbb{G}}.$$

A *morphism* of semigraphs with p-rank $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ is defined by a morphism of the underlying semigraphs $\beta : \mathbb{G}^1 \to \mathbb{G}^2$. We shall refer to the morphism β as the underlying morphism of $\mathfrak{b}$.

A semigraph with p-rank is called connected if the underlying semigraph $\mathbb{G}$ is a connected semigraph.

Remark 2.1.1. We explain the geometric motivation of the above definitions. Let $\mathscr{X} \overset{\text{def}}{=} (X, D_X)$ be a pointed semistable curve over an algebraically closed field of characteristic $p > 0$. Write $\Gamma_{\mathscr{X}}$ for the dual semigraph (Section 1B2) of $\mathscr{X}$ and we define $\sigma_{\Gamma_{\mathscr{X}}}(v)$, $v \in v(\Gamma_{\mathscr{X}})$, to be the p-rank (Section 1B3) of the normalization of the irreducible component X_v corresponding to v. Then $(\Gamma_{\mathscr{X}}, \sigma_{\Gamma_{\mathscr{X}}})$ is a semigraph with p-rank. On the other hand, a semigraph with p-rank $\mathfrak{G} \overset{\text{def}}{=} (\mathbb{G}, \sigma_{\mathfrak{G}})$ is not arose from a pointed semistable curve in positive characteristic in general since $\sigma_{\mathfrak{G}}$ can attain *negative* integers.

2A2. *Settings.* Let G be a finite p-group of order p^r.

2A3. Let $\mathfrak{b} : \mathfrak{G}^1 \overset{\text{def}}{=} (\mathbb{G}^1, \sigma_{\mathfrak{G}^1}) \to \mathfrak{G}^2 \overset{\text{def}}{=} (\mathbb{G}^2, \sigma_{\mathfrak{G}^2})$ be a morphism of semigraphs with p-rank and $\beta : \mathbb{G}^1 \to \mathbb{G}^2$ the underlying morphism of $\mathfrak{b}$.

Definition 2.2. (a) We shall call that $\mathfrak{b}$ is *p-étale* (resp. *purely inseparable*) at an edge $e \in e(\mathbb{G}^1)$ if $\#\beta^{-1}(\beta(e)) = p$ (resp. $\#\beta^{-1}(\beta(e)) = 1$). We shall call that $\mathfrak{b}$ is *p-generically étale* at $v \in v(\mathbb{G}^1)$ if one of the following conditions holds (see Section 1A1 for $e(v)$):

(Type-I) $\#\beta^{-1}(\beta(v)) = p$ and $\sigma_{\mathfrak{G}^1}(v) = \sigma_{\mathfrak{G}^2}(\beta(v))$.

(Type-II) $\#\beta^{-1}(\beta(v)) = 1$ and

$$\sigma_{\mathfrak{G}^1}(v) - 1 = p(\sigma_{\mathfrak{G}^2}(\beta(v)) - 1) + \sum_{e \in e(v)} \left(\frac{p}{\#\beta^{-1}(\beta(e))} - 1 \right).$$

(b) We shall call that $\mathfrak{b}$ is *purely inseparable* at $v \in v(\mathbb{G}^1)$ if $\#\beta^{-1}(\beta(v)) = 1$, $\mathfrak{b}$ is purely inseparable at each element of $e(v)$, and $\sigma_{\mathfrak{G}^1}(v) = \sigma_{\mathfrak{G}^2}(\beta(v))$.

(c) We shall call that $\mathfrak{b}$ is a *p-covering* if the following conditions hold (see Section 1A1 for $v(e)$):

(i) There exists a $\mathbb{Z}/p\mathbb{Z}$-action (which may be trivial) on $\mathbb{G}^1$ and a trivial $\mathbb{Z}/p\mathbb{Z}$-action on $\mathbb{G}^2$ such that the underlying morphism β of $\mathfrak{b}$ is compatible with the $\mathbb{Z}/p\mathbb{Z}$-actions.

(ii) The natural morphism $\mathbb{G}^1/(\mathbb{Z}/p\mathbb{Z}) \to \mathbb{G}^2$ induced by β is an isomorphism, where $\mathbb{G}^1/(\mathbb{Z}/p\mathbb{Z})$ denotes the quotient semigraph.

(iii) For each $v \in v(\mathbb{G}^1)$, $\mathfrak{b}$ is either p-generically étale or purely inseparable at v.

(iv) Let $e \in e^{\mathrm{cl}}(\mathbb{G}^1)$ and $v(e) = \{v, v'\}$ (note that $v = v'$ if and only if e is a loop (Section 1A1)). Suppose that $\mathfrak{b}$ is p-generically étale at v and v'. Then $\mathfrak{b}$ is p-étale at e.

(v) For each $v \in v(\mathbb{G}^1)$, then $\sigma_{\mathfrak{G}^1}(v) = \sigma_{\mathfrak{G}^1}(\tau(v))$ for each $\tau \in \mathbb{Z}/p\mathbb{Z}$.

Note that the definition of p-coverings implies that the identity morphism of a semigraph with p-rank is a p-covering.

(d) We shall call that $\mathfrak{b}$ is a *covering* if $\mathfrak{b}$ is a composite of p-coverings.

(e) We maintain the notation introduced in Section 2A2. We shall call

$$\Phi : \{1\} = G_r \subset G_{r-1} \subset \cdots \subset G_1 \subset G_0 = G$$

a *maximal normal filtration* of G if G_j is a normal subgroup of G and $G_j/G_{j+1} \cong \mathbb{Z}/p\mathbb{Z}$ for $j \in \{0, \ldots, r-1\}$. Note that since G is a p-group, a maximal normal filtration of G exists.

Suppose that $\mathbb{G}^1$ admits a G-action (which may be trivial), that $\mathbb{G}^2$ admits a trivial G-action, and that the underlying morphism β of $\mathfrak{b}$ is compatible with the G-actions. A maximal normal filtration Φ of G induces a sequence of semigraphs:

$$\mathbb{G}^1 = \mathbb{G}_r \xrightarrow{\beta_r} \mathbb{G}_{r-1} \xrightarrow{\beta_{r-1}} \cdots \xrightarrow{\beta_1} \mathbb{G}_0,$$

where $\mathbb{G}_j$, $j \in \{0, \ldots, r\}$, denotes the quotient semigraph $\mathbb{G}^1/G_j$. We shall call that $\mathfrak{b}$ is a *G-covering* if there exist a maximal normal filtration Φ of G and a set of p-coverings $\{\mathfrak{b}_j : \mathfrak{G}_j \to \mathfrak{G}_{j-1},\ j = 1, \ldots, r\}$ such that the following conditions are satisfied:

(i) The underlying semigraph of $\mathfrak{G}_j$ is equal to $\mathbb{G}_j$ for $j \in \{0, \ldots, r\}$ such that $\mathbb{G}_0 = \mathbb{G}^2$.

(ii) The underlying morphism of $\mathfrak{b}_j$ is equal to β_j for $j \in \{1, \ldots, r\}$.

(iii) The composite morphism $\mathfrak{b}_1 \circ \cdots \circ \mathfrak{b}_r$ is equal to $\mathfrak{b}$.

(f) Let $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ be a G-covering. By the above definition of G-coverings, we obtain a maximal normal filtration Φ of G and a sequence of p-coverings:

$$\Phi_{\mathfrak{G}^1/\mathfrak{G}^2} : \mathfrak{G}^1 = \mathfrak{G}_r \xrightarrow{\mathfrak{b}_r} \mathfrak{G}_{r-1} \xrightarrow{\mathfrak{b}_{r-1}} \cdots \xrightarrow{\mathfrak{b}_1} \mathfrak{G}_0 = \mathfrak{G}^2.$$

We shall call $\Phi_{\mathfrak{G}^1/\mathfrak{G}^2}$ *a sequence of p-coverings induced by* Φ.

Remark 2.2.1. We explain the geometric motivation of the above definitions. Let R be a discrete valuation ring with algebraically closed residue field of characteristic $p > 0$, and let $f : \mathscr{Y} \overset{\mathrm{def}}{=} (Y, D_Y) \to \mathscr{X} \overset{\mathrm{def}}{=} (X, D_X)$ be a *finite* G-pointed semistable covering over R (Definition 1.5). Write $(\Gamma_{\mathscr{Y}_s}, \sigma_{\Gamma_{\mathscr{Y}_s}})$ and $(\Gamma_{\mathscr{X}_s}, \sigma_{\Gamma_{\mathscr{X}_s}})$ for the semigraphs with p-rank associated to the special fibers $\mathscr{Y}_s$ and $\mathcal{X}_s$ of $\mathscr{Y}$ and $\mathscr{X}$ (see Remark 2.1.1), respectively. Then the morphism of special fibers induced by f induces a G-covering $(\Gamma_{\mathscr{Y}_s}, \sigma_{\Gamma_{\mathscr{Y}_s}}) \to (\Gamma_{\mathscr{X}_s}, \sigma_{\Gamma_{\mathscr{X}_s}})$ (see Section 3A).

On the other hand, the definitions of p-étale, purely inseparable, p-generically étale, purely inseparable, and p-coverings of semigraphs with p-rank are motivated by p-étale, purely inseparable, p-generically étale, purely inseparable, and p-coverings of special fibers of finite $\mathbb{Z}/p\mathbb{Z}$-pointed semistable coverings over R. In particular, Definition 2.2(a-Type-II) is motivated by the Deuring-Shafarevich formula (see Proposition 1.4), and Definition 2.2(c-iv) is motivated by the Zariski–Nagata purity theorem of finite $\mathbb{Z}/p\mathbb{Z}$-pointed semistable coverings over R.

2A4. Let $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ be a G-covering, $\beta : \mathbb{G}^1 \to \mathbb{G}^2$ the underlying morphism of $\mathfrak{b}$, $v^1 \in v(\mathbb{G}^1)$, and $e^1 \in e(\mathbb{G}^1)$. By the definition of G-coverings, we have a maximal normal filtration Φ of G and a sequence of p-coverings induced by Φ:

$$\Phi_{\mathfrak{G}^1/\mathfrak{G}^2} : \mathfrak{G}^1 = \mathfrak{G}_r \xrightarrow{\mathfrak{b}_r} \mathfrak{G}_{r-1} \xrightarrow{\mathfrak{b}_{r-1}} \cdots \xrightarrow{\mathfrak{b}_1} \mathfrak{G}_0 = \mathfrak{G}^2.$$

Write $\beta_j : \mathbb{G}_j \to \mathbb{G}_{j-1}$, $j \in \{1, \dots, r\}$, for the underlying morphism of $\mathfrak{b}_j$. Write v_j (resp. e_j) for the image $\beta_{j+1} \circ \cdots \circ \beta_r(v^1)$ (resp. $\beta_{j+1} \circ \cdots \circ \beta_r(e^1)$), $j \in \{0, \dots, r-1\}$, and v_r for v^1. We put

$$\#I_{v^1} = p^{\#\{j \in \{1,\dots,r\} \mid \mathfrak{b}_j \text{ is purely inseparable at } v_j\}} \quad \text{and} \quad \#I_{e^1} = p^{\#\{j \in \{1,\dots,r\} \mid \mathfrak{b}_j \text{ is purely inseparable at } e_j\}}.$$

Note that $\#I_{v^1}$ and $\#I_{e^1}$ do not depend on the choice of Φ. Moreover, we put $D_{v^1} \overset{\text{def}}{=} \{\tau \in G \mid \tau(v^1) = v^1\}$, and

$$\#D_{v^1}$$

the cardinality of D_{v^1}.

2A5. We maintain the notation introduced in Section 2A4. If $e^1 \in e(v^1)$, then we have $\#I_{v^1} \mid \#I_{e^1}$. In particular, if e^1 is a loop, then Definition 2.2(c-iv) implies that $\#I_{v^1} = \#I_{e^1}$. Moreover, Definition 2.2 (c-iv) also implies that $\#I_{e^1} \mid \#D_{v^1}$. Write v^2 (resp. e^2) for $\beta(v^1)$ (resp. $\beta(e^1)$). Let $(v^1)'$ (resp. $(e^1)'$) be an arbitrary element of $\beta^{-1}(v^2)$ (resp. $\beta^{-1}(e^2)$). By the action of G on $\mathbb{G}^1$, we have $\#I_{v^1} = \#I_{(v^1)'}$, $\#I_{e^1} = \#I_{(e^1)'}$, and $\#D_{v^1} = \#D_{(v^1)'}$. Thus, we may use the notation $\#I_{v^2}$ (resp. $\#I_{e^2}$, $\#D_{v^2}$) to denote $\#I_{v^1}$ (resp. $\#I_{e^1}$, $\#D_{v^1}$). Namely, $\#I_{v^1}$ (resp. $\#I_{e^1}$, $\#D_{v^1}$) does not depend on the choice of $v^1 \in \beta^{-1}(\beta(v^1))$. Then we have $\#I_{v^2} \mid \#I_{e^2} \mid \#D_{v^2}$.

2A6. We maintain the notation introduced in Sections 2A4 and 2A5. One may compute the p-rank $\sigma_{\mathfrak{G}^1}(v^1)$ by using Definition 2.2(a). Then we have the following Deuring–Shafarevich type formula for the p-rank of G-coverings (see Proposition 1.4 for the Deuring–Shafarevich formula for curves)

$$\begin{aligned}\sigma_{\mathfrak{G}^1}(v^1) - 1 &= (\#D_{v^2}/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e^2 \in e(v^2)} (\#D_{v^2}/\#I_{e^2})(\#I_{e^2}/\#I_{v^2} - 1) \\ &= (\#D_{v^2}/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e^2 \in e(v^2) \setminus e^{\mathrm{lp}}(v^2)} (\#D_{v^2}/\#I_{e^2})(\#I_{e^2}/\#I_{v^2} - 1).\end{aligned}$$

Here, the second equality follows from Definition 2.2(c-iv).

2B. ***An operator concerning coverings.*** In this subsection, we introduce an operator (or a deformation) concerning coverings of semigraphs with p-rank which is a key in our computations of p-rank.

2B1. *Settings.* We fix some notation. Let G be a finite p-group of order p^r, and let $\mathfrak{b} : \mathfrak{G}^1 \overset{\text{def}}{=} (\mathbb{G}^1, \sigma_{\mathfrak{G}^1}) \to \mathfrak{G}^2 \overset{\text{def}}{=} (\mathbb{G}^2, \sigma_{\mathfrak{G}^2})$ be a covering of semigraphs with p-rank (Definition 2.2(d)) and $\beta : \mathbb{G}^1 \to \mathbb{G}^2$ the underlying morphism of $\mathfrak{b}$ (Definition 2.1). We put

$$V^1 \overset{\text{def}}{=} \{v \in v(\mathbb{G}^1) \mid \#\beta^{-1}(\beta(v^1)) = 1\} \subseteq v(\mathbb{G}^1) \quad \text{and} \quad V^2 \overset{\text{def}}{=} \beta(V^1) \subseteq v(\mathbb{G}^2).$$

Moreover, we suppose that $\mathbb{G}^1$, $\mathbb{G}^2$ are *connected*, that $\mathbb{G}^1$ (resp. $\mathbb{G}^2$) admits an action (resp. a trivial action) of G such that β is a G-equivariant, and that $\mathbb{G}^1/G = \mathbb{G}^2$.

2B2. Let $v^2 \in v(\mathbb{G}^2)$ and $v^1 \in \beta^{-1}(v^2)$. Firstly, we define a new semigraph $\mathbb{G}^1_{v^2}$ associated to v^2 as follows (see Example 2.3 below):

(a) Suppose $v^2 \in V^2$. We put $\mathbb{G}^1_{v^2} \overset{\text{def}}{=} \mathbb{G}^1$.

(b) Suppose $v^2 \notin V^2$. We have the following:

(i) $v(\mathbb{G}^1_{v^2}) \overset{\text{def}}{=} (v(\mathbb{G}^1) \setminus \beta^{-1}(v^2)) \sqcup \{v^2_\star\}$, $e^{\text{cl}}(\mathbb{G}^1_{v^2}) \overset{\text{def}}{=} e^{\text{cl}}(\mathbb{G}^1)$, and $e^{\text{op}}(\mathbb{G}^1_{v^2}) \overset{\text{def}}{=} e^{\text{op}}(\mathbb{G}^1)$, where $v^2_\star$ is a new vertex and $\sqcup$ means disjoint union.

(ii) The collection of maps $\{\zeta_e^{\mathbb{G}^1_{v^2}}\}_e$ is as follows:

(1) For each $e \in e^{\text{op}}(\mathbb{G}^1_{v^2}) \overset{\text{def}}{=} e^{\text{op}}(\mathbb{G}^1)$ and $b \in e$ (i.e., a branch of e, see Section 1A1), we put

$$\zeta_e^{\mathbb{G}^1_{v^2}}(b) = \begin{cases} \{v(\mathbb{G}^1_{v^2})\} & \text{if } \zeta_e^{\mathbb{G}^1}(b) = \{v(\mathbb{G}^1)\}, \\ v^2_\star & \text{if } \zeta_e^{\mathbb{G}^1}(b) \in \beta^{-1}(v^2), \\ \zeta_e^{\mathbb{G}^1}(b) & \text{otherwise.} \end{cases}$$

(2) For each $e \in e^{\text{cl}}(\mathbb{G}^1_{v^2}) \overset{\text{def}}{=} e^{\text{cl}}(\mathbb{G}^1)$ and $b \in e$, we put

$$\zeta_e^{\mathbb{G}^1_{v^2}}(b) = \begin{cases} v^2_\star & \text{if } \zeta_e^{\mathbb{G}^1}(b) \in \beta^{-1}(v^2), \\ \zeta_e^{\mathbb{G}^1}(b) & \text{otherwise.} \end{cases}$$

Next, we define a morphism of semigraphs $\beta_{v^2} : \mathbb{G}^1_{v^2} \to \mathbb{G}^2$ as follows (see Example 2.3 below):

(i) For each $v \in v(\mathbb{G}^1_{v^2})$, we put

$$\beta_{v^2}(v) = \begin{cases} v^2 & \text{if } v = v^2_\star, \\ \beta(v) & \text{otherwise.} \end{cases}$$

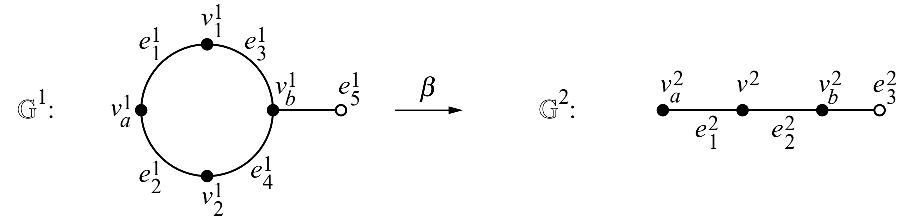
(ii) For each $e \in e(\mathbb{G}^1_{v^2}) = e^{\text{cl}}(\mathbb{G}^1_{v^2}) \cup e^{\text{op}}(\mathbb{G}^1_{v^2})$, we put $\beta_{v^2}(e) \overset{\text{def}}{=} \beta(e)$.

Example 2.3. We give an example to explain the above constructions. We use the notation "•" and "∘ with a line segment" to denote a vertex and an open edge, respectively.

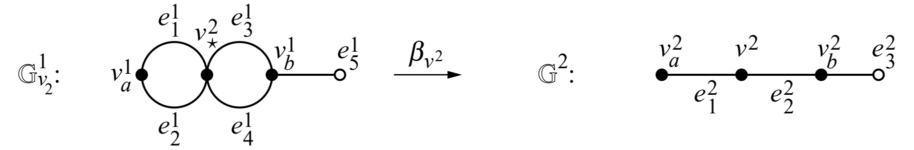
Let $p = 2$, and let $\mathbb{G}^1$, $\mathbb{G}^2$ be the semigraphs below. Moreover, let $\beta : \mathbb{G}^1 \to \mathbb{G}^2$ be a morphism of semigraphs such that

$$\beta(v^1_a) = v^2_a, \quad \beta(v^1_b) = v^2_b, \quad \beta(v^1_1) = \beta(v^1_2) = v^2, \quad \beta(e^1_1) = \beta(e^1_2) = e^2_1, \quad \beta(e^1_3) = \beta(e^1_4) = e^2_2, \quad \beta(e^1_5) = e^2_3.$$

Note that $\mathbb{G}^1$ admits an action of $\mathbb{Z}/2\mathbb{Z}$ such that $\mathbb{G}^1/(\mathbb{Z}/p\mathbb{Z}) = \mathbb{G}^2$. Then we have the following:



By the definitions of $\mathbb{G}^1_{v^2}$ and β_{v^2}, we have the following:



2B3. We maintain the notation introduced in Section 2B2. Next, we define a p-rank map $\sigma_{\mathfrak{G}^1_{v^2}} : v(\mathbb{G}^1_{v^2}) \to \mathbb{Z}$ for $\mathbb{G}^1_{v^2}$ as follows:

(a) Suppose $v^2 \in V^2$. We put $\sigma_{\mathfrak{G}^1_{v^2}} \overset{\text{def}}{=} \sigma_{\mathfrak{G}^1}$.

(b) Suppose $v^2 \notin V^2$. Let $v \in v(\mathbb{G}^1_{v^2})$. We have the following:

(i) If $v \neq v^2_\star$, we put $\sigma_{\mathfrak{G}^1_{v^2}}(v) \overset{\text{def}}{=} \sigma_{\mathfrak{G}^1}(v)$.

(ii) If $v = v^2_\star$, we put (see Section 1A1 for $e(v^2)$ and Section 2A6 for $\#I_{v^2}$, $\#I_e$)

$$\sigma_{\mathfrak{G}^1_{v^2}}(v^2_\star) \overset{\text{def}}{=} (\#G/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e \in e(v^2)} (\#G/\#I_e)(\#I_e/\#I_{v^2} - 1) + 1.$$

2B4. We maintain the notation introduced in Sections 2B2 and 2B3. Let $v^2 \in v(\mathbb{G}^2)$. We define a semigraph with p-rank and a morphism of semigraphs with p-rank associated to $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ and v^2, respectively, to be

$$\mathfrak{G}^1_{v^2} \overset{\text{def}}{=} (\mathbb{G}^1_{v^2}, \sigma_{\mathfrak{G}^1_{v^2}}), \quad \mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2,$$

where the underlying morphism of $\mathfrak{b}_{v^2}$ is β_{v^2}.

2B5. We maintain the settings introduced in Section 2B1. Let $\mathfrak{G}^i \setminus \{V^i\}$, $i \in \{1, 2\}$, be the (possibly nonconnected) semigraph with p-rank whose underlying semigraph is $\mathbb{G}^i \setminus \{V^i\}$ (in the sense of Section 1A2(b)), and whose p-rank map is $\sigma_{\mathfrak{G}^i}|_{v(\mathbb{G}^i \setminus \{V^i\})}$. We shall call $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ a *quasi-G-covering* if the covering $\mathfrak{G}^1 \setminus \{V^1\} \to \mathfrak{G}^2 \setminus \{V^2\}$ induced by $\mathfrak{b}$ is a G-covering.

Definition 2.4. Let $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ be a quasi-G-covering of connected semigraphs with p-rank and $v^2 \in v(\mathbb{G}^2)$. We define an operator $\rightleftharpoons^{\mathrm{I}}_{\mathrm{II}} [v^2]$ on $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ to be

$$\rightleftharpoons^{\mathrm{I}}_{\mathrm{II}} [v^2](\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2) \overset{\text{def}}{=} \mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2.$$

Here $\rightleftharpoons^{\mathrm{I}}_{\mathrm{II}}$ means that "from (Type-I) to (Type-II)" in the sense of Definition 2.2(a).

Remark 2.4.1. Suppose that $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ is a G-covering of semigraphs with p-rank. Then $\sigma_{\mathfrak{G}^1_{v^2}}(v^2_\star)$ is not contained in $\mathbb{Z}_{\geq 0}$ in general. Thus, $\mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2$ cannot be arose from a G-pointed semistable covering in general (see also Remark 2.2.1). On the other hand, in the next subsection, we will see (Proposition 2.6 below) that the operator defined above *does not change* global p-rank (i.e., $\sigma(\mathfrak{G}^1_{v^2}) = \sigma(\mathfrak{G}^1)$).

2B6. Let $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ be a quasi-G-covering and $v^2 \in v(\mathbb{G}^2)$. Then the semigraph with p-rank $\mathbb{G}^1_{v^2}$ admits a natural G-action as follows:

(1) The action of G on $v(\mathbb{G}^1_{v^2} \setminus \{v^2_\star\}) = v(\mathbb{G}^1) \setminus \beta^{-1}(v^2)$ (resp. $e(\mathbb{G}^1_{v^2}) = e(\mathbb{G}^1)$) is the action of G on $v(\mathbb{G}^1) \setminus \beta^{-1}(v^2)$ (resp. $e(\mathbb{G}^1)$) induced by the action of G on $\mathbb{G}^1$.

(2) The action of G on $v^2_\star$ is a trivial action.

We see immediately that $\mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2$ is a quasi-G-covering.

Let $\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2$ be a G-covering. Suppose that G is an *abelian* p-group. Then together with the G-action defined above, it is easy to check that $\mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2$ is a G-covering.

On the other hand, if G is *not abelian*, then $\mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2$ is *not* a G-covering in general for the following reason. Let $w \overset{\text{def}}{=} v^2_\star = \beta^{-1}_{v^2}(v^2)$. With the action of G on $\mathfrak{G}^1_{v^2}$ defined above, if I_{v^1}, $v^1 \in \beta^{-1}(v^2)$, is not a normal subgroup of G, then the order $\#I_w$ of the inertia subgroup I_w of w is not equal to $\#I_{v^2} \overset{\text{def}}{=} \#I_{v^1}$ (Section 2A5) in general. If $\mathfrak{b}_{v^2}$ is a G-covering, we have (Section 2A6)

$$\sigma_{\mathfrak{G}^1_{v^2}}(w) = (\#G/\#I_w)(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e \in e(v^2)} (\#G/\#I_e)(\#I_e/\#I_w - 1) + 1$$

which is not equal to (Section 2B3(b-ii))

$$\#G/\#I_{v^2}(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e \in e(v^2)} \#G/\#I_e(\#I_e/\#I_{v^2} - 1) + 1$$

in general if $\#I_w \neq \#I_{v^2}$. This contradicts the definition of $\mathfrak{G}^1_{v^2}$. Thus, $\mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2$ is not a G-covering in general.

2C. *Formula for p-rank of coverings.* In this subsection, we give an explicit formula (i.e., Theorem 2.7) for the p-rank of G-coverings of semigraphs with p-rank.

2C1. *Settings.* We maintain the settings introduced in Section 2B1. Moreover, we assume that $\mathfrak{b} : \mathfrak{G}^1 \overset{\text{def}}{=} (\mathbb{G}^1, \sigma_{\mathfrak{G}^1}) \to \mathfrak{G}^2 \overset{\text{def}}{=} (\mathbb{G}^2, \sigma_{\mathfrak{G}^2})$ is a quasi-G-covering (Section 2B5).

2C2. Firstly, we have the following lemma.

Lemma 2.5. *Let $i \in \{1, \ldots, n\}$, and let $\mathbb{G}$ be a connected semigraph, $\mathbb{G}_i$ a connected subsemigraph of $\mathbb{G}$ 1A2, and $v_i \in v(\mathbb{G}_i)$ a vertex of $\mathbb{G}_i$. Suppose $\mathbb{G}_s \cap \mathbb{G}_t = \varnothing$ for each $s, t \in \{1, \ldots, n\}$ if $s \neq t$. Let $\mathbb{G}^{\mathrm{c}}$ be a semigraph defined as follows*:

(i) $v(\mathbb{G}^{\mathrm{c}}) = v(\mathbb{G}) \sqcup \{v^{\mathrm{c}}\}$, $e^{\mathrm{op}}(\mathbb{G}^{\mathrm{c}}) = e^{\mathrm{op}}(\mathbb{G})$, $e^{\mathrm{cl}}(\mathbb{G}^{\mathrm{c}}) = e^{\mathrm{cl}}(\mathbb{G}) \sqcup \{e_i^{\mathrm{c}}\}_{i \in \{1,\dots,n\}}$.

(ii) *Let $e \in e(\mathbb{G}^{\mathrm{c}}) \setminus \{e_i^{\mathrm{c}}\}_{i\in\{1,\dots,n\}} = e(\mathbb{G})$ and $b \in e$ a branch of e* (*Section 1A1*). *We put*

$$\zeta_e^{\mathbb{G}^{\mathrm{c}}}(b) = \begin{cases} \zeta_e^{\mathbb{G}}(b) & \text{if } \zeta_e^{\mathbb{G}}(b) \neq \{v(\mathbb{G})\}, \\ \{v(\mathbb{G}^{\mathrm{c}})\} & \text{if } \zeta_e^{\mathbb{G}}(b) = \{v(\mathbb{G})\}. \end{cases}$$

(iii) *Let $e_i^{\mathrm{c}} = \{b^1_{e_i^{\mathrm{c}}}, b^2_{e_i^{\mathrm{c}}}\}$. We put $\zeta^{\mathbb{G}^{\mathrm{c}}}_{e_i^{\mathrm{c}}}(b^1_{e_i^{\mathrm{c}}}) = v_i$, $\zeta^{\mathbb{G}^{\mathrm{c}}}_{e_i^{\mathrm{c}}}(b^2_{e_i^{\mathrm{c}}}) = v^{\mathrm{c}}$.*

Then we have (*see Section 1A3 for $\gamma_{\mathbb{G}}$, $\gamma_{\mathbb{G}^{\mathrm{c}}}$*)

$$\gamma_{\mathbb{G}} = \gamma_{\mathbb{G}^{\mathrm{c}}} - n + 1.$$

Proof. The lemma follows from the construction of $\mathbb{G}^{\mathrm{c}}$. □

2C3. We have the following key proposition which says that the operator introduced in Definition 2.4 does not change the p-rank of semigraphs with p-rank.

Proposition 2.6. *We maintain the settings introduced in Section 2C1. Let $v^2 \in v(\mathbb{G}^2)$ be an arbitrary vertex of $\mathbb{G}^2$ and $\rightleftharpoons^{\mathrm{I}}_{\mathrm{II}} [v^2](\mathfrak{b} : \mathfrak{G}^1 \to \mathfrak{G}^2) = \mathfrak{b}_{v^2} : \mathfrak{G}^1_{v^2} \to \mathfrak{G}^2$ (Definition 2.4). Then we have*

$$\sigma(\mathfrak{G}^1) = \sigma(\mathfrak{G}^1_{v^2}),$$

where $\sigma(\mathfrak{G}^1)$ and $\sigma(\mathfrak{G}^1_{v^2})$ are the p-rank of $\mathfrak{G}^1$ and $\mathfrak{G}^1_{v^2}$, respectively, defined in Definition 2.1.

Proof. Suppose $\#\beta^{-1}(v^2) = 1$ (i.e., $v^2 \in V^2$). Then the proposition is trivial since $\mathfrak{G}^1 = \mathfrak{G}^1_{v^2}$. Thus, we may assume $\#\beta^{-1}(v^2) \neq 1$ (i.e., $v^2 \notin V^2$).

Write β_{v^2} for the underlying morphism of $\mathfrak{b}_{v^2}$. Moreover, we put

$$W \overset{\mathrm{def}}{=} \beta^{-1}(v^2), \;\; W^* \overset{\mathrm{def}}{=} \beta^{-1}_{v^2}(v^2) = \{v^2_\star\}.$$

For simplicity, we shall write γ (resp. $\gamma_{\setminus\{v^2\}}$, γ^*, $\gamma^*_{\setminus\{v^2\}}$) for the Betti number (Section 1A3) of $\mathbb{G}^1$ (resp. $\mathbb{G}^1 \setminus W$, $\mathbb{G}^1_{v^2}$, $\mathbb{G}^1_{v^2} \setminus W^*$), where $\mathbb{G}^1 \setminus W$ and $\mathbb{G}^1_{v^2} \setminus W^*$ are semigraphs defined in Section 1A2.

Then we have

$$\sigma(\mathfrak{G}^1) = \gamma_{\setminus\{v^2\}} + \gamma - \gamma_{\setminus\{v^2\}} + \sum_{v \in v(\mathbb{G}^1 \setminus W)} \sigma_{\mathfrak{G}^1}(v) + \sum_{v \in W} \sigma_{\mathfrak{G}^1}(v),$$
$$\sigma(\mathfrak{G}^1_{v^2}) = \sigma_{\mathfrak{G}^1_{v^2}}(v^2_\star) + \gamma^*_{\setminus\{v^2\}} + \gamma^* - \gamma^*_{\setminus\{v^2\}} + \sum_{v \in v(\mathbb{G}^1_{v^2} \setminus W^*)} \sigma_{\mathfrak{G}^1_{v^2}}(v).$$

Note that the construction of $\mathfrak{G}^1_{v^2}$ (Sections 2B2, 2B3) implies

$$A \overset{\mathrm{def}}{=} \sum_{v \in v(\mathbb{G}^1 \setminus W)} \sigma_{\mathfrak{G}^1}(v) = \sum_{v \in v(\mathbb{G}^1_{v^2} \setminus W^*)} \sigma_{\mathfrak{G}^1_{v^2}}(v), \;\; B \overset{\mathrm{def}}{=} \gamma_{\setminus\{v^2\}} = \gamma^*_{\setminus\{v^2\}}.$$

We calculate $\gamma - \gamma_{\setminus\{v^2\}}$ and $\gamma^* - \gamma^*_{\setminus\{v^2\}}$. By applying Lemma 2.5, it is sufficient to treat the case where $\mathbb{G}^1 \setminus W = \mathbb{G}^1_{v^2} \setminus W^*$ is connected. Then we obtain (see Section 1A1 for $e(v^2)$, $e^{\mathrm{lp}}(v^2)$ and

Sections 2A4 and 2A5 for $\#D_{v^2}$, $\#I_{v^2}$, $\#I_e$)

$$\gamma - \gamma_{\backslash\{v^2\}} = (\#G/\#D_{v^2})\biggl(\biggl(\sum_{e\in(e(v^2)\cap e^{\mathrm{cl}}(\mathbb{G}^2))\backslash e^{\mathrm{lp}}(v^2)} \#D_{v^2}/\#I_e\biggr) - 1\biggr) + \#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2}),$$

$$\gamma^* - \gamma^*_{\backslash\{v^2\}} = \biggl(\sum_{e\in(e(v^2)\cap e^{\mathrm{cl}}(\mathbb{G}^2))\backslash e^{\mathrm{lp}}(v^2)} \#G/\#I_e\biggr) - 1 + \#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2}).$$

On the other hand, for each $v \in W \overset{\mathrm{def}}{=} \beta^{-1}(v^2)$, we have (Section 2A6)

$$\begin{aligned}\sigma_{\mathfrak{G}^1}(v) &= (\#D_{v^2}/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e\in e(v^2)} (\#D_{v^2}/\#I_e)(\#I_e/\#I_{v^2} - 1) + 1\\ &= (\#D_{v^2}/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e\in e(v^2)\backslash e^{\mathrm{lp}}(v^2)} (\#D_{v^2}/\#I_e)(\#I_e/\#I_{v^2} - 1) + 1.\end{aligned}$$

Moreover, the construction of $\mathfrak{G}^1_{v^2}$ (Section 2B3) implies that

$$\begin{aligned}\sigma_{\mathfrak{G}^1_{v^2}}(v^2_\star) &= (\#G/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e\in e(v^2)} (\#G/\#I_e)(\#I_e/\#I_{v^2} - 1) + 1\\ &= (\#G/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e\in e(v^2)\backslash e^{\mathrm{lp}}(v^2)} (\#G/\#I_e)(\#I_e/\#I_{v^2} - 1) + 1\end{aligned}$$

We obtain

$$\begin{aligned}\sigma(\mathfrak{G}^1) &= A + B + \sum_{v\in W} \sigma_{\mathfrak{G}^1}(v) + \gamma - \gamma_{\backslash\{v^2\}}\\ &= A + B + \sum_{v\in W}\biggl((\#D_{v^2}/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e\in e(v^2)\backslash e^{\mathrm{lp}}(v^2)} (\#D_{v^2}/\#I_e)(\#I_e/\#I_{v^2} - 1) + 1\biggr)\\ &\qquad + (\#G/\#D_{v^2})\biggl(\biggl(\sum_{e\in(e(v^2)\cap e^{\mathrm{cl}}(\mathbb{G}^2))\backslash e^{\mathrm{lp}}(v^2)} \#D_{v^2}/\#I_e\biggr) - 1\biggr) + \#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2})\\ &= A + B + (\#G/\#D_{v^2})\biggl((\#D_{v^2}/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2) - 1) + \sum_{e\in e(v^2)\backslash e^{\mathrm{lp}}(v^2)} (\#D_{v^2}/\#I_e)(\#I_e/\#I_{v^2} - 1) + 1\biggr)\\ &\qquad + (\#G/\#D_{v^2})\biggl(\biggl(\sum_{e\in(e(v^2)\cap e^{\mathrm{cl}}(\mathbb{G}^2))\backslash e^{\mathrm{lp}}(v^2)} \#D_{v^2}/\#I_e\biggr) - 1\biggr) + \#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2})\\ &= A + B + (\#G/\#I_{v^2})\sigma_{\mathfrak{G}^2}(v^2) - \#G/\#I_{v^2} + \sum_{e\in e(v^2)\backslash e^{\mathrm{lp}}(v^2)} \#G/\#I_{v^2} - \sum_{e\in e(v^2)\backslash e^{\mathrm{lp}}(v^2)} \#G/\#I_e\\ &\qquad\qquad + \sum_{e\in(e(v^2)\cap e^{\mathrm{cl}}(\mathbb{G}^2))\backslash e^{\mathrm{lp}}(v^2)} \#G/\#I_e + \#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2})\\ &= A + B + (\#G/\#I_{v^2})\sigma_{\mathfrak{G}^2}(v^2) - \#G/\#I_{v^2} + \sum_{e\in e(v^2)\backslash e^{\mathrm{lp}}(v^2)} \#G/\#I_{v^2}\\ &\qquad\qquad - \sum_{e\in(e(v^2)\cap e^{\mathrm{op}}(\mathbb{G}^2))\backslash e^{\mathrm{lp}}(v^2)} \#G/\#I_e + \#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2}).\end{aligned}$$

Note that the last equality holds since we have

$$e(v^2)\setminus e^{\mathrm{lp}}(v^2)=((e(v^2)\cap e^{\mathrm{op}}(\mathbb{G}^2))\setminus e^{\mathrm{lp}}(v^2))\sqcup((e(v^2)\cap e^{\mathrm{lp}}(\mathbb{G}^2))\setminus e^{\mathrm{lp}}(v^2)).$$

On the other hand, we obtain

$$\begin{aligned}\sigma(\mathfrak{G}^1_{v^2}) &= A+B+\sigma_{\mathfrak{G}^1}(v^2_\star)+\gamma^*-\gamma^*_{\setminus\{v^2\}}\\ &= A+B+(\#G/\#I_{v^2})(\sigma_{\mathfrak{G}^2}(v^2)-1)+\sum_{e\in e(v^2)\setminus e^{\mathrm{lp}}(v^2)}(\#G/\#I_e)(\#I_e/\#I_{v^2}-1)+1\\ &\qquad+\Bigg(\sum_{e\in(e(v^2)\cap e^{\mathrm{cl}}(\mathbb{G}^2))\setminus e^{\mathrm{lp}}(v^2)}\#G/\#I_e\Bigg)-1+\#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2})\\ &= A+B+(\#G/\#I_{v^2})\sigma_{\mathfrak{G}^2}(v^2)-\#G/\#I_{v^2}+\sum_{e\in e(v^2)\setminus e^{\mathrm{lp}}(v^2)}\#G/\#I_{v^2}\\ &\qquad-\sum_{e\in(e(v^2)\cap e^{\mathrm{op}}(\mathbb{G}^2))\setminus e^{\mathrm{lp}}(v^2)}\#G/\#I_e+\#e^{\mathrm{lp}}(v^2)(\#G/\#I_{v^2}).\end{aligned}$$

Namely, we have

$$\sigma(\mathfrak{G}^1)=\sigma(\mathfrak{G}^1_{v^2}).$$

We complete the proof of the proposition. □

2C4. The main result of the present section is as follows:

Theorem 2.7. *Let $\mathfrak{b}:\mathfrak{G}^1\to\mathfrak{G}^2$ be a G-covering of connected semigraphs with p-rank* (*Definition 2.2(e)*)*. Then we have* (*see Section 1A1 for $e(v)$, $e^{\mathrm{lp}}(v)$*)

$$\begin{aligned}\sigma(\mathfrak{G}^1)=\sum_{v\in v(\mathbb{G}^2)}\Bigg((\#G/\#I_v)(\sigma_{\mathfrak{G}^2}(v)-1)+\sum_{e\in e(v)\setminus e^{\mathrm{lp}}(v)}(\#G/\#I_e)(\#I_e/\#I_v-1)+1\Bigg)\\ +\sum_{e\in e^{\mathrm{cl}}(\mathbb{G}^2)\setminus e^{\mathrm{lp}}(\mathbb{G}^2)}(\#G/\#I_e-1)+\sum_{v\in v(\mathbb{G}^2)}\#e^{\mathrm{lp}}(v)(\#G/\#I_v-1)+\gamma_{\mathbb{G}^2}.\end{aligned}$$

Proof. By applying Proposition 2.6 and the operator $\overset{\mathrm{I}}{\underset{\mathrm{II}}{\rightleftharpoons}}$ (Definition 2.4), we may construct a quasi-G-covering $\mathfrak{b}^*:\mathfrak{G}^{1,*}\to\mathfrak{G}^2$ from $\mathfrak{b}$ such that the following conditions are satisfied:

(i) We have $\#(\beta^*)^{-1}(v)=1$ for each $v\in v(\mathbb{G}^2)$, where β^* denotes the underlying morphism of $\mathfrak{b}^*$.

(ii) For each $v\in v(\mathbb{G}^2)$ and $v^*\in(\beta^*)^{-1}(v)$, we have

$$\begin{aligned}\sigma_{\mathfrak{G}^{1,*}}(v^*) &= (\#G/\#I_v)(\sigma_{\mathfrak{G}^2}(v)-1)+\sum_{e\in e(v)}(\#G/\#I_e)(\#I_e/\#I_v-1)+1\\ &= (\#G/\#I_v)(\sigma_{\mathfrak{G}^2}(v)-1)+\sum_{e\in e(v)\setminus e^{\mathrm{lp}}(v)}(\#G/\#I_e)(\#I_e/\#I_v-1)+1.\end{aligned}$$

(iii) $\sigma(\mathfrak{G}^{1,*})=\sigma(\mathfrak{G}^1)$.

Write $\mathbb{G}^{1,*}$ for the underlying semigraph of $\mathfrak{G}^{1,*}$. We observe that

$$\begin{aligned}\gamma_{\mathbb{G}^{1,*}} &= \gamma_{\mathbb{G}^2} + \sum_{e\in e^{\mathrm{cl}}(\mathbb{G}^2)\setminus e^{\mathrm{lp}}(\mathbb{G}^2)} (\#G/\#I_e - 1) - \sum_{v\in v(\mathbb{G}^2)} \#e^{\mathrm{lp}}(v) + \sum_{v\in v(\mathbb{G}^2)} \#e^{\mathrm{lp}}(v)(\#G/\#I_v) \\ &= \gamma_{\mathbb{G}^2} + \sum_{e\in e^{\mathrm{cl}}(\mathbb{G}^2)\setminus e^{\mathrm{lp}}(\mathbb{G}^2)} (\#G/\#I_e - 1) + \sum_{v\in v(\mathbb{G}^2)} \#e^{\mathrm{lp}}(v)(\#G/\#I_v - 1).\end{aligned}$$

Thus, we obtain

$$\begin{aligned}\sigma(\mathfrak{G}^1) = \sigma(\mathfrak{G}^{1,*}) = \sum_{v\in v(\mathbb{G}^2)} \Bigg((\#G/\#I_v)(\sigma_{\mathfrak{G}^2}(v) - 1) + \sum_{e\in e(v)\setminus e^{\mathrm{lp}}(v)} (\#G/\#I_e)(\#I_e/\#I_v - 1) + 1 \Bigg) \\ + \sum_{e\in e^{\mathrm{cl}}(\mathbb{G}^2)\setminus e^{\mathrm{lp}}(\mathbb{G}^2)} (\#G/\#I_e - 1) + \sum_{v\in v(\mathbb{G}^2)} \#e^{\mathrm{lp}}(v)(\#G/\#I_v - 1) + \gamma_{\mathbb{G}^2}.\end{aligned}$$

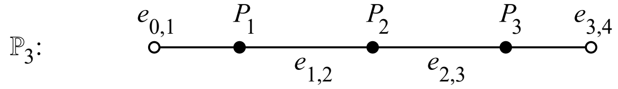
This completes the proof of the theorem. □

2C5. We introduce a kind of special semigraph. Let n be a positive natural number and $\mathbb{P}_n$ a semigraph (see Example 2.8 below) such that the following conditions are satisfied:

(i) $v(\mathbb{P}_n) = \{P_1, \ldots, P_n\}$, $e^{\mathrm{cl}}(\mathbb{P}_n) = \{e_{1,2}, \ldots, e_{n-1,n}\}$, and $e^{\mathrm{op}}(\mathbb{P}_n) = \{e_{0,1}, e_{n,n+1}\}$.

(ii) $\zeta^{\mathbb{P}_n}_{e_{0,1}}(e_{0,1}) = \{P_1, \{v(\mathbb{P}_n)\}\}$, $\zeta^{\mathbb{P}_n}_{e_{n,n+1}}(e_{n,n+1}) = \{P_n, \{v(\mathbb{P}_n)\}\}$, and $\zeta^{\mathbb{P}_n}_{e_{i,i+1}}(e_{i,i+1}) = \{P_i, P_{i+1}\}$, $i \in \{1, \ldots, n-1\}$.

Example 2.8. We give an example to explain the notion defined above. If $n = 3$, then $\mathbb{P}_3$ is as follows:



Definition 2.9. Let $\mathbb{P}_n$ be a semigraph defined above and $\sigma_{\mathfrak{P}_n} : v(\mathbb{P}_n) \to \mathbb{Z}$ a map such that $\sigma_{\mathfrak{P}_n}(P_i) = 0$ for each $i = \{1, \ldots, n\}$. We define a semigraph with p-rank $\mathfrak{P}_n$ to be

$$\mathfrak{P}_n \overset{\mathrm{def}}{=} (\mathbb{P}_n, \sigma_{\mathfrak{P}_n}),$$

and shall call $\mathfrak{P}_n$ an *n-chain*.

Remark 2.9.1. In Section 3C, we will see that n-chains can be naturally arose from quotients of the vertical fibers associated to *singular* vertical points (Definition 1.8) of G-pointed semistable coverings.

2C6. When $\mathfrak{G}^2 = \mathfrak{P}_n$ is a n-chain, Theorem 2.7 has the following important consequence.

Corollary 2.10. *Let $\mathfrak{b} : \mathfrak{G} \to \mathfrak{P}_n$ be a G-covering of connected semigraphs with p-rank. Then we have*

$$\sigma(\mathfrak{G}) = \sum_{i=1}^{n} \#G/\#I_{P_i} - \sum_{i=1}^{n+1} \#G/\#I_{e_{i-1,i}} + 1.$$

Proof. The construction of $\mathbb{P}_n$ implies

$$\sum_{v\in v(\mathbb{P}_n)} \#e^{\mathrm{lp}}(v)(\#G/\#I_v - 1) = \gamma_{\mathbb{P}_n} = 0.$$

Then the corollary follows immediately from Theorem 2.7. □

3. Formulas for p-rank of coverings of curves

In this section, we construct various semigraphs with p-rank from G-pointed semistable coverings. Moreover, we prove various formulas for p-rank concerning G-pointed semistable coverings when G is a finite p-group. More precisely, we prove a formula for p-rank of special fibers (see Theorem 3.2), a formula for p-rank of vertical fibers over vertical points (see Theorem 3.4), and a simpler form of Theorem 3.4 when the vertical points are singular (see Theorem 3.9 which plays a key in Section 4). In particular, Theorems 3.4 and 3.9 generalize Raynaud's result (Theorem 1.9) to the case of *arbitrary closed points*.

3A. *p-rank of special fibers.*

3A1. *Settings.* We maintain the settings introduced in Section 1C1. Let G be a finite p-group of order p^r, and let $f : \mathscr{Y} = (Y, D_Y) \to \mathscr{X} = (X, D_X)$ be a G-pointed semistable covering (Definition 1.5) over S. Moreover, let

$$\Phi : \{1\} = G_r \subset G_{r-1} \subset \cdots \subset G_1 \subset G_0 = G$$

be a maximal normal filtration (Definition 2.2) of G. By applying [Raynaud 1990, Appendice, Corollaire], we have that $\mathscr{X}^{\mathrm{sst}} = (X^{\mathrm{sst}}, D_{X^{\mathrm{sst}}}) \overset{\mathrm{def}}{=} \mathscr{Y}/G$ is a pointed semistable curve over S. Write $h : \mathscr{Y} \to \mathscr{X}^{\mathrm{sst}}$ and $g : \mathscr{X}^{\mathrm{sst}} \to \mathscr{X}$ for the natural morphisms of pointed semistable curves over S induced by f such that $f = g \circ h : \mathscr{Y} \xrightarrow{h} \mathscr{X}^{\mathrm{sst}} \xrightarrow{g} \mathscr{X}$.

3A2. Let $j \in \{0, \dots, r\}$, [Raynaud 1990, Appendice, Corollaire] implies that $\mathscr{Y}_j \overset{\mathrm{def}}{=} \mathscr{Y}/G_j$ is a pointed semistable curve over S. Then the maximal normal filtration Φ of G induces a sequence of morphism of pointed semistable curves

$$\Phi_{\mathscr{Y}/\mathscr{X}^{\mathrm{sst}}} : \mathscr{Y}_r \overset{\mathrm{def}}{=} \mathscr{Y} \xrightarrow{\phi_r} \mathscr{Y}_{r-1} \xrightarrow{\phi_{r-1}} \cdots \xrightarrow{\phi_1} \mathscr{Y}_0 \overset{\mathrm{def}}{=} \mathscr{X}^{\mathrm{sst}}$$

over S such that $\phi_1 \circ \cdots \circ \phi_r = h$. Note that ϕ_j is a *finite* $\mathbb{Z}/p\mathbb{Z}$-pointed semistable covering over S.

Write $\Gamma_{\mathscr{Y}_j}$ for the dual semigraph (Section 1B2) of the special fiber $(\mathscr{Y}_j)_s$ of $\mathscr{Y}_j$. Then, for each $j \in \{1, \dots, r\}$, the morphism of the special fibers $(\phi_j)_s : (\mathscr{Y}_j)_s \to (\mathscr{Y}_{j-1})_s$ induces a map of semigraphs $\beta_j : \Gamma_{\mathscr{Y}_j} \to \Gamma_{\mathscr{Y}_{j-1}}$. Moreover, Proposition 1.7 implies that β_j, $j \in \{1, \dots, r\}$, is a *morphism* of semigraphs.

3A3. *Semigraph with p-rank associated to* $(\mathscr{Y}_j)_s$. Let $v \in v(\Gamma_{\mathscr{Y}_j})$ and $j \in \{0, \dots, r\}$. We write $\widetilde{Y}_{j,v}$ for the normalization of the irreducible component $Y_{j,v} \subseteq (\mathscr{Y}_j)_s$ corresponding to v. We define a semigraph with p-rank associated to $(\mathscr{Y}_j)_s$ to be

$$\mathfrak{G}_{\mathscr{Y}_j} \overset{\mathrm{def}}{=} (\mathbb{G}_{\mathscr{Y}_j}, \sigma_{\mathfrak{G}_{\mathscr{Y}_j}}), \quad j \in \{0, \dots, r\},$$

where $\mathbb{G}_{\mathscr{Y}_j} \overset{\mathrm{def}}{=} \Gamma_{\mathscr{Y}_j}$ and $\sigma_{\mathfrak{G}_{\mathscr{Y}_j}}(v) \overset{\mathrm{def}}{=} \sigma(\widetilde{Y}_{j,v})$ for $v \in v(\mathbb{G}_{\mathscr{Y}_j})$.

3A4. *G-covering of semigraphs with p-rank associated to f.* The sequence of pointed semistable coverings $\Phi_{\mathscr{Y}/\mathscr{X}^{\mathrm{sst}}}$ induces a sequence of morphisms of semigraphs with p-rank

$$\Phi_{\mathfrak{G}_{\mathscr{Y}}/\mathfrak{G}_{\mathscr{X}^{\mathrm{sst}}}}:\mathfrak{G}_{\mathscr{Y}}\overset{\mathrm{def}}{=}\mathfrak{G}_{\mathscr{Y}_r}\xrightarrow{\mathfrak{b}_r}\mathfrak{G}_{\mathscr{Y}_{r-1}}\xrightarrow{\mathfrak{b}_{r-1}}\cdots\xrightarrow{\mathfrak{b}_1}\mathfrak{G}_{\mathscr{X}^{\mathrm{sst}}}\overset{\mathrm{def}}{=}\mathfrak{G}_{\mathscr{Y}_0},$$

where $\mathfrak{b}_j:\mathfrak{G}_{\mathscr{Y}_j}\to\mathfrak{G}_{\mathscr{Y}_{j-1}}$, $j\in\{1,\dots,r\}$, is induced by $\beta_j:\Gamma_{\mathscr{Y}_j}\to\Gamma_{\mathscr{Y}_{j-1}}$. By using the Deuring–Shafarevich formula (Proposition 1.4) and the Zariski–Nagata purity theorem [SGA 1 1971, Exposé X, Théorème de pureté 3.1], we see that $\mathfrak{b}_j$, $j\in\{1,\dots,r\}$, is a p-covering (Definition 2.2(c)). Moreover, $\mathfrak{b}\overset{\mathrm{def}}{=}\mathfrak{b}_1\circ\cdots\circ\mathfrak{b}_r$ is a G-covering (Definition 2.2(e)). Then we have

$$\sigma(\mathfrak{G}_{\mathscr{Y}})=\sigma(\mathscr{Y}_s).$$

Summarizing the discussions above, we obtain the following proposition.

Proposition 3.1. *We maintain the notation introduced above. Let $f:\mathscr{Y}\to\mathscr{X}$ be a G-pointed semistable covering over S and $\mathscr{Y}_s$ the special fiber of $\mathscr{Y}$ over s. Then there exists a G-covering of semigraphs with p-rank $\mathfrak{b}:\mathfrak{G}_{\mathscr{Y}}\to\mathfrak{G}_{\mathscr{X}^{\mathrm{sst}}}$ associated to f (which is constructed above) such that $\sigma(\mathscr{Y}_s)=\sigma_{\mathfrak{G}_{\mathscr{Y}}}(\mathfrak{G}_{\mathscr{Y}})$.*

3A5. We maintain the notation introduced in Section 3A1 and write $\Gamma_{\mathscr{X}_s^{\mathrm{sst}}}$ for the dual semigraph of the special fiber $\mathscr{X}_s^{\mathrm{sst}}=(X_s^{\mathrm{sst}},D_{X_s^{\mathrm{sst}}})$ of $\mathscr{X}^{\mathrm{sst}}$. Let $v\in v(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})$ and $e\in e(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})$ (Section 1A1). We write Y_v and y_e for an irreducible component of $h^{-1}(X_v)_{\mathrm{red}}$ and a closed point of $h^{-1}(x_e)_{\mathrm{red}}$, respectively, where X_v and x_e denote the irreducible component and the closed point of $\mathscr{X}_s^{\mathrm{sst}}$ corresponding to v and e (Section 1B2), respectively. Write $I_{Y_v}\subseteq G$ and $I_{y_e}\subseteq G$ for the inertia subgroup of Y_v and y_e, respectively. Note that since $\#I_{Y_v}$ and $\#I_{y_e}$ do not depend on the choices of Y_v and y_e, respectively, we may denote $\#I_{Y_v}$ and $\#I_{y_e}$ by $\#I_v$ and $\#I_e$, respectively. We put (see Section 1A1 for $v(e)$)

$$\#I_e^{\mathrm{m}}\overset{\mathrm{def}}{=}\max_{v\in v(e)}\{\#I_v\},\quad e\in e^{\mathrm{cl}}(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}}).$$

Note that Corollary 1.13 implies that $\#I_e=\#I_e^{\mathrm{m}}$.

We have the following formula for p-rank of special fibers of G-pointed stable coverings when G is a finite p-group.

Theorem 3.2. *We maintain the settings introduced above. Let G be a finite p-group, and let $f:\mathscr{Y}\to\mathscr{X}$ be a G-pointed semistable covering over S. Then we have (see Section 1B2 for $\widetilde{X}_v$, Section 1A1 for $e^{\mathrm{cl}}(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})$, $e^{\mathrm{lp}}(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})$, $e(v)$, $e^{\mathrm{lp}}(v)$, and Section 1A3 for $\gamma_{\Gamma_{\mathscr{X}_s^{\mathrm{sst}}}}$)*

$$\sigma(\mathscr{Y}_s)=\sum_{v\in v(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})}\Bigl(1+(\#G/\#I_v)(\sigma(\widetilde{X}_v)-1)+\sum_{e\in e(v)\setminus e^{\mathrm{lp}}(v)}(\#G/\#I_e)(\#I_e/\#I_v-1)\Bigr)$$
$$+\sum_{e\in e^{\mathrm{cl}}(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})\setminus e^{\mathrm{lp}}(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})}(\#G/\#I_e-1)+\sum_{v\in v(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})}\#e^{\mathrm{lp}}(v)(\#G/\#I_v-1)+\gamma_{\Gamma_{\mathscr{X}_s^{\mathrm{sst}}}}.$$

In particular, if $f : \mathscr{Y} \to \mathscr{X}$ is a G-semistable covering (*i.e.*, $D_X = \varnothing$), *then we have*

$$\sigma(\mathscr{Y}_s) = \sum_{v \in v(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})} \Bigg(1 + (\#G/\#I_v)(\sigma(\widetilde{X}_v) - 1) + \sum_{e \in e(v) \setminus e^{\mathrm{lp}}(v)} (\#G/\#I_e^{\mathrm{m}})(\#I_e^{\mathrm{m}}/\#I_v - 1)\Bigg) \\ + \sum_{e \in e^{\mathrm{cl}}(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}}) \setminus e^{\mathrm{lp}}(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})} (\#G/\#I_e^{\mathrm{m}} - 1) + \sum_{v \in v(\Gamma_{\mathscr{X}_s^{\mathrm{sst}}})} \#e^{\mathrm{lp}}(v)(\#G/\#I_v - 1) + \gamma_{\Gamma_{\mathscr{X}_s^{\mathrm{sst}}}}.$$

Proof. The theorem follows from Theorem 2.7 and Proposition 3.1. □

Remark 3.2.1. Note that it is easy to check that *the formula of Theorem 3.2 depends only on the G-pointed stable coverings.*

3B. *p-rank of vertical fibers.*

3B1. *Settings.* We maintain the settings introduced in Section 3A1. Let x be a *vertical point* (see Definition 1.8) associated to f. Write $\psi : Y' \to X$ for the normalization of X in the function field $K(Y)$ induced by the natural injection $K(X) \hookrightarrow K(Y)$ induced by f. Then Y' admits a natural action of G induced by the action of G on the generic fiber of Y.

Let $y' \in \psi^{-1}(x)$. Write $I_{y'} \subseteq G$ for the inertia subgroup of y'. Proposition 1.6 implies that the morphism of pointed smooth curves $(Y_\eta/I_{y'}, D_{Y_\eta}/I_{y'}) \to \mathscr{X}_\eta$ over η induced by f extends to a pointed semistable covering $\mathscr{Y}_{I_{y'}} \to \mathscr{X}$ over S. In order to calculate the p-rank of $f^{-1}(x)$, since the morphism $\mathscr{Y}_{I_{y'}} \to \mathscr{X}$ is finite étale over x, by replacing $\mathscr{X}$ by $\mathscr{Y}_{I_{y'}}$, we may assume that G is equal to $I_{y'}$. In the remainder of this subsection, we shall assume $G = I_{y'}$ (note that $G = I_{y'}$ if and only if $f^{-1}(x)$ is *connected*).

3B2. Write $\mathscr{X}_s^{\mathrm{sst}} = (X_s^{\mathrm{sst}}, D_{X_s^{\mathrm{sst}}})$ and $\mathscr{Y}_s = (Y_s, D_{Y_s})$ for the special fibers of $\mathscr{X}^{\mathrm{sst}}$ and $\mathscr{Y}$ over s, respectively. By the general theory of semistable curves, $g^{-1}(x)_{\mathrm{red}} \subset X_s^{\mathrm{sst}}$ and $f^{-1}(x)_{\mathrm{red}} = h^{-1}(g^{-1}(x))_{\mathrm{red}} \subset Y_s$ are semistable curves over s, where $(-)_{\mathrm{red}}$ denotes the reduced induced closed subscheme of $(-)$. In particular, the irreducible components of $g^{-1}(x)_{\mathrm{red}}$ are isomorphic to $\mathbb{P}_k^1$.

Write V_X for the set of closed points

$$g^{-1}(x)_{\mathrm{red}} \cap \overline{\{X_s^{\mathrm{sst}} \setminus g^{-1}(x)_{\mathrm{red}}\}},$$

where $\overline{\{X_s^{\mathrm{sst}} \setminus g^{-1}(x)_{\mathrm{red}}\}}$ denotes the topological closure of $X_s^{\mathrm{sst}} \setminus g^{-1}(x)_{\mathrm{red}}$ in X_s^{sst}. Write $V_Y \subset \mathscr{Y}_s$ for the set of closed points $\{h^{-1}(q)_{\mathrm{red}}\}_{q \in V_X}$. We have $\#V_X = 1$ if x is a *smooth point* of $\mathscr{X}_s$, and $\#V_X = 2$ if x is a *node* of $\mathscr{X}_s$.

3B3. We define two pointed semistable curves over s to be

$$\mathscr{E}_X \overset{\mathrm{def}}{=} (g^{-1}(x)_{\mathrm{red}}, (D_{X^{\mathrm{sst}}} \cap g^{-1}(x)_{\mathrm{red}}) \cup V_X) \quad \text{and} \quad \mathscr{E}_Y \overset{\mathrm{def}}{=} (f^{-1}(x)_{\mathrm{red}}, (D_Y \cap f^{-1}(x)_{\mathrm{red}}) \cup V_Y).$$

Then we obtain a *finite* morphism of pointed semistable curves $\rho_{\mathscr{E}_Y/\mathscr{E}_X} : \mathscr{E}_Y \to \mathscr{E}_X$ induced by h. Since $f^{-1}(x)$ is connected, $\mathscr{E}_Y$ admits a natural action of G induced by the action of G on the special fiber $\mathscr{Y}_s$ of $\mathscr{Y}$. Write $\Gamma_{\mathscr{E}_Y}$ and $\Gamma_{\mathscr{E}_X}$ for the dual semigraphs of $\mathscr{E}_Y$ and $\mathscr{E}_X$, respectively. Note that $\Gamma_{\mathscr{E}_X}$ is a tree, and is *not* a n-chain (Definition 2.9) in general if x is not a node. We obtain a map of semigraphs

$$\delta_{\mathscr{E}_Y/\mathscr{E}_X} : \Gamma_{\mathscr{E}_Y} \to \Gamma_{\mathscr{E}_X}$$

induced by $\rho_{\mathscr{E}_Y/\mathscr{E}_X}$. Moreover, Proposition 1.7 implies that the map $\delta_{\mathscr{E}_Y/\mathscr{E}_X} : \Gamma_{\mathscr{E}_Y} \to \Gamma_{\mathscr{E}_X}$ is a morphism of semigraphs.

3B4. *Semigraphs with p-rank associated to $\mathscr{E}_Y$ and $\mathscr{E}_X$.* Let $v \in v(\Gamma_{\mathscr{E}_Y})$. Write $\widetilde{Y}_v$ for the normalization of the irreducible component $Y_v \subseteq \mathscr{E}_Y$ corresponding to v. We define semigraphs with p-rank associated to $\mathscr{E}_Y$ and $\mathscr{E}_X$, respectively, as follows:

$$\mathfrak{E}_Y \overset{\text{def}}{=} (\mathbb{E}_Y, \sigma_{\mathfrak{E}_Y}), \qquad \mathfrak{E}_X \overset{\text{def}}{=} (\mathbb{E}_X, \sigma_{\mathfrak{E}_X}),$$

where $\mathbb{E}_Y \overset{\text{def}}{=} \Gamma_{\mathscr{E}_Y}$, $\mathbb{E}_X \overset{\text{def}}{=} \Gamma_{\mathscr{E}_X}$, $\sigma_{\mathfrak{E}_Y}(v) \overset{\text{def}}{=} \sigma(\widetilde{Y}_v)$ for $v \in v(\mathbb{E}_Y)$, and $\sigma_{\mathfrak{E}_X}(w) \overset{\text{def}}{=} 0$ for $w \in v(\mathbb{E}_X)$.

3B5. *G-coverings of semigraphs with p-rank associated to vertical fibers.* The morphism of dual semigraphs $\delta_{\mathscr{E}_Y/\mathscr{E}_X} : \Gamma_{\mathscr{E}_Y} \to \Gamma_{\mathscr{E}_X}$ induces a morphism of semigraphs with p-rank

$$\mathfrak{d}_{\mathfrak{E}_Y/\mathfrak{E}_X} : \mathfrak{E}_Y \to \mathfrak{E}_X.$$

Moreover, we see that $\mathfrak{d}_{\mathfrak{E}_Y/\mathfrak{E}_X}$ is a G-covering. Then we have

$$\sigma(\mathfrak{E}_Y) = \sigma(f^{-1}(x)_{\text{red}}) = \sigma(f^{-1}(x)).$$

Summarizing the discussions above, we obtain the following proposition.

Proposition 3.3. *We maintain the notation introduced above. Let $f : \mathscr{Y} \to \mathscr{X}$ be a G-pointed semistable covering over S and x a vertical point associated to f. Suppose that $f^{-1}(x)$ is connected. Then there exists a G-covering of semigraphs with p-rank $\mathfrak{d}_{\mathfrak{E}_Y/\mathfrak{E}_X} : \mathfrak{E}_Y \to \mathfrak{E}_X$ associated to f and x* (*which is constructed above*) *such that $\sigma(\mathfrak{E}_Y) = \sigma(f^{-1}(x))$.*

3B6. Then we have the following formula for p-rank of vertical fibers.

Theorem 3.4. *We maintain the settings introduced in Section 1C1. Let G be a finite p-group, and let $f : \mathscr{Y} \to \mathscr{X}$ be a G-pointed semistable covering* (*Definition 1.5*) *over S and x a vertical point* (*Definition 1.8*) *associated to f. We maintain the notation introduced in Sections 3B2 and 3B3. Suppose that $f^{-1}(x)$ is connected. Then we have* (*see Section 3A5 for $\#I_v$, $\#I_e$, and Section 1A1 for $v(\Gamma_{\mathscr{E}_X})$, $e(v)$, $e^{\text{cl}}(\Gamma_{\mathscr{E}_X})$*)

$$\sigma(f^{-1}(x)) = \sum_{v \in v(\Gamma_{\mathscr{E}_X})} \left(1 - \#G/\#I_v + \sum_{e \in e(v)} (\#G/\#I_e)(\#I_e/\#I_v - 1)\right) + \sum_{e \in e^{\text{cl}}(\Gamma_{\mathscr{E}_X})} (\#G/\#I_e - 1).$$

Proof. The theorem follows from Theorem 2.7 and Proposition 3.3. □

3B7. We maintain the notation introduced in Theorem 3.4. We explain that Raynaud's result (i.e., Theorem 1.9) can be directly calculated by using Theorem 3.4 if $x \in X_s \setminus (X_s^{\mathrm{sing}} \cup D_{X_s})$. Note that, since $x \notin D_{X_s}$, we have $g^{-1}(x)_{\mathrm{red}} \cap D_{X_s^{\mathrm{sst}}} = \varnothing$.

Let X_0' be the irreducible component of X_s which contains x. Moreover, we write X_0 for the strict transform of X_0' under the birational morphism $g : \mathscr{X}^{\mathrm{sst}} \to \mathscr{X}$. Then there exists a unique irreducible component $X_1 \subseteq g^{-1}(x)_{\mathrm{red}} \subseteq X_s^{\mathrm{sst}}$ such that $X_0 \cap X_1 \neq \varnothing$. Note that $\#(X_0 \cap X_1) = 1$. Write v_1 for the vertex of $v(\Gamma_{\mathscr{E}_X})$ corresponding to X_1. Since $\Gamma_{\mathscr{E}_X}$ is a connected tree, for each $v \in v(\Gamma_{\mathscr{E}_X})$, there exists a path $l(v_1, v)$ connecting v_1 and v. We define

$$\mathrm{leng}(l(v_1, v)) \overset{\mathrm{def}}{=} \#\{l(v_1, v) \cap v(\Gamma_{\mathscr{E}_X})\}$$

to be the length of the path $l(v_1, v)$. Moreover, for each $v \in v(\Gamma_{\mathscr{E}_X})$, we write

$$l_{v_1, v}$$

for the path such that $\mathrm{leng}(l_{v_1,v}) = \min\{\mathrm{leng}(l(v_1, v))\}_{l(v_1,v)}$.

By applying the general theory of semistable curves, Lemma 1.10, and Corollary 1.13, one may prove the following:

> Let $v, v' \in v(\Gamma_{\mathscr{E}_X})$ and X_v, $X_{v'}$ the irreducible components of $g^{-1}(x)_{\mathrm{red}}$ corresponding to v, v', respectively. Suppose that $\{x_e\} \overset{\mathrm{def}}{=} X_v \cap X_{v'} \neq \varnothing$, and that $\mathrm{leng}(l_{v_1,v}) < \mathrm{leng}(l_{v_1,v'})$. Write $e \in e^{\mathrm{cl}}(\Gamma_{\mathscr{E}_X})$ for the closed edge corresponding to x_e. Then we have $\#I_v = \#I_e$ and $\#I_{v'} \mid \#I_v$.

Note that the inertia subgroup of the unique open edge of $\Gamma_{\mathscr{E}_X}$ (which abuts to v_1) is equal to G. Then Theorem 3.4 implies that $\sigma(f^{-1}(x)) = 0$.

3C. *p-rank of vertical fibers associated to singular vertical points.* In this subsection, we will see that Theorem 3.4 has a very simple form if x is a *singular vertical point* which plays a central role in Section 4.

3C1. *Settings.* We maintain the settings introduced in Section 3B1. Moreover, we suppose that the vertical point x is a *node* of $\mathscr{X}_s$. Write X_1' and X_2' (which may be equal) for the irreducible components of $\mathscr{X}_s$ containing x. Write X_1 and X_2 for the strict transforms of X_1' and X_2' under the birational morphism $g : \mathscr{X}^{\mathrm{sst}} \to \mathscr{X}$, respectively.

By the general theory of semistable curves, $g^{-1}(x)_{\mathrm{red}} \subseteq X_s^{\mathrm{sst}}$ is a semistable curve over s and $g^{-1}(x)_{\mathrm{red}} \cap D_{X_s^{\mathrm{sst}}} = \varnothing$. Moreover, the irreducible components of $g^{-1}(x)_{\mathrm{red}}$ are isomorphic to $\mathbb{P}_k^1$. Let C be the semistable subcurve of $g^{-1}(x)_{\mathrm{red}}$ which is a chain of projective lines $\bigcup_{i=1}^n P_i$ such that the following conditions are satisfied:

(i) For any $w, t \in \{1, \dots, n\}$, $P_w \cap P_t = \varnothing$ if $|w - t| \geq 2$, and $P_w \cap P_t$ is reduced to a point if $|w - t| = 1$.

(ii) $P_1 \cap X_1$ (resp. $P_n \cap X_2$) is reduced to a point.

(iii) $C \cap \overline{\{X_s^{\mathrm{sst}} \setminus g^{-1}(x)_{\mathrm{red}}\}} = (P_1 \cap X_1) \cup (P_n \cap X_2)$, where $\overline{\{X_s^{\mathrm{sst}} \setminus g^{-1}(x)_{\mathrm{red}}\}}$ denotes the topological closure of $X_s^{\mathrm{sst}} \setminus g^{-1}(x)_{\mathrm{red}}$ in X_s^{sst}.

Then we have

$$g^{-1}(x)_{\mathrm{red}} = C \cup B,$$

where B denotes the topological closure of $g^{-1}(x)_{\mathrm{red}} \setminus C$ in $g^{-1}(x)_{\mathrm{red}}$. Note that $B \cap C$ are smooth points of C. Then Theorem 1.9 (or Section 3B7) implies that the p-rank of the connected components of $h^{-1}(B)$ are equal to 0. Thus, we have $\sigma(f^{-1}(x)) = \sigma(h^{-1}(C))$.

3C2. We introduce the following notation concerning inertia subgroups of irreducible components of vertical fibers.

Definition 3.5. We maintain the notation introduced above:

(a) Let $\mathcal{V}_x \overset{\mathrm{def}}{=} \{V_0, V_1, \dots, V_n, V_{n+1}\}$ be a set of irreducible components of the special fiber $\mathscr{Y}_s$ of $\mathscr{Y}$. We shall call $\mathcal{V}_x$ a *collection of vertical fibers* associated to x if the following conditions are satisfied:

(i) $h(V_i) = P_i$ for $i \in \{1, \dots, n\}$.

(ii) $h(V_0) = X_1$ and $h(V_{n+1}) = X_2$.

(iii) The union $\bigcup_{i=0}^{n+1} V_i \subseteq \mathscr{Y}_s$ is a connected semistable subcurve of $\mathscr{Y}_s$ over s. Note that we have $\big(\bigcup_{i=1}^{n} V_i\big) \cap D_{Y_s} = \varnothing$.

Moreover, we write $I_{V_i} \subseteq G$, $i \in \{0, \dots, n+1\}$, for the inertia subgroup of V_i, and put

$$\mathcal{I}_{\mathcal{V}_x} \overset{\mathrm{def}}{=} \{I_{V_0}, \dots, I_{V_{n+1}}\}.$$

Note that Corollary 1.13 implies that either $I_{V_i} \subseteq I_{V_{i+1}}$ or $I_{V_i} \supseteq I_{V_{i+1}}$ holds for $i \in \{0, \dots, n\}$.

(b) Let $(u, w) \in \{0, \dots, n+1\} \times \{0, \dots, n+1\}$ be a pair such that $u \leq w$. We shall call that a group $I_{u,w}^{\min}$ is a *minimal element* of $\mathcal{I}_{\mathcal{V}_x}$ if one of the following conditions are satisfied, where "$\subset$" means that "is a subset which is not equal":

(i) $u = 0$, $w \neq 0$, $w \neq n+1$, and $I_{0,w}^{\min} = I_{V_0} = I_{V_1} = \cdots = I_{V_w} \subset I_{V_{w+1}}$.

(ii) $u \neq 0$, $w = n+1$, and $I_{V_{u-1}} \supset I_{V_u} = I_{V_{u+1}} \cdots = I_{V_{n+1}} = I_{u,n+1}^{\min}$.

(iii) $u \neq 0$, $w \neq n+1$, and $I_{V_{u-1}} \supset I_{u,w}^{\min} = I_{V_u} = I_{V_{u+1}} \cdots = I_{V_w} \subset I_{V_{w+1}}$.

Note that we *do not* define $I_{0,0}^{\min}$. We shall call that a group $J_{u,w}^{\max}$ is a *maximal element* of $\mathcal{I}_{\mathcal{V}_x}$ if one of the following conditions are satisfied:

(i) $(u, w) = (0, n+1)$ and $J_{0,n+1}^{\max} = I_{V_i}$ for all $i \in \{0, \dots, n+1\}$.

(ii) $u = 0$, $w \neq n+1$, and $J_{0,w}^{\max} = I_{V_0} = I_{V_1} = \cdots = I_{V_w} \supset I_{V_{w+1}}$.

(iii) $u \neq 0$, $w = n+1$, and $I_{V_{u-1}} \subset I_{V_u} = I_{V_{u+1}} \cdots = I_{V_{n+1}} = J_{u,n+1}^{\max}$.

(iv) $u \neq 0$, $w \neq n+1$, and $I_{V_{u-1}} \subset J_{u,w}^{\max} = I_{V_u} = I_{V_{u+1}} \cdots = I_{V_w} \supset I_{V_{w+1}}$.

Moreover, we put

$$\mathcal{I}(x) \overset{\mathrm{def}}{=} \bigsqcup_{I_{u,w}^{\min}\text{: a minimal element of } \mathcal{I}_{\mathcal{V}_x}} \{\# I_{u,w}^{\min}\} \quad \text{and} \quad \mathcal{J}(x) \overset{\mathrm{def}}{=} \bigsqcup_{J_{u,w}^{\max}\text{: a maximal element of } \mathcal{I}_{\mathcal{V}_x}} \{\# J_{u,w}^{\max}\},$$

where $\sqcup$ means disjoint union.

Note that the set $\mathcal{I}(x)$ may be empty (e.g., if $I_{V_0} \subset I_{V_1} \subset \cdots \subset I_{V_{n+1}}$, then $\mathcal{I}(x)$ is empty). On the other hand, since $\#I_{V_i}$, $i \in \{0, \dots, n+1\}$, does not depend on the choice of V_i (i.e., if $h(V_i) = h(V_i')$ for irreducible components V_i, V_i' of $\mathscr{Y}_s$, then $\#I_{V_i} = \#I_{V_i'}$), $\mathcal{I}(x)$ and $\mathcal{J}(x)$ *do not depend on* the choice of $\mathcal{V}_x$.

We shall call $\mathcal{I}(x)$ *the set of minimal orders of inertia subgroups associated to x and f*, and $\mathcal{J}(x)$ *the set of maximal orders of inertia subgroups associated to x and f*, respectively.

3C3. We have the following lemmas.

Lemma 3.6. *We maintain the notation introduced above. Let $y_i \in V_i$ be a closed point and $I_{y_i} \subseteq G$, $i \in \{1, \dots, n\}$ the inertia subgroup of y_i. Write Ray_{V_i}, $i = 1, \dots, n$, for the set of the closed points $h^{-1}(C \cap B)_{\mathrm{red}} \cap V_i$. Then we have $I_{y_i} = I_{V_i}$ for any $y_i \in \mathrm{Ray}_{V_i}$.*

Proof. Since $I_{y_i} \supseteq I_{V_i}$, we only need to prove that $I_{y_i} \subseteq I_{V_i}$. Note that I_{V_i} is a normal subgroup of I_{y_i}. To verify the lemma, by replacing G and $\mathscr{X}^{\mathrm{sst}}$ by I_{y_i} and $\mathscr{Y}/I_{y_i}$, respectively, we may assume $G = I_{y_i}$. Then we have $\#h^{-1}(h(y_i))_{\mathrm{red}} = 1$.

We consider the quotient $\mathscr{Y}/I_{V_i}$. By [Raynaud 1990, Appendice, Corollaire], we have that $\mathscr{Y}/I_{V_i}$ is a pointed semistable curve over S. Write $h_{I_{V_i}}$ for the quotient morphism $\mathscr{Y} \to \mathscr{Y}/I_{V_i}$ and $g_{I_{V_i}}$ for the morphism $\mathscr{Y}/I_{V_i} \to \mathscr{X}^{\mathrm{sst}}$ induced by h such that $h = g_{I_{V_i}} \circ h_{I_{V_i}}$. Write E_{y_i} for the connected component of $h^{-1}(B)_{\mathrm{red}}$ which contains y_i. By contracting $h_{I_{V_i}}(E_{y_i}) \subset \mathscr{Y}/I_{V_i} \times_S s$ (resp. $h(E_{y_i}) \subset \mathscr{X}_s^{\mathrm{sst}}$) [Bosch et al. 1990, 6.7 Proposition 4], we obtain a fiber surface $(\mathscr{Y}/I_{V_i})^{\mathrm{c}}$ and a semistable curve $(\mathscr{X}^{\mathrm{sst}})^{c}$ over S. Moreover, we have contracting morphisms as follows:

$$c_{h_{I_{V_i}}(E_{y_i})} : \mathscr{Y}/I_{V_i} \to (\mathscr{Y}/I_{V_i})^{\mathrm{c}}, \ c_{h(E_{y_i})} : \mathscr{X}^{\mathrm{sst}} \to (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}.$$

Furthermore, we obtain a morphism of fiber surfaces

$$g^{\mathrm{c}}_{I_{V_i}} : (\mathscr{Y}/I_{V_i})^{\mathrm{c}} \to (\mathscr{X}^{\mathrm{sst}})^{c}$$

induced by $g_{I_{V_i}}$ such that $c_{h(E_{y_i})} \circ g_{I_{V_i}} = g^{\mathrm{c}}_{I_{V_i}} \circ c_{h_{I_{V_i}}(E_{y_i})}$. Note that $(c_{h(E_{y_i})} \circ h)(y_i)$ is a smooth point of the special fiber of $(\mathscr{X}^{\mathrm{sst}})^{c}$, and $g^{\mathrm{c}}_{I_{V_i}}$ is étale at the generic point of $(c_{h_{I_{V_i}}(E_{y_i})} \circ h_{I_{V_i}})(V_i)$.

We put $y_i^{\mathrm{c}} \overset{\mathrm{def}}{=} (c_{h_{I_{V_i}}(E_{y_i})} \circ h_{I_{V_i}})(y_i) \in (\mathscr{Y}/I_{V_i})^{\mathrm{c}}$ and $x_i^{c} \overset{\mathrm{def}}{=} (c_{h(E_{y_i})} \circ h)(y_i) \in (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}$. Consider the local morphism

$$g_{y_i^{\mathrm{c}}} : \operatorname{Spec} \mathcal{O}_{(\mathscr{Y}/I_{V_i})^{\mathrm{c}}, y_i^{\mathrm{c}}} \to \operatorname{Spec} \mathcal{O}_{(\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}, x_i^{\mathrm{c}}}$$

induced by $g^{\mathrm{c}}_{I_{V_i}}$. Note that [Raynaud 1990, Proposition 1] implies that $\operatorname{Spec} \mathcal{O}_{(\mathscr{Y}/I_{V_i})^{\mathrm{c}}, y_i^{\mathrm{c}}} \times_S s$ is irreducible. Then $g_{y_i^{\mathrm{c}}}$ is generically étale at the generic point of $\operatorname{Spec} \mathcal{O}_{(\mathscr{Y}/I_{V_i})^{\mathrm{c}}, y_i^{\mathrm{c}}} \times_S s$. Thus, the Zariski–Nagata purity theorem implies that $g_{y_i^{\mathrm{c}}}$ is étale.

If $I_{V_i} \neq I_{y_i}$, then $g_{y_i^{\mathrm{c}}}$ is not an identity. Namely, we have $\#h^{-1}(h(y_i))_{\mathrm{red}} \neq 1$. This contradicts our assumption. Then we obtain $I_{V_i} = I_{y_i}$. We complete the proof of the lemma. □

Lemma 3.7. *We maintain the notation introduced in above. Then we have*

$$G = \langle I_{V_0}, I_{V_{n+1}} \rangle,$$

where $\langle I_{V_0}, I_{V_{n+1}} \rangle$ denotes the subgroup of G generated by I_{V_0} and $I_{V_{n+1}}$.

Proof. Suppose that $G \neq \langle I_{V_0}, I_{V_{n+1}} \rangle$. Since G is a p-group, there exists a normal subgroup $H \subseteq G$ of index p such that $\langle I_{V_0}, I_{V_{n+1}} \rangle \subseteq H$. Write $\mathscr{Y}'$ for the normalization of $\mathscr{X}$ in the function field $K(Y)$ induced by the natural injection $K(X) \hookrightarrow K(Y)$ induced by f. The normalization $\mathscr{Y}'$ admits an action of G induced by the action of G on $\mathscr{Y}$. Consider the quotient $\mathscr{Y}'/H$. Then we obtain a morphism of fiber surfaces $f_H : \mathscr{Y}'/H \to \mathscr{X}$ over S induced by f. Moreover, $\mathscr{Y}'/H$ admits an action of $G/H \cong \mathbb{Z}/p\mathbb{Z}$ induced by the action of G on $\mathscr{Y}'$. Then f_H is generically étale over X'_1 and X'_2. Thus, [Tamagawa 2004b, Lemma 2.1(iii)] implies that f_H is étale above x. Then $f^{-1}(x)$ is not connected. This contradicts our assumptions. We complete the proof of the lemma. □

3C4. We define pointed semistable curves over s as follows:

$$\mathscr{C}_Y \overset{\text{def}}{=} (h^{-1}(C)_{\text{red}}, h^{-1}((C \cap X_1) \cup (C \cap X_2))) \quad \text{and} \quad \mathscr{C}_X \overset{\text{def}}{=} (C, (C \cap X_1) \cup (C \cap X_2)).$$

Moreover, we have a natural morphism of pointed semistable curves

$$\rho_{\mathscr{C}_Y/\mathscr{C}_X} : \mathscr{C}_Y \to \mathscr{C}_X$$

over s induced by $h : \mathscr{Y} \to \mathscr{X}^{\text{sst}}$. Since $f^{-1}(x)_{\text{red}}$ is connected, $\mathscr{C}_Y$ admits a natural action of G induced by the action of G on $f^{-1}(x)_{\text{red}}$. Write $\Gamma_{\mathscr{C}_Y}$ and $\Gamma_{\mathscr{C}_X}$ for the dual semigraphs of $\mathscr{C}_Y$ and $\mathscr{C}_X$, respectively. Proposition 1.7 implies that the map of semigraphs

$$\delta_{\mathscr{C}_Y/\mathscr{C}_X} : \Gamma_{\mathscr{C}_Y} \to \Gamma_{\mathscr{C}_X}$$

induced by $\rho_{\mathscr{C}_Y/\mathscr{C}_X}$ is a morphism of semigraphs.

3C5. *Semigraphs with p-rank associated to vertical fibers over singular vertical points.* Let $v \in v(\Gamma_{\mathscr{C}_Y})$ and $\widetilde{Y}_v$ the normalization of the irreducible component $Y_v \subseteq \mathscr{C}_Y$ corresponding to v. We define semigraphs with p-rank associated to $\mathscr{C}_Y$ and $\mathscr{C}_X$, respectively, as follows:

$$\mathfrak{C}_Y \overset{\text{def}}{=} (\mathbb{C}_Y, \sigma_{\mathfrak{C}_Y}), \qquad \mathfrak{C}_X \overset{\text{def}}{=} (\mathbb{C}_X, \sigma_{\mathfrak{C}_X}),$$

where $\mathbb{C}_Y \overset{\text{def}}{=} \Gamma_{\mathscr{C}_Y}$, $\mathbb{C}_X \overset{\text{def}}{=} \Gamma_{\mathscr{C}_X}$, $\sigma_{\mathfrak{C}_Y}(v) \overset{\text{def}}{=} \sigma(\widetilde{Y}_v)$ for $v \in v(\mathbb{C}_Y)$, and $\sigma_{\mathfrak{C}_X}(w) \overset{\text{def}}{=} 0$ for $w \in v(\mathbb{C}_X)$.

3C6. *G-coverings of semigraphs with p-rank associated to vertical fibers over singular vertical points.* The morphism of dual semigraphs $\delta_{\mathscr{C}_Y/\mathscr{C}_X} : \Gamma_{\mathscr{C}_Y} \to \Gamma_{\mathscr{C}_X}$ induces a morphism of semigraphs with p-rank

$$\mathfrak{d}_{\mathfrak{C}_Y/\mathfrak{C}_X} : \mathfrak{C}_Y \to \mathfrak{C}_X.$$

Moreover, by Lemma 3.6, we see that $\sigma_{\mathfrak{C}_Y}(v)$ satisfies the Deuring–Shafarevich type formula for $v \in v(\mathbb{C}_Y)$. This implies that $\mathfrak{d}_{\mathfrak{C}_Y/\mathfrak{C}_X}$ is a G-covering of semigraphs with p-rank. Note that by the above construction, $\mathfrak{C}_X$ is an *n-chain* (Definition 2.9). Furthermore, we have

$$\sigma(\mathfrak{C}_Y) = \sigma(h^{-1}(C)) = \sigma(f^{-1}(x)).$$

Summarizing the discussion above, we obtain the following proposition.

Proposition 3.8. *We maintain the notation introduced above. Let $f : \mathscr{Y} \to \mathscr{X}$ be a G-pointed semistable covering over S and $x \in \mathscr{X}_s$ a vertical point associated to f. Suppose that $f^{-1}(x)$ is connected, and that x is a node of $\mathscr{X}_s$. Then there exists a G-covering of semigraphs with p-rank $\mathfrak{d}_{\mathfrak{C}_Y/\mathfrak{C}_X} : \mathfrak{C}_Y \to \mathfrak{C}_X$ associated to f and x (which is constructed above) such that $\mathfrak{C}_X$ is an n-chain and $\sigma(\mathfrak{C}_Y) = \sigma(f^{-1}(x))$.*

3C7. Then we have the following theorem.

Theorem 3.9. *We maintain the settings introduced in Section 1C1. Let G be a finite p-group, and let $f : \mathscr{Y} \to \mathscr{X}$ be a G-pointed semistable covering (Definition 1.5) over S and $x \in \mathscr{X}_s$ a vertical point (Definition 1.8) associated to f. Suppose that $f^{-1}(x)$ is connected, and that x is a node of $\mathscr{X}_s$. Let $\mathcal{I}(x)$ and $\mathcal{J}(x)$ be the sets of minimal and maximal orders of inertia subgroups associated to x and f (Definition 3.5(b)), respectively. Then we have*

$$\sigma(f^{-1}(x)) = \sum_{\#I \in \mathcal{I}(x)} \#G/\#I - \sum_{\#J \in \mathcal{J}(x)} \#G/\#J + 1.$$

Proof. Let $\mathcal{V}_x$ be a collection of vertical fibers associated to x (Definition 3.5(a)). By Proposition 3.8, Corollary 2.10, and Lemma 1.10, we have

$$\sigma(f^{-1}(x)) = \sum_{i=1}^{n} \#G/\#I_{V_i} - \sum_{i=1}^{n+1} \#G/\#\langle I_{V_{i-1}}, I_{V_i}\rangle + 1,$$

where $\langle I_{V_{i-1}}, I_{V_i}\rangle$ denotes the subgroup of G generated by $I_{V_{i-1}}$ and I_{V_i}. The theorem follows from Corollary 1.13 and Lemma 3.7. □

3C8. In the remainder of the present subsection, we suppose that G is a cyclic p-group. We show that the formula of Theorem 3.9 coincides with the formula of Saïdi [1998a, Proposition 1]. Since G is an abelian group, I_{V_i}, $i = \{0, \dots, n+1\}$, does not depend on the choice of V_i. Then we may use the notation I_{P_i}, $i \in \{0, \dots, n+1\}$, to denote I_{V_i}.

Lemma 3.10. *We maintain the notation introduced above. If G is a cyclic p-group, then there exists $0 \le u \le n+1$ such that*

$$I_{P_0} \supseteq I_{P_1} \supseteq I_{P_2} \supseteq \cdots \supseteq I_{P_u} \subseteq \cdots \subseteq I_{P_{n-1}} \subseteq I_{P_n} \subseteq I_{P_{n+1}}.$$

Proof. If the lemma is not true, then there exist w, t and v such that $I_{P_v} \neq I_{P_w}$, $I_{P_v} \neq I_{P_t}$ and $I_{P_w} \subset I_{P_{w+1}} = \cdots = I_{P_v} = \cdots = I_{P_{t-1}} \supset I_{P_t}$. Since G is a cyclic group, we may assume $I_{P_w} \supseteq I_{P_t}$. Consider the quotient of $\mathscr{Y}$ by I_{P_w}, we obtain a natural morphism of pointed semistable curves $h_w : \mathscr{Y}/I_{P_w} \to \mathscr{X}^{\mathrm{sst}}$ over S.

We define B_j, $j = \{0, \dots, n+1\}$, to be the union of the connected components of B (Section 3C1) which intersect with P_j nontrivially. By contracting [Bosch et al. 1990, 6.7 Proposition 4]

$$P_{w+1}, \dots, P_{t-1}, B_{w+1}, \dots, B_{t-1},$$
$$(h_w)^{-1}(P_{w+1})_{\mathrm{red}}, \dots, (h_w)^{-1}(P_{t-1})_{\mathrm{red}}, (h_w)^{-1}(B_{w+1})_{\mathrm{red}}, \dots, (h_w)^{-1}(B_{t-1})_{\mathrm{red}},$$

respectively, we obtain a pointed semistable curve $(\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}$ and a fiber surface $(\mathscr{Y}/I_{P_w})^{\mathrm{c}}$ over S. Write

$$c_{\mathscr{X}^{\mathrm{sst}}} : \mathscr{X}^{\mathrm{sst}} \to (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}},\ c_{\mathscr{Y}/I_{P_w}} : \mathscr{Y}/I_{P_w} \to (\mathscr{Y}/I_{P_w})^{\mathrm{c}}$$

for the resulting contracting morphisms, respectively. The morphism h_w induces a morphism of fiber surfaces $h_w^{\mathrm{c}} : (\mathscr{Y}/I_{P_w})^{\mathrm{c}} \to (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}$. Then we have the following commutative diagram:

$$\begin{tikzcd}
\mathscr{Y}/I_{P_w} \arrow[r, "c_{\mathscr{Y}/I_{P_w}}"] \arrow[d, "h_w"'] & (\mathscr{Y}/I_{P_w})^{\mathrm{c}} \arrow[d, "h_w^{\mathrm{c}}"'] \\
\mathscr{X}^{\mathrm{sst}} \arrow[r, "c_{\mathscr{X}^{\mathrm{sst}}}"] & (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}
\end{tikzcd}$$

Write P_w^{c} and P_t^{c} for the images $c_{\mathscr{X}^{\mathrm{sst}}}(P_w)$ and $c_{\mathscr{X}^{\mathrm{sst}}}(P_t)$, respectively, and x_{wt}^{c} for the closed point $P_w^{\mathrm{c}} \cap P_t^{\mathrm{c}}$. Since h_w^{c} is generically étale above P_w^{c} and P_t^{c}, [Tamagawa 2004b, Lemma 2.1(iii)] implies that $(h_w^{\mathrm{c}})^{-1}(x_{wt}^{\mathrm{c}})_{\mathrm{red}}$ are nodes. Thus, $(\mathscr{Y}/I_{P_w})^{\mathrm{c}}$ is a semistable curve over S, and moreover, h_w^{c} is étale over x_{wt}^{c}. Then the inertia subgroups of the closed points $(h_w^{\mathrm{c}})^{-1}(x_{wt}^{\mathrm{c}})_{\mathrm{red}}$ of the special fiber $(\mathscr{Y}/I_{P_w})_s^{\mathrm{c}}$ of $(\mathscr{Y}/I_{P_w})^{\mathrm{c}}$ are trivial.

On the other hand, since I_{P_w} is a proper subgroup of I_{P_v}, we have that the inertia subgroups of the irreducible components of $h_w^{-1}\big(\bigcup_{j=w+1}^{t-1} P_j\big)_{\mathrm{red}}$ is I_{P_v}/I_{P_w}. Thus, the inertia subgroups of the closed points $c_{\mathscr{Y}/I_{P_w}}(h_w^{-1}\big(\bigcup_{j=w+1}^{t-1} P_j\big)_{\mathrm{red}}) = (h_w^{\mathrm{c}})^{-1}(x_{wt}^{\mathrm{c}})_{\mathrm{red}} \subseteq (\mathscr{Y}/I_{P_w})_s^{\mathrm{c}}$ are not trivial. This is a contradiction. Then we complete the proof of the lemma. □

The above lemma implies the following corollary.

Corollary 3.11. *We maintain the settings introduced in Theorem 3.9. Suppose that G is a cyclic p-group, and that I_{P_0} is equal to G. Then we have*

$$\sigma(f^{-1}(x)) = \#G/\#I_{\min} - \#G/\#I_{P_{n+1}},$$

where $I_{\min}$ denotes the group $\bigcap_{i=0}^{n+1} I_{P_i}$.

Proof. The corollary follows immediately from Theorem 3.9 and Lemma 3.10. □

Remark 3.11.1. The formula in Corollary 3.11 had been obtained by Saïdi [1998a, Proposition 1]. On the other hand, Corollary 3.11 implies immediately that

$$\sigma(f^{-1}(x)) \leq \#G - 1$$

when G is a cyclic p-group, which is the main theorem of [Saïdi 1998a, Theorem 1].

4. Bounds of p-rank of vertical fibers

In this section, we gives an affirmative answer to an open problem posed by Saïdi concerning bounds of p-rank of vertical fibers posed by Saïdi if G is an arbitrary finite *abelian* p-group. The main result of the present section is Theorem 4.3.

4A. The following was asked by Saïdi [1998a, Question]:

> Let G be a finite p-group, and let $f : \mathscr{Y} \to \mathscr{X}$ be a *G-semistable covering* (i.e., $D_X = \varnothing$, see Definition 1.5) over S and $x \in \mathscr{X}_s$ a vertical point (Definition 1.8) associated to f. Suppose that $f^{-1}(x)$ is connected. Whether or not $\sigma(f^{-1}(x))$ can be bounded by a constant which depends only on $\#G$?

The above problem was solved by Saïdi when G is a cyclic p-group (Remark 3.11.1).

4B. ***Settings.*** We maintain the settings introduced in Section 1C1 and assume that $\mathscr{X}$ is a *stable curve* over S (i.e., $D_X = \varnothing$). Moreover, when x is a *node* of $\mathscr{X}_s^{\mathrm{sst}}$, let $\mathcal{V}_x$ be a collection of vertical fibers (Definition 3.5) and $\mathcal{I}_{\mathcal{V}_x} \overset{\mathrm{def}}{=} \{I_{V_i} \subseteq G\}_{i=\{0,\dots,n+1\}}$ the set of inertia subgroups of V_i (Definition 3.5). Furthermore, in the remainder of the present section, *we assume that G is an finite abelian p-group.*

4C. Since G is abelian, I_{V_i}, $\{i \in \{0, \dots, n+1\}$, does not depend on the choice of V_i. We use the notation I_{P_i} to denote I_{V_i} for $i \in \{0, \dots, n+1\}$. Then we have the following proposition.

Proposition 4.1. *Let I' and I'' be minimal elements of $\mathcal{I}_{\mathcal{V}_x}$ (Definition 3.5(b)) distinct from each other. Then neither $I' \subseteq I''$ nor $I' \supseteq I''$ holds.*

Proof. Without loss of generality, we may assume that $I' = I_{P_a}$ and $I'' = I_{P_b}$ such that $0 \le a < b \le n+1$, $I_{P_a} \neq I_{P_{a+1}}$, and $I_{P_{b-1}} \neq I_{P_b}$. Note that by the definition of minimal elements (Definition 3.5 (b)), $I_{P_{a+1}}$ (resp. $I_{P_{b-1}}$) contains I_{P_a} (resp. I_{P_b}).

If $I' \subseteq I''$, we consider the quotient curve $\mathscr{Y}/I''$. Then we obtain morphisms of semistable curves $\xi_1 : \mathscr{Y} \to \mathscr{Y}/I''$ and $\xi_2 : \mathscr{Y}/I'' \to \mathscr{X}^{\mathrm{sst}}$ such that $\xi_2 \circ \xi_1 = h$. Note that $h(V_a) = P_a$ and $h(V_b) = P_b$, respectively. By contracting $\bigcup_{i=a+1}^{b-1} P_i$ and $\xi_2^{-1}\big(\bigcup_{i=a+1}^{b-1} P_i\big)_{\mathrm{red}}$ [Bosch et al. 1990, 6.7 Proposition 4], respectively, we obtain contracting morphisms $c_{\mathscr{X}^{\mathrm{sst}}} : \mathscr{X}^{\mathrm{sst}} \to (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}$ and $c_{\mathscr{Y}/I''} : \mathscr{Y}/I'' \to (\mathscr{Y}/I'')^{\mathrm{c}}$, respectively. Moreover, ξ_2 induces a morphism $\xi_2^{\mathrm{c}} : (\mathscr{Y}/I'')^{\mathrm{c}} \to (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathscr{Y}/I'' \arrow[r, "c_{\mathscr{Y}/I''}"] \arrow[d, "\xi_2"'] & (\mathscr{Y}/I'')^{\mathrm{c}} \arrow[d, "\xi_2^{\mathrm{c}}"'] \\
\mathscr{X}^{\mathrm{sst}} \arrow[r, "c_{\mathscr{X}^{\mathrm{sst}}}"] & (\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}
\end{tikzcd}$$

Note that $(\mathscr{X}^{\mathrm{sst}})^{\mathrm{c}}$ is a semistable curve over S.

Since $I' = I_{P_a} \subseteq I'' = I_{P_b}$, ξ_2^{c} is étale at the generic points of $c_{\mathscr{Y}/I''} \circ \xi_1(V_a)$ and $c_{\mathscr{Y}/I''} \circ \xi_1(V_b)$. Thus, by applying the Zariski–Nagata purity theorem and [Tamagawa 2004b, Lemma 2.1(iii)], we obtain that ξ_2^{c} is étale at $c_{\mathscr{Y}/I''} \circ \xi_1(V_a) \cap c_{\mathscr{Y}/I''} \circ \xi_1(V_b)$ (i.e., the inertia group of each point of $c_{\mathscr{Y}/I''} \circ \xi_1(V_a) \cap c_{\mathscr{Y}/I''} \circ \xi_1(V_b)$ is trivial). On the other hand, since $I_{P_{b-1}}$ contains I_{P_b}, the inertia group of each point of $c_{\mathscr{Y}/I''} \circ \xi_1(V_a) \cap c_{\mathscr{Y}/I''} \circ \xi_1(V_b)$ is $I_{P_{b-1}}/I''$. Then we obtain $I_{P_{b-1}} = I''$. This is a contradiction. Then I'' does not contain I'.

Similar arguments to the arguments given in the proof above imply that I' does not contain I''. We complete the proof of the proposition. □

4D. Let N be a finite p-group and H a subgroup of N. Write $\mathrm{Sub}(-)$ for the set of the subgroups of $(-)$. We put

$$\#I(H) \overset{\text{def}}{=} \max\big\{\#\mathcal{S} \mid \mathcal{S} \subseteq \mathrm{Sub}(N),\, H \in \mathcal{S},\ \text{for any } H',\, H'' \in \mathcal{S} \text{ such that } H' \neq H'',\ \text{neither } H' \subseteq H'' \text{ nor } H' \supseteq H'' \text{ holds}\big\}.$$

Moreover, we put

$$M(N) \overset{\text{def}}{=} \max\{\#I(N')\}_{N' \in \mathrm{Sub}(N)}.$$

For any $1 \leq d \leq \#N$, write $S_d(N)$ for the set of the subgroups of N with order d. Let A be an elementary abelian p-group (i.e., $pA = 0$) such that $\#A = \#N$. We put

$$B(\#N) \overset{\text{def}}{=} \#\,\mathrm{Sub}(A).$$

Note that $B(\#N)$ depends only on $\#N$.

4E. We need a lemma of finite groups.

Lemma 4.2. *Let N be a finite p-group, A an elementary abelian p-group with order $\#N$, and $1 \leq d \leq \#N$ an integer number. Then we have $\#S_d(N) \leq \#S_d(A)$. In particular, we have $M(N) \leq B(\#N)$.*

Proof. Since N is a p-group, N has a nontrivial central subgroup. Fix a central subgroup Z of order p in N. Write $S_d^Z(N)$ (resp. $S_d^{\backslash Z}(N)$) for the set of subgroups of N of order d which contain Z (resp. do not contain Z). If H is a subgroup of N/Z, let $S_d^{(Z,H)}(N)$ be the set of $L \in S_d^{\backslash Z}(N)$ whose projection on N/Z is H. Let $S_d[N/Z]$ be the set of $H \in S_d(N/Z)$ for which $S_d^{(Z,H)}(N) \neq \varnothing$.

Let $H \in S_d[N/Z]$. Then we obtain $\#S_d^{(Z,H)}(N) \leq \#H^1(H, Z) = \#\,\mathrm{Hom}(H^{\mathrm{ab},p}, Z)$, where $(-)^{\mathrm{ab},p}$ denotes $(-)/((-)^p[(-),(-)])$. Moreover, let H' be a subgroup of A of order d and $Z' \cong \mathbb{Z}/p\mathbb{Z}$ a subgroup of A of order p. Then we have

$$\#\,\mathrm{Hom}(H^{\mathrm{ab},p}, Z) \leq \#\,\mathrm{Hom}((H')^{\mathrm{ab},p}, Z').$$

If $d = 1$, the lemma is trivial. Then we may assume that p divides d. We have

$$\begin{aligned}
\#S_d(N) &= \#S_d^Z(N) + \#S_d^{\backslash Z}(N) = \#S_{d/p}(N/Z) + \#S_d^{\backslash Z}(N)\\
&= \#S_{d/p}(N/Z) + \sum_{H \in S_d[N/Z]} \#S_d^{(Z,H)}(N)\\
&\leq \#S_{d/p}(N/Z) + \sum_{H \in S_d[N/Z]} \#(\mathrm{Hom}(H^{\mathrm{ab},p}, Z))\\
&\leq \#S_{d/p}(N/Z) + \#S_d(N/Z)\#(\mathrm{Hom}((H')^{\mathrm{ab},p}, Z'))
\end{aligned}$$

By induction, we have $\#S_{d/p}(N/Z) \leq \#S_{d/p}(A/Z')$ and $\#S_d(N/Z) \leq \#S_d(A/Z')$. Moreover, we have

$$\begin{aligned}\#S_d(A) &= \#S_{d/p}(A/Z') + \sum_{H' \in S_d[A/Z']} \#S_d^{(Z',H')}(A) \\ &= \#S_{d/p}(A/Z') + \sum_{H' \in S_d[A/Z']} \#(\mathrm{Hom}((H')^{\mathrm{ab},p}, Z')) \\ &= \#S_{d/p}(A/Z') + \#S_d(A/Z')\#(\mathrm{Hom}((H')^{\mathrm{ab},p}, Z')).\end{aligned}$$

Thus, we obtain

$$\#S_d(N) \leq \#S_d(A).$$

This completes the proof of the lemma. □

4F. We have the following result.

Theorem 4.3. *We maintain the settings introduced in Section 1C1. Let G be a finite p-group, and let $f : \mathscr{Y} \to \mathscr{X}$ be a G-semistable covering (i.e., $D_X = \varnothing$, see Definition 1.5) over S and $x \in \mathscr{X}_s$ a vertical point (Definition 1.8) associated to f. Suppose that $f^{-1}(x)$ is connected, and that G is an abelian p-group. Then we have (see Section 4D for $M(G)$, $B(\#G)$)*

$$\sigma(f^{-1}(x)) \leq M(G)\#G - 1 \leq B(\#G)\#G - 1.$$

In particular, if G is an abelian p-group, then the p-rank $\sigma(f^{-1}(x))$ can be bounded by a constant $B(\#G)$ which depends only on $\#G$.

Proof. If x is a smooth point of the special fiber $\mathscr{X}_s$ of $\mathscr{X}$, then $\sigma(f^{-1}(x)) = 0$ (Theorem 1.9). Thus, we may assume that x is a singular point of $\mathscr{X}_s$.

If $\mathcal{I}(x) = \varnothing$ (Definition 3.5(b)), then Theorem 3.9 implies that $\sigma(f^{-1}(x)) = 0$. If $\mathcal{I}(x) \neq \varnothing$, by applying Theorem 3.9 and Proposition 4.1, we obtain

$$\sigma(f^{-1}(x)) = \sum_{I \in \#I \in \mathcal{I}(x)} \#G/\#I - \sum_{\#J \in \mathcal{J}(x)} \#G/\#J + 1 \leq \#\mathcal{I}\#G - 1 \leq M(G)\#G - 1 \leq B(\#G)\#G - 1. \quad \square$$

Remark 4.3.1. If G is a cyclic p-group, then by the definition of $M(G)$, we have $M(G) = 1$. Thus, if G is a cyclic p-group, we have $\sigma(f^{-1}(x)) \leq \#G - 1$. This is the main theorem of [Saïdi 1998a, Theorem 1].

Acknowledgements

Parts of the results of the present paper were obtained in April 2016. I would like to express my deepest gratitude to Prof. Michel Raynaud for his interest in this work, positive comments, and encouraging me to write this paper. It is with deep regret and sadness to hear of his passing. I would like to thank Prof. Qing Liu for helpful comments concerning Proposition 1.6 and Remark 1.6.1, and to thank the referees very much for carefully reading the manuscript and for giving me comments which substantially helped improving the quality of the paper. This research was supported by JSPS KAKENHI Grant Numbers 16J08847 and 20K14283.

References

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Math. (3) **21**, Springer, 1990. MR Zbl

[Crew 1984] R. M. Crew, "Étale p-covers in characteristic p", *Compositio Math.* **52**:1 (1984), 31–45. MR Zbl

[Knudsen 1983] F. F. Knudsen, "The projectivity of the moduli space of stable curves, II: The stacks $M_{g,n}$", *Math. Scand.* **52**:2 (1983), 161–199. MR Zbl

[Lepage 2013] E. Lepage, "Resolution of nonsingularities for Mumford curves", *Publ. Res. Inst. Math. Sci.* **49**:4 (2013), 861–891. MR Zbl

[Liu 2006] Q. Liu, "Stable reduction of finite covers of curves", *Compositio Math.* **142**:1 (2006), 101–118. MR Zbl

[Mochizuki 1996] S. Mochizuki, "The profinite Grothendieck conjecture for closed hyperbolic curves over number fields", *J. Math. Sci. Univ. Tokyo* **3**:3 (1996), 571–627. MR Zbl

[Mochizuki 2006] S. Mochizuki, "Semi-graphs of anabelioids", *Publ. Res. Inst. Math. Sci.* **42**:1 (2006), 221–322. MR Zbl

[Pop and Stix 2017] F. Pop and J. Stix, "Arithmetic in the fundamental group of a p-adic curve: on the p-adic section conjecture for curves", *J. Reine Angew. Math.* **725** (2017), 1–40. MR Zbl

[Raynaud 1990] M. Raynaud, "p-groupes et réduction semi-stable des courbes", pp. 179–197 in *The Grothendieck Festschrift*, vol. 3, edited by P. Cartier et al., Progr. Math. **88**, Birkhäuser, Boston, 1990. MR Zbl

[Saïdi 1998a] M. Saïdi, "p-rank and semi-stable reduction of curves", *C. R. Acad. Sci. Paris Sér. I Math.* **326**:1 (1998), 63–68. MR Zbl

[Saïdi 1998b] M. Saïdi, "p-rank and semi-stable reduction of curves, II", *Math. Ann.* **312**:4 (1998), 625–639. MR Zbl

[SGA 1 1971] A. Grothendieck, *Revêtements étales et groupe fondamental* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), Lecture Notes in Math. **224**, Springer, 1971. MR Zbl

[Stix 2002] J. Stix, *Projective anabelian curves in positive characteristic and descent theory for log-étale covers*, Ph.D. thesis, Friedrich-Wilhelms-Universität Bonn, 2002, available at https://www.math.uni-frankfurt.de/~stix/research/preprints/STIXdissB.pdf. MR Zbl

[Tamagawa 2004a] A. Tamagawa, "Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups", *J. Algebraic Geom.* **13**:4 (2004), 675–724. MR Zbl

[Tamagawa 2004b] A. Tamagawa, "Resolution of nonsingularities of families of curves", *Publ. Res. Inst. Math. Sci.* **40**:4 (2004), 1291–1336. MR Zbl

[Vidal 2001] I. Vidal, *Contributions à la cohomologie étale des schémas et des log-schémas*, Ph.D. thesis, Université Paris-Sud, 2001, available at https://www.theses.fr/2001PA112246.

[Yang 2018] Y. Yang, "On the admissible fundamental groups of curves over algebraically closed fields of characteristic $p > 0$", *Publ. Res. Inst. Math. Sci.* **54**:3 (2018), 649–678. MR Zbl

[Yang 2019] Y. Yang, "On the existence of non-finite coverings of stable curves over complete discrete valuation rings", *Math. J. Okayama Univ.* **61**:1 (2019), 1–18. MR Zbl

[Yang 2020] Y. Yang, "On the averages of generalized Hasse–Witt invariants of pointed stable curves in positive characteristic", *Math. Z.* **295**:1-2 (2020), 1–45. MR Zbl

Communicated by Antoine Chambert-Loir
Received 2022-04-18 Revised 2022-09-22 Accepted 2023-04-13

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

ALGEBRA AND NUMBER THEORY 18:2 (2024)
https://doi.org/10.2140/ant.2024.18.319

A deterministic algorithm for Harder–Narasimhan filtrations for representations of acyclic quivers

Chi-Yu Cheng

Let M be a representation of an acyclic quiver Q over an infinite field k. We establish a deterministic algorithm for computing the Harder–Narasimhan filtration of M. The algorithm is polynomial in the dimensions of M, the weights that induce the Harder–Narasimhan filtration of M, and the number of paths in Q. As a direct application, we also show that when k is algebraically closed and when M is unstable, the same algorithm produces Kempf's maximally destabilizing one parameter subgroups for M.

1. Introduction

Our goal in this paper is to provide a constructive approach to Harder–Narasimhan filtrations of representations of acyclic quivers. Specifically, we first establish in Theorem A a link between the Harder–Narasimhan filtration and the *discrepancy* of a representation. The later notion, introduced in [Chindris and Kline 2021], allows us to apply algebraic complexity tools to the study of Harder–Narasimhan filtrations of representations of acyclic quivers. The main result, Theorem 2 of [Chindris and Kline 2021] is a deterministic, polynomial time algorithm for finding witnesses to the discrepancies of representations of bipartite quivers. Huszar [2021, Proposition 3.5] then extended the result to acyclic quivers in Theorem 3.5 in our paper. Our first main result Theorem A affirms that for any representation, its Harder–Narasimhan filtration has a term that witnesses its discrepancy. So the next natural question to ask is that is there also a systematic way to compute Harder–Narasimhan filtrations? Combining Theorem 3.5 and Theorem A, we are able to establish a deterministic algorithm, Algorithm 1, in Theorem B that computes the Harder–Narasimhan filtration of a representation of an acyclic quiver. We would like to point out that Algorithm 1

MSC2020: 14L24, 14Q20, 16G20.
Keywords: geometric invariant theory, weight stability, slope stability, representation, quiver, Harder–Narasimhan filtration, discrepancy.

is not polynomial in the number of edges of the quiver, but in the number of paths (see Theorem 3.7). When the quiver is bipartite where arrows only go from one partition to the other, the number of arrows equals that of the paths. In this case Algorithm 1 indeed has polynomial time complexity.

This paper was originally motivated by the relations between "maximally destabilizing subobjects" under different stability conditions in the case of representations of quivers. Stability plays an important role in algebraic geometry for constructing moduli spaces of algebro-geometric objects. In the case of representations of quivers, two commonly used stability conditions are weight stability and slope stability. We now briefly introduce the two stability conditions, and we shall see that failing either one of them would require some subobject that contradicts the condition. We let Q be an acyclic quiver.[†] That is, Q does not have an oriented cycle, and we let Q_0 denote the set of vertices of Q.

Weight stability was formulated in [King 1994] to construct moduli of representations of finite dimensional algebras. King considered representations of Q of a fixed dimension $\boldsymbol{d} \in \mathbb{N}^{Q_0}$, and a $\mathbb{Z}$-linear weight function $\theta : \mathbb{Z}^{Q_0} \to \mathbb{Z}$ such that $\theta(\boldsymbol{d}) = 0$. For a representation M of Q, we let $\dim M \in \mathbb{N}^{Q_0}$ be its dimension vector. By $\theta(M)$ we mean $\theta(\dim M)$. King defined that for a representation M of dimension $\boldsymbol{d}$, M is *θ-semistable* if and only if $\theta(M') \leq \theta(M) = 0$ for every subrepresentation M' of M. Otherwise, M is *θ-unstable*. Namely, there is a subrepresentation M' of M such that $\theta(M') > 0$. In [Chindris and Kline 2021], the *discrepancy* of any representation M *with respect to* θ is defined to be the number

$$\operatorname{disc}(M, \theta) = \max_{M' \subseteq M} \theta(M'),$$

where $M' \subseteq M$ means M' is a subrepresentation of M. We see that if M is θ-unstable, then the subrepresentation that witnesses $\operatorname{disc}(M, \theta)$ contradicts θ-semistability of M the most.

On the other hand, weight stability is in fact a reinterpretation of the Hilbert–Mumford criterion Theorem 4.3. When M is θ-unstable, the original Hilbert–Mumford criterion states that there is a one parameter subgroup (of the group to be defined in Section 4B) that contradicts θ-semistability for M. Kempf [1978] showed that among all destabilizing one parameter subgroups, there is a unique indivisible one, up to conjugation by a parabolic subgroup, that maximally contradicts θ-semistability in the numerical sense that will be made precise in Section 4. The maximally destabilizing one parameter subgroups of an unstable representation induce a unique filtration, which was referred to as Kempf filtration in [Zamora 2014]. The other type of filtration, known as the Harder–Narasimhan filtration, comes from slope instability.

Slope stability depends on two weights $\Theta, \kappa : \mathbb{Z}^{Q_0} \to \mathbb{Z}$, where $\kappa((\mathbb{Z}^+)^{Q_0}) > 0$. The slope μ of a nonzero representation M is defined as

$$\mu(M) = \frac{\Theta(M)}{\kappa(M)}.$$

[†] The assumption that the quiver is acyclic is not required to define either stability condition. Nevertheless, we will stick to acyclic quivers throughout the paper for consistency, as the algorithm deals with acyclic quivers only.

Unlike weight stability, slope stability is defined for any nonzero representation, whether its slope is zero or not. In [Hille and de la Peña 2002], a nonzero representation M is said to be μ-semistable if $\mu(M') \leq \mu(M)$ for all $0 \neq M' \subseteq M$. In Section 2, we recall in Lemma 2.7 a way to go between weight and slope stability. In any case, we shall stick to the following convention throughout the paper, whose convenience will become apparent later: If a statement only involves weight stability, we shall use the lower case θ as the weight. When slope stability is involved, we use the upper case Θ as the numerator of the slope.

The Harder–Narasimhan filtration of a representation M with respect to μ is constructed inductively in [Hille and de la Peña 2002]. As the first step, set M_1 as the unique subrepresentation that is maximal among all subrepresentations having the highest slope. Such a subrepresentation is called the *strongly contradicting semistability* (abbreviated as scss) *subrepresentation of M*. One then goes on to set M_{i+1}/M_i as the scss subrepresentation of M/M_i until M/M_i is μ-semistable. The resulting filtration $0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$ is called the *Harder–Narasimhan filtration* of M.

We now have the following maximally destabilizing subobjects associated to an unstable representation M:

(1) The discrepancy of M, and its witnessing subrepresentations (not necessarily unique).

(2) The scss subrepresentation of M, and the Harder–Narasimhan filtration of M.

(3) The one parameter subgroups that maximally contradict the semistability of M, and the Kempf filtration induced by those one parameter subgroups.

The relation between (2) and (3) is already unraveled by the paper [Zamora 2014]. The main result is that for an unstable representation, its Harder–Narasimhan filtration coincides with its Kempf filtration. The first of our two main results Theorem A establishes a link between (1) and (2). The second main result Theorem B establishes a deterministic algorithm Algorithm 1 for computing the Harder–Narasimhan filtration and therefore the maximally destabilizing one parameter subgroups of any unstable representation.

1A. *The main results.*

We let Q be an acyclic quiver.

Theorem A (Lemma 3.1, Theorem 3.3, Corollary 3.4). *Let Θ be a weight and let M be a representation of Q with $\Theta(M) = 0$. For any weight κ with $\kappa((\mathbb{Z}^+)^{Q_0}) > 0$, if $\mu = \Theta/\kappa$ is the slope function, then any subrepresentation M' with $\Theta(M') = \operatorname{disc}(M, \Theta)$ contains the scss subrepresentation of M (with respect to μ). Moreover, if*

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{r-1} \subsetneq M_r = M$$

is the Harder–Narasimhan filtration of M (with respect to μ), then there is an M_l in the filtration such that $\Theta(M_l) = \operatorname{disc}(M, \Theta)$.

It is noteworthy that the discrepancy depends only on Θ, but the Harder–Narasimhan filtration depends on μ, which has an extra piece κ. While the Harder–Narasimhan filtration of M may change due to different choices of κ, the results of Theorem A are independent of κ for a fixed Θ.

Theorem B (Theorems 3.7 and 4.6). *Let M be a representation of Q over an infinite field. There exists a deterministic algorithm to compute the Harder–Narasimhan filtration of M. When the ground field is algebraically closed and when M is unstable, a maximally destabilizing one parameter subgroup for M can be constructed based on its Harder–Narasimhan filtration. Hence the algorithm also produces a maximally destabilizing one parameter subgroup for M. Moreover, in the case that Q is bipartite where all arrows go from one partite to the other, the algorithm has polynomial time complexity.*

Theorem B is inviting for several purposes. First, finding Kempf's maximally destabilizing one parameter subgroups in general is very hard. Roughly speaking, suppose V is a representation of a reductive group G. If G is a torus, then finding Kempf's one parameter subgroup for an unstable point $v \in V$ is done by linear programming, whose constraints come from the states of v. For a general reductive group, one can first restrict the action to a maximal torus, then conduct linear programming on the entire orbit $G \cdot v$. The set of states of all points in the orbit can be as large as the power set of $\{1, 2, \ldots, \dim V\}$, minus the empty subset. Hence the time complexity to compute Kempf's one parameter subgroups using brute force is exponential. Theorem B provides an alternative to brute force for finding Kempf's one parameter subgroups in the context of representations of acyclic quivers. In addition, if the quiver is bipartite as stated in Theorem B, the algorithm has polynomial time complexity.

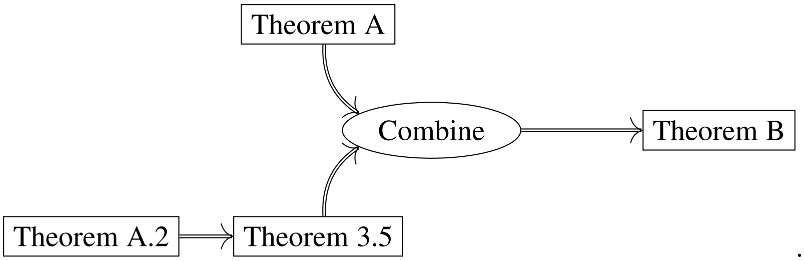
Second, Hoskins [2014] shows that the stratification of the space of representations of a quiver of a fixed dimension by Harder–Narasimhan types coincides with the stratification by Kempf's one parameter subgroups. Hence Theorem B sheds new light on computing the stratification by either type.

1B. ***Outline of the paper.*** We briefly recall slope stability Definition 2.1, weight stability Definition 2.5, and a way to go between the two Lemma 2.7 in Section 2. In Section 3, we establish Theorem A (Lemma 3.1, Theorem 3.3, Corollary 3.4) and the first part of Theorem B (Theorem 3.7). Specifically the first part of Theorem B constructs Algorithm 1, and calculates its complexity. The second part of Theorem B constructs maximally destabilizing one parameter subgroups for unstable representations from their Harder–Narasimhan filtrations. Due to the technicality involved in invariant theory, we postpone the second part of Theorem B to Section 4.

In Section 4A, we recall the Hilbert–Mumford criterion Theorem 4.3, and define maximally destabilizing one parameter subgroups Definition 4.4. We also present Kempf's main result, our Theorem 4.5, from the paper [Kempf 1978]. Theorem 4.5 describes the existence and the uniqueness of maximally destabilizing one parameter subgroups. We then apply the machinery to the case of representation of quivers at Section 4B. Finally, we are able to finish the second part of Theorem B in Theorem 4.6.

In Section 5, we construct an unstable representation to showcase that not all subrepresentations that witness the discrepancy occur in the Harder–Narasimhan filtration. We also provide two approaches to compute its maximally destabilizing one parameter subgroups. The first one uses Theorem B and the second one is the brute force procedure that can be applied to any representation of any reductive group. Although the second approach works in more generality, the cost will be apparent in the example. The point is to give the readers an idea of the hardness of finding maximally destabilizing one parameter subgroups and the value of Theorem B.

We note that our Algorithm 1 relies on Theorem 3.5, which is an algorithm that computes discrepancies and was established in [Huszar 2021]. Theorem 3.5 in turn is a consequence of [Ivanyos et al. 2018, Theorem 1.5], our Theorem A.2. We supply an almost self-contained account of how Theorem 3.5 is established based on Theorem A.2 in the Appendix. Although this was the work of [2021], we intend to fill in some details not supplied in the original paper. Here is a visualization of the logical dependency of the results in our paper:



Finally, we will work with an arbitrary ground field throughout Sections 2 and 3 until Theorem 3.5. Originally, the machinery of Theorem 3.5 only requires the ground field to have *enough* elements. For simplicity we will work with an infinite field, starting from Theorem 3.5. In Section 4, we will assume further that the ground field is algebraically closed for the formulation of Kempf's maximally destabilizing one parameter subgroups.

2. Stability conditions for representations of quivers

In this section we recall slope stability (Definition 2.1) and weight stability (Definition 2.5) for representations of quivers.

Weight stability defined in this section is originally the Hilbert–Mumford criterion (Theorem 4.3) formulated in [King 1994] in the context of representations of quivers. For the purpose of the exposition of this paper, we postpone a more detailed account of weight stability to Section 4. At the end of this section we recall in Lemma 2.7 a way to translate between slope stability and weight stability.

2A. ***Set up.*** Let k be a field, not necessarily algebraically closed. A quiver $Q = (Q_0, Q_1, t, h)$ consists of Q_0 (vertices) and Q_1 (arrows) together with two maps $t, h : Q_1 \to Q_0$. The image of an arrow under t (resp. h) is the tail (resp. head) of the arrow. We represent Q as a directed graph with vertices Q_0 and directed arrows $a : ta \to ha$ for $a \in Q_1$. A *path* in Q is a composition of arrows in Q. We give each vertex v the trivial arrow $e_v : v \to v$. For any path $p : x \to v$ (resp. $q : v \to y$), we set $e_v p = p$ (resp. $q e_v = q$). We let Q be a finite acyclic quiver throughout the paper. That is, both Q_0 and Q_1 are finite, and Q does not have any oriented cycle other than the self-loops $\{e_v\}_{v \in Q_0}$. In this way, the number of paths in Q is finite.

A representation M of Q consists of a collection of finite dimensional k-vector spaces M_v, for each $v \in Q_0$ together with a collection of k-linear maps $M(a) : M_{ta} \to M_{ha}$, for each $a \in Q_1$. For each $v \in Q_0$, we set $M(e_v) : M_v \to M_v$ to be the identity map.

If M, N are two representations of Q, then a morphism from M to N is a collection of k-linear maps $\varphi_v : M_v \to N_v$ for each $v \in Q_0$, such that $N(a)\varphi_{ta} = \varphi_{ha} M(a)$ for each $a \in Q_1$. In particular, M' is a subrepresentation of M whenever each M'_v is a subspace of M_v and each $M'(a)$ is the restriction of $M(a)$ to M'_{ta}. We will write $M' \subseteq M$ if M' is a subrepresentation of M. We also note that the collection of representations of Q forms an abelian category.

The dimension vector of a representation M of Q is the tuple $\dim M \in \mathbb{Z}^{Q_0}$ where $(\dim M)_v = \dim M_v$ as a k-vector space for each $v \in Q_0$. A *weight* is a $\mathbb{Z}$-linear function $\mathbb{Z}^{Q_0} \to \mathbb{Z}$. If θ is a weight, we write $\theta(\dim M)$ as $\theta(M)$.

For clarity, below is a summary of some important notations that we stick to throughout the paper:

Notation. Let M be a representation of Q. For each vertex $v \in Q_0$, we write M_v as the vector space of M at v. For each $a \in Q_1$, $M(a)$ denotes the map $M_{ta} \to M_{ha}$ that is part of the data of M. For any weight $\theta : \mathbb{Z}^{Q_0} \to \mathbb{Z}$, $\theta(v)$ instead of θ_v is the weight of θ at v. We also decree that $\theta(M)$ means $\sum_{v \in Q_0} \theta(v) \dim M_v$. For a dimension vector $\boldsymbol{d} \in \mathbb{Z}^{Q_0}$, we write $\boldsymbol{d}_v$ instead of $\boldsymbol{d}(v)$ for its component at v.

2B. ***Slope stability.*** In this section we recall semistability of representations of quivers with respect to a slope, along with some important properties stated in Lemmas 2.2 and 2.3. We then recall the construction from [Hille and de la Peña 2002] of the Harder–Narasimhan filtration of a representation in Theorem 2.4. These results will be widely used at Section 3.

Fix two weights $\Theta, \kappa : \mathbb{Z}^{Q_0} \to \mathbb{Z}$ where we require $\kappa((\mathbb{Z}^+)^{Q_0}) > 0$. We set $\mu(M) = \Theta(M)/\kappa(M)$ for any nonzero representation M. We implicitly assume that a representation is nonzero whenever the slope function is applied to it.

Definition 2.1. We say a representation M of Q is *μ-semistable* if $\mu(N) \le \mu(M)$ for every subrepresentation N of M.

Lemma 2.2 [Hille and de la Peña 2002, Lemma 2.1]. *Let* $0 \to L \to M \to N \to 0$ *be a short exact sequence of representations of Q. Then the following conditions are equivalent*:

(1) $\mu(L) \le \mu(M)$.

(2) $\mu(L) \le \mu(N)$.

(3) $\mu(M) \le \mu(N)$.

A fundamental result is the following:

Lemma 2.3 [Hille and de la Peña 2002, Lemma 2.2]. *Let M be a representation of Q. There is a unique subrepresentation N such that*

(1) *$\mu(N)$ is maximal among subrepresentations of M, and*

(2) *if $\mu(N') = \mu(N)$, then $N' \subseteq N$.*

We call such a representation N the *strongly contradicting semistability* (abbreviated as scss) *subrepresentation of M*.

Theorem 2.4 [Hille and de la Peña 2002, Theorem 2.5]. *Let M be a representation of Q. There is a unique filtration $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{r-1} \subsetneq M_r = M$ such that*

(1) $\mu(M_i/M_{i-1}) > \mu(M_{i+1}/M_i)$ *for* $i = 1, \ldots, r-1$,

(2) *the representation M_i/M_{i-1} is μ-semistable for $i = 1, \ldots, r$.*

The above filtration is called the *Harder–Narasimhan filtration of M*. It is constructed by setting M_1 to be the scss subrepresentation of M, then by inductively setting M_{i+1}/M_i as the scss subrepresentation of M/M_i until M/M_i is μ-semistable.

2C. *Weight stability.* Another stability condition on representations of quivers comes from GIT and was introduced in [King 1994]. Like the slope stability we introduced earlier, GIT stability also depends on a choice of parameters. In the case of representations of quivers the parameter is a single weight. We therefore refer to this stability condition as weight stability. We will relate weight and slope stability in Lemma 2.7 at the end of this section.

Definition 2.5. Let $\boldsymbol{d} \in \mathbb{Z}^{Q_0}$ be a dimension vector and let θ be a weight with $\theta(\boldsymbol{d}) = 0$. A representation M with dimension vector $\boldsymbol{d}$ is *θ-semistable* if $\theta(N) \leq 0$ for all subrepresentations $N \subseteq M$.

The notion of *discrepancy* was introduced in [Chindris and Kline 2021] to describe the subrepresentations that contradict the weight stability the most. This very notion allows us to compute the Harder–Narasimhan filtrations of representations of an acyclic quiver using tools from algebraic complexity, as we shall see in Section 3.

Definition 2.6. Let M be a representation and let θ be a weight. We do not require $\theta(M) = 0$. The *discrepancy of M with respect to θ* is defined as

$$\operatorname{disc}(M, \theta) = \max_{N \subseteq M} \theta(N).$$

We say a subrepresentation N is *θ-optimal in M*, or N *witnesses* $\operatorname{disc}(M, \theta)$ if $\theta(N) = \operatorname{disc}(M, \theta)$.

We recall the following way to go between weight stability and slope stability.

Lemma 2.7. *Let Θ and κ be two weights with $\kappa(N) > 0$ for every nonzero representation N. Let μ be the corresponding slope Θ/κ. For every dimension vector $\boldsymbol{d} \in \mathbb{Z}^{Q_0}$, define the new weight*

$$\theta_{\boldsymbol{d}}(N) := \kappa(\boldsymbol{d})\Theta(N) - \Theta(\boldsymbol{d})\kappa(N) \quad \textit{for each } N.$$

Then a representation M of dimension $\boldsymbol{d}$ is μ-semistable if and only if M is $\theta_{\boldsymbol{d}}$-semistable. Moreover, the new slope $\mu_{\boldsymbol{d}} = \theta_{\boldsymbol{d}}/\kappa$ defines the same slope stability condition so that the Harder–Narasimhan filtrations of a representation with respect to μ and $\mu_{\boldsymbol{d}}$ coincide.

Proof. Let M be a representation of dimension $\boldsymbol{d}$ and let $N \subset M$ be any subrepresentation. We then have

$$\mu(N) = \frac{\Theta(N)}{\kappa(N)} \leq \mu(M) = \frac{\Theta(\boldsymbol{d})}{\kappa(\boldsymbol{d})} \Leftrightarrow \kappa(\boldsymbol{d})\Theta(N) - \Theta(\boldsymbol{d})\kappa(N) = \theta_{\boldsymbol{d}}(N) \leq 0$$

The first statement follows.

For the second statement, simply note that

$$\mu_{\boldsymbol{d}}(N) = \kappa(\boldsymbol{d}) \cdot \mu(N) - \Theta(\boldsymbol{d}).$$

Hence $\mu_{\boldsymbol{d}}$ is a positive scalar multiple of μ, followed by a translation. □

3. The main results

Fix an acyclic quiver Q. In this section we prove two major results: Theorems 3.3 and 3.7. Theorem 3.3 provides a sufficient condition for the Harder–Narasimhan filtration of a representation of Q to contain a term that witnesses the discrepancy. We then propose Algorithm 1 to compute the Harder–Narasimhan filtrations of representations of Q. The correctness of Algorithm 1 is ensured by Proposition 3.6. We also recall the algebraic complexity machinery Theorem 3.5 derived from [Ivanyos et al. 2018]. With the aid of Theorem 3.5, we establish in Theorem 3.7 the time complexity of Algorithm 1. The derivation of Theorem 3.5 is supplied in the Appendix for interested readers.

We fix two weights Θ, κ on $\mathbb{Z}^{Q_0}$ where $\kappa(N) > 0$ for each nonzero representation N. We let $\mu = \Theta/\kappa$ be the slope. We do not assume anything about the ground field until Theorem 3.5, where we will begin to assume the ground field is infinite.

We now present Lemma 3.1, which is the cornerstone of this paper.

Lemma 3.1. *Let M be a μ-unstable representation, and let M_1 be the scss subrepresentation of M. Suppose $\Theta(M_1) > 0$ and M' is Θ-optimal in M. Then M' contains M_1. Moreover, M' is μ-semistable if and only if $M' = M_1$.*

Proof. Note that $\Theta(M_1) > 0$ implies $\operatorname{disc}(M, \Theta) = \Theta(M') > 0$. Suppose on the contrary that $M_1 \not\subset M'$. We then have a proper inclusion $M' \subsetneq M_1 + M'$. In particular, $\kappa(M') < \kappa(M_1 + M')$. On the other hand, $\Theta(M') \geq \Theta(M_1 + M')$ as M' attains the discrepancy. If $\Theta(M_1 + M') \leq 0$, we automatically have $\mu(M') > \mu(M_1 + M')$. If $\Theta(M_1 + M') > 0$, we have

$$\frac{\Theta(M')}{\kappa(M')} \geq \frac{\Theta(M_1 + M')}{\kappa(M')} > \frac{\Theta(M_1 + M')}{\kappa(M_1 + M')}.$$

In any case we deduce that $\mu(M') > \mu(M_1 + M')$. By Lemma 2.2, the following short exact sequence

$$0 \to M' \to M_1 + M' \to (M_1 + M')/M' \simeq M_1/(M_1 \cap M') \to 0$$

implies $\mu(M') > \mu(M_1 + M') > \mu(M_1/(M_1 \cap M'))$.

On the other hand, since M_1 is the scss subrepresentation of M, we have $\mu(M_1 \cap M') \leq \mu(M_1)$. Now Lemma 2.2 applied to the following short exact sequence

$$0 \to M_1 \cap M' \to M_1 \to M_1/(M_1 \cap M') \to 0$$

implies $\mu(M_1/(M_1 \cap M')) \geq \mu(M_1)$. In sum, we obtained

$$\mu(M') > \mu(M_1 + M') > \mu(M_1/(M_1 \cap M')) \geq \mu(M_1).$$

However, M_1 is the scss subrepresentation of M. We arrive at a contradiction.

For the second implication of the lemma, if M' is the scss subrepresentation of M, it is obviously μ-semistable. Conversely, if M' is μ-semistable, since it contains M_1, we must have $\mu(M_1) \leq \mu(M')$. This implies $\mu(M_1) = \mu(M')$ so that $M' = M_1$. □

Now we can make sense of the following proposition.

Proposition 3.2. *Let M be a μ-unstable representation, and let M_1 be the scss subrepresentation of M with $\Theta(M_1) > 0$. If M' is Θ-optimal in M, we then have*

$$\Theta(M'/M_1) = \operatorname{disc}(M/M_1, \Theta).$$

Namely, M'/M_1 is Θ-optimal in M/M_1.

Proof. Suppose N/M_1 is Θ-optimal in M/M_1. We then obviously have

$$\Theta(M'/M_1) \leq \operatorname{disc}(M/M_1, \Theta) = \Theta(N/M_1).$$

This is equivalent to $\Theta(M') \leq \Theta(N)$. However, M' is Θ-optimal in M by assumption. So we must have $\Theta(M') = \Theta(N)$, resulting in $\Theta(M'/M_1) = \Theta(N/M_1) = \operatorname{disc}(M/M_1, \Theta)$. The proposition is proved. □

Theorem 3.3. *Let M be a μ-unstable representation and let*

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{r-1} \subsetneq M_r = M$$

be its Harder–Narasimhan filtration. Suppose there is an integer l such that $\mu(M_l/M_{l-1}) > 0$ but $\mu(M_{l+1}/M_l) \leq 0$. Then the term M_l in the filtration is Θ-optimal in M. In addition, M_l has the highest slope among all Θ-optimal subrepresentations.

Proof. We will prove the theorem by induction on l. Let $l = 1$. We need to show that $\Theta(M_1) \geq \Theta(M')$ for every $M' \subset M$. We break this down into several steps:

1. For any $M_1' \subset M_1$, we show that $\Theta(M_1') \leq \Theta(M_1)$.
2. Next, assuming on the contrary that there is an $M' \subset M$ with $\Theta(M') > \Theta(M_1)$, we prove that such an M' induces the proper inclusion $M_1 \subsetneq M_1 + M'$.
3. Finally, we deduce from steps (1) and (2) that $\mu((M_1 + M')/M_1) > \mu(M_2/M_1)$, contradicting the fact that M_2/M_1 is the scss subrepresentation of M/M_1.

For step (1), suppose on the contrary that there is an $M_1' \subsetneq M_1$ such that $\Theta(M_1') > \Theta(M_1)$. We would then have

$$\mu(M_1') = \frac{\Theta(M_1')}{\kappa(M_1')} > \frac{\Theta(M_1)}{\kappa(M_1')} > \frac{\Theta(M_1)}{\kappa(M_1)} = \mu(M_1).$$

Note that again we are using the assumption that $\Theta(M_1)$ is positive. Since M_1 is the scss subrepresentation of M, we arrive at a contradiction. Step (1) is completed.

For step (2), since M_1 is scss in M, we get $\mu(M') \leq \mu(M_1)$. This together with the assumption that $\Theta(M') > \Theta(M_1)$ imply $\kappa(M') > \kappa(M_1)$. This clearly implies that M' is not contained in M_1 so that $M_1 \subsetneq M_1 + M'$, finishing step (2).

For step (3), simply note that $\Theta(M') > \Theta(M_1) \geq \Theta(M_1 \cap M')$ by step (1). We then have

$$\mu((M_1 + M')/M_1) = \mu(M'/(M_1 \cap M')) = \frac{\Theta(M') - \Theta(M_1 \cap M')}{\kappa(M') - \kappa(M_1 \cap M')} > 0 \geq \mu(M_2/M_1).$$

These complete all three steps and therefore the base case of the induction.

If $\mu(M_{l+1}/M_l) > 0$ but $\mu(M_{l+2}/M_{l+1}) \leq 0$, consider the Harder–Narasimhan filtration for M/M_1:

$$0 \subsetneq M_2/M_1 \subsetneq \cdots \subsetneq M/M_1.$$

By the induction hypothesis, $\Theta(M_{l+1}/M_1) = \operatorname{disc}(M/M_1, \theta)$. Moreover, Proposition 3.2 implies $\operatorname{disc}(M/M_1, \Theta) = \operatorname{disc}(M, \Theta) - \Theta(M_1)$. Combining these two, we get $\Theta(M_{l+1}) = \operatorname{disc}(M, \Theta)$, as desired.

Finally, the maximality of slope of M_l can also be proved by induction on l, together with Lemma 3.1. □

Corollary 3.4. *Suppose M is a μ-unstable representation of Q, and $\Theta(M) = 0$. Then there exists a term M_i in the Harder–Narasimhan filtration of M such that $\Theta(M_i) = \operatorname{disc}(M, \Theta)$, and such that M_i has the highest slope among all subrepresentations of M that witness* $\operatorname{disc}(M, \Theta)$.

Proof. Let $0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$ be the Harder–Narasimhan filtration of M. The integer l described in Theorem 3.3 must exist. For if this is not the case, we then have

$$0 = \Theta(M) > \Theta(M_{r-1}) > \cdots > \Theta(M_1) > 0,$$

which is absurd. □

We now turn our attention to the computation of Harder–Narasimhan filtrations for representations of Q. This comes down to computing the scss subrepresentation. The main ideas come from Lemma 3.1, and the following machinery that works for arbitrary infinite fields.

Theorem 3.5. *Let Q be an acylcic quiver and let M be a representation of Q over an infinite field. Fix a weight $\theta : \mathbb{Z}^{Q_0} \to \mathbb{Z}$ with $\theta(M) = 0$. There is a deterministic algorithm that finds the discrepancy* $\operatorname{disc}(M, \theta)$, *together with a subrepresentation M' so that $\theta(M') = \operatorname{disc}(M, \theta)$. If we set $\Omega = \sum_{v \in Q_0} |\theta(v)|$, $K = \sum_{v \in Q_0} \dim M_v$, and P as the number of paths in Q, then the algorithm has run time complexity that is polynomial in Ω, K, P.*

We refer interested readers to the Appendix for a proof of the theorem. It is presented at Corollary A.8. We now explain how Lemma 3.1, together with the algorithm of Theorem 3.5 can be applied for deriving the scss subrepresentation. For convenience, we adopt the following notations.

Notation. For any representation M of Q of dimension $\boldsymbol{d}$, $F(M)$ denotes the output subrepresentation of the algorithm in Theorem 3.5 applied to M and to the weight $\theta_{\boldsymbol{d}}$. We let $G(M) = \operatorname{disc}(M, \theta_{\boldsymbol{d}}) = \theta_{\boldsymbol{d}}(F(M))$.

As a first instance of the convenience of notations just introduced, we can say a representation M is μ-semistable (resp. μ-unstable) if and only if $G(M) = 0$ (resp. $G(M) > 0$) (see Lemma 2.7).

Now let $M = M^0$ be a representation of Q. If $G(M^0) = 0$, then M^0 itself is the scss subrepresentation. Otherwise, let $M^1 = F(M^0)$. Lemma 3.1 then dictates that $G(M^1) = 0$ if and only if M^1 is the scss subrepresentation of M. If $G(M^1) > 0$, then $M^2 = F(M^1)$ is a proper subrepresentation of M^1. We continue to produce $M^i = F(M^{i-1})$ if $G(M^{i-1}) > 0$. The procedure must end in a finite number of steps as M is finite dimensional at each vertex, and each M^i is a proper subrepresentation of M^{i-1}. At the end, we have a filtration

$$0 \subsetneq M^r \subsetneq M^{r-1} \subsetneq \cdots \subsetneq M^1 \subsetneq M^0,$$

where

(1) $\theta_{\boldsymbol{d}_{i-1}}(M^i) > 0$,

(2) M^i is $\theta_{\boldsymbol{d}_{i-1}}$-optimal in M^{i-1}, and

(3) M^r is μ-semistable.

The following proposition ensures that in this case M^r is the scss subrepresentation of M.

Proposition 3.6. *Let* $0 \subsetneq M^r \subsetneq \ldots \subsetneq M^0$ *be a filtration of representations of* Q *and let* $\dim M^i = \boldsymbol{d}_i \in \mathbb{Z}^{Q_0}$. *Suppose for each* i,

$$\theta_{\boldsymbol{d}_{i-1}}(M^i) = \operatorname{disc}(M^{i-1}, \theta_{\boldsymbol{d}_{i-1}}) > 0.$$

Then M^r *is* μ*-semistable if and only if* M^r *is the scss subrepresentation of* M^i *for* $i = 0, \ldots, r-1$.

Proof. The if part is trivial. The proof for the only if part can be carried out by induction. We let M_1^i be the scss subrepresentation of M^i. Suppose M^r is μ-semistable. Then Lemma 3.1 (applied to $\theta_{\boldsymbol{d}_{r-1}}$) implies $M^r = M_1^{r-1}$. Now suppose $M^r = M_1^i$, we will show that $M^r = M_1^{i-1}$. For this, since M^i is $\theta_{\boldsymbol{d}_{i-1}}$-optimal in M^{i-1}, Lemma 3.1 implies M^i contains M_1^{i-1}. This immediately implies $M_1^{i-1} = M_1^i$. By the induction hypothesis, $M^r = M_1^i$ so that $M^r = M_1^{i-1}$, finishing the induction. □

We therefore propose the following algorithm to compute the Harder–Narasimhan filtration of a representation of an acyclic quiver. The outer while loop tests at each i-th step if M/M_i is μ-semistable. If not, the inner while loop then computes the scss subrepresentation M_{i+1}/M_i of M/M_i. The correctness of the inner loop is established by Proposition 3.6. In the end of the algorithm we have M_1, $M_2/M_1, \ldots, M/M_{r-1}$ for some $r \geq 1$, where each M_{i+1}/M_i is the scss subrepresentation of M/M_{i+1}, and M/M_{r-1} is μ-semistable. From these the Harder–Narasimhan filtration for M is immediate.

We now show that the above algorithm satisfies the complexity bound given in Theorem 3.5.

Algorithm 1: An algorithm for Harder–Narasimhan filtrations

```
Input  : A Representation $M$ of $Q$
Output : The Harder–Narasimhan filtration of $M$
if $G(M) = 0$ then
    return $M$    /* In this case $M$ is semistable, so the filtration is $M$ itself. */
end if
while $G(M) > 0$ do
    $N \leftarrow F(M)$
    while $G(N) > 0$ do
        $N \leftarrow F(N)$
    end while
    Record $N$                       /* $N$ is the scss subrepresentation of $M$ */
    Compute $M/N$
    $M \leftarrow M/N$
end while
```

Theorem 3.7. *Let Q be an acyclic quiver and let M be a representation of Q over an infinite field. Let $\Theta, \kappa : \mathbb{Z}^{Q_0} \to \mathbb{Z}$ be two weights that define the slope $\mu = \Theta/\kappa$, P be the number of paths in Q, $\Omega = \sum_v |\Theta(v)|$, and let $K = \kappa(M)$. Algorithm 1 constructs the Harder–Narasimhan filtration of M within time complexity that is polynomial in Ω, K, and P.*

Note that this is only the first part of Theorem B. We postpone the precise statement and the proof of the second part to Theorem 4.6 at the end of the next section.

Proof of Theorem 3.7. For starters, in the i-th outer while loop of Algorithm 1 (i starts from 0), the first line uses the algorithm of Theorem 3.5 to test μ-stability of M/M_i. Let $\boldsymbol{d}^i$ be the dimension vector for the quotient M/M_i. Theorem 3.5 states that the time complexity to determine stability of M/M_i is polynomial in $\sum_v |\theta_{\boldsymbol{d}^i}(v)|$, $\sum_v \dim(M/M_i)_v$, and P. Obviously the second term is bounded by K. To bound the first term by a polynomial in Ω and K, we first note that

$$|\Theta(M/M_i)| \leq \sum_v |\Theta(v)| \dim(M/M_i)_v \leq \Omega K.$$

Therefore

$$\begin{aligned}\sum_v |\theta_{\boldsymbol{d}^i}(v)| &= \sum_v |\kappa(M/M_i)\Theta(v) - \Theta(M/M_i)\kappa(v)| \\ &\leq \sum_v \kappa(M/M_i)|\Theta(v)| + |\Theta(M/M_i)|\kappa(v) \\ &\leq \Omega K + \Omega K^2.\end{aligned}$$

Hence, the first line of Algorithm 1 in the outer while loop has time complexity polynomial in Ω, K, P.

Next, in the j-th inner while loop, we are testing μ-stability of some subrepresentation M_i^j/M_i of M/M_i using Theorem 3.5. As before, the time complexity is bounded by a polynomial in Ω, K, P. Since there are at most $\sum_v \dim M_v \leq K$ many inner while loops, completing the inner while loop has again time complexity polynomial in Ω, K, P.

After the inner loop, we arrive at the scss subrepresentation M_{i+1}/M_i of M/M_i. To compute a basis for the quotient $(M/M_{i+1})_v$ at each vertex v, we may compute a basis for a complement of $(M_{i+1}/M_i)_v$ in $(M/M_i)_v$. This can be done by computing the null space of the basis matrix for $(M_{i+1}/M_i)_v$, which has complexity $O(\dim(M_{i+1}/M_i)_v^2 \dim(M/M_i)_v)$. The complexity to compute bases at all vertices can therefore be bounded by $O(K^3)$. Next, for each arrow $a \in Q_1$, the map $(M/M_{i+1})(a)$ can be obtained via the following change of bases to the original map

$$(M/M_i)(a) : (M_{i+1}/M_i)_{ta} \oplus (M/M_{i+1})_{ta} \to (M_{i+1}/M_i)_{ha} \oplus (M/M_{i+1})_{ha},$$

which has time complexity bounded by $O(K^3)$. Therefore, the time complexity to compute the quotient M/M_{i+1} is bounded by a polynomial in K and P.

In sum, we showed that each outer while loop has time complexity polynomial in Ω, K, P. Since there can be at most $\sum_v \dim M_v \leq K$ outer loops, the total time complexity is still polynomial in Ω, K, P. □

4. Completing Theorem B

The major goal of this section is to complete Theorem B. That is, we are going to construct a maximally destabilizing one parameter subgroup from the Harder–Narasimhan filtration of an unstable representation. This is where GIT comes into play.

GIT stability and its numerical criterion, known as the Hilbert–Mumford criterion (Theorem 4.3), were established by Mumford in [Mumford et al. 1994]. The Hilbert–Mumford criterion reduces testing stability for reductive group actions to one dimensional torus actions. This is done by restricting the action to one parameter subgroups of the reductive group. Mumford first conjectured the existence of the one parameter subgroups that fail the numerical criterion maximally. The conjecture was then resolved by Kempf [1978] in his famous paper. Beyond existence Kempf actually established the uniqueness of maximally destabilizing one parameter subgroups up to conjugacy by some parabolic subgroup (Theorem 4.5).

In Section 4A, we will first recall Mumford's definition of stability (Definition 4.1) and the Hilbert–Mumford criterion (Theorem 4.3) in the affine setting. We then make precise the meaning of maximally destabilizing one parameter subgroups (Definition 4.4), and present Kempf's theorem (Theorem 4.5).

We then apply these machinery in the context of representations of quivers in Section 4B. Finally in Section 4C, we recall in Theorem 4.6 a way due to Zamora [2014] to construct a maximally destabilizing one parameter subgroup from the Harder–Narasimhan filtration of an unstable representation. This completes Theorem B.

4A. ***Instability in affine geometric invariant theory.*** Here we recall necessary notions and theorems from affine GIT. We work with a fixed algebraically closed field k. Let G be a reductive group acting on an affine variety X. We let $\mathbf{\Gamma}(G)$ denote the set of one parameter subgroups of G. We fix a norm $\|-\|$ on $\mathbf{\Gamma}(G)$. The norm satisfies the following two properties:

(1) $\|-\|$ is invariant under conjugation. Namely, for any $g \in G$ and any $\lambda \in \mathbf{\Gamma}(G)$, we have

$$\|\lambda\| = \|g\lambda g^{-1}\|.$$

(2) For any maximal torus $T \subset G$, the restriction of $\|-\|$ to the lattice $\mathbf{\Gamma}(T)$ is induced by an inner product on the vector space $\mathbf{\Gamma}(T) \otimes \mathbb{R}$ that is integral on $\mathbf{\Gamma}(T) \times \mathbf{\Gamma}(T)$.

For the precise notion of a norm on the set of one parameter subgroups, we refer the readers to page 58 of [Mumford et al. 1994].

Stability in GIT depends on the choice of a linearized line bundle. In the affine setting, a character $\chi : G \to k^\times$ of G induces a linearization of the trivial line bundle $\mathscr{O}_X$. Fix a character χ.

For any one parameter subgroup $\lambda : k^\times \to G$ of G, we let $\langle \chi, \lambda \rangle$ be the integer that satisfies $(\chi \circ \lambda)(t) = t^{\langle \chi, \lambda \rangle}$ for all $t \in k^\times$.

Definition 4.1. An element $f \in k[X]$ is *χ-invariant of weight d* if $f(g \cdot x) = \chi^d(g^{-1}) f(x)$ for all $g \in G$ and for all $x \in X$. We say a point $x \in X$ is *χ-semistable* if there is a χ-invariant f of positive weight such that $f(x) \neq 0$. We say a point $x \in X$ is *χ-unstable* if x is not χ-semistable. We write $X^{\mathrm{ss}}(\chi)$ as the set of χ-semistable points in X and $X^{\mathrm{us}}(\chi)$ as the complement $X - X^{\mathrm{ss}}(\chi)$.

It follows from the definition that $X^{\mathrm{ss}}(\chi)$ is a G-invariant open subvariety and that $X^{\mathrm{us}}(\chi)$ is a G-invariant closed subvariety. Moreover, $X^{\mathrm{ss}}(\chi) = X^{\mathrm{ss}}(\chi^d)$ for any $d > 0$.

Remark 4.2 [Mumford et al. 1994]. Let $k[X]_{\chi,d}$ be the space of χ-invariant elements of weight d. The space $\bigoplus_{d \geq 0} k[X]_{\chi,d}$ has a natural graded ring structure. Let

$$X /\!\!/_\chi G := \operatorname{Proj}\Bigl(\bigoplus_{d \geq 0} k[X]_{\chi,d}\Bigr).$$

Then there is a map $X^{\mathrm{ss}}(\chi) \to X /\!\!/_\chi G$ that is constant on G-orbits, submersive and induces a bijection between points in $X /\!\!/_\chi G$ and closed orbits in $X^{\mathrm{ss}}(\chi)$. Moreover, $X /\!\!/_\chi G$ is a quasiprojective variety that is known as *the GIT quotient of X by G with respect to χ*.

We now introduce the Hilbert–Mumford criterion, which tests stability by restricting the group action to certain one parameter subgroups. Let $\lambda : k^\times \to G$ be a one parameter subgroup and let $x \in X$ be a point. We say $\lim_{t \to 0} \lambda(t) \cdot x$ exists if the domain of the map $\lambda_x : k^\times \to X$ defined by $t \mapsto \lambda(t) \cdot x$ can be extended to the entire affine line.

Theorem 4.3 (Hilbert–Mumford criterion [Mumford et al. 1994; King 1994]). *A point $x \in X$ is χ-semistable if and only if for each one parameter subgroup $\lambda : k^\times \to G$ such that* $\lim_{t \to 0} \lambda(t) \cdot x$ *exists, we have $\langle \chi, \lambda \rangle \leq 0$.*

Next, we define a numerical measure for instabilities contributed by destabilizing one parameter subgroups. For a point $x \in X$, set

$$C_x = \{\lambda \in \mathbf{\Gamma}(G) \mid \lim_{t \to 0} \lambda(t) \cdot x \text{ exists}\}.$$

According to Theorem 4.3, $x \in X^{\mathrm{us}}(\chi)$ if and only if there is a one parameter subgroup λ such that

(1) $\lambda \in C_x$, and

(2) $\langle \chi, \lambda \rangle > 0$.

Therefore, for an $x \in X^{\mathrm{us}}(\chi)$, it is natural to ask if there is a one parameter subgroup that contributes to the highest instability measured by the quantities $\langle \chi, \lambda \rangle$ among all $\lambda \in C_x$. An immediate problem is that $\langle \chi, \lambda^N \rangle = N \cdot \langle \chi, \lambda \rangle$ for any $N \in \mathbb{N}$. To get rid of the dependency on multiples of one parameter subgroups, we divide the function $\langle \chi, - \rangle : \mathbf{\Gamma}(G) \to \mathbb{Z}$ by the norm $\|-\|$ on $\mathbf{\Gamma}(G)$.

For $x \in X^{\mathrm{us}}(\chi)$, we set

$$\mathcal{M}^\chi(x) := \sup_{\lambda \in C_x \setminus \{0\}} \frac{\langle \chi, \lambda \rangle}{\|\lambda\|}.$$

Definition 4.4. We say a one parameter subgroup λ is *indivisible* if λ is a primitive lattice in a (and hence in any) maximal torus containing λ. We say a one parameter subgroup λ is χ*-adapted to* x if $\langle \chi, \lambda \rangle / \|\lambda\| = \mathcal{M}^\chi(x)$. We let $\Lambda^\chi(x)$ denote the set of indivisible one parameter subgroups that are χ-adapted to x.

We also recall that for any one parameter subgroup λ, there is the associated parabolic subgroup

$$P(\lambda) = \{g \in G \mid \lim_{t \to 0} \lambda(t) g \lambda(t)^{-1} \text{ exists in } G\}$$

of G. An important property about $P(\lambda)$ we want to mention is that it preserves filtration in the following sense: Let V be a representation of G and let $\bigoplus_{n \in \mathbb{Z}} V^{(n)}$ be the weight decomposition of some one parameter subgroup λ of G. Namely, λ acts on $V^{(n)}$ with weight n. Suppose $p \in P(\lambda)$, we then have

$$p \cdot V^{(\geq n)} = V^{(\geq n)}$$

where $V^{(\geq n)} = \bigoplus_{m \geq n} V^{(m)}$.

We are now ready for Kempf's theorem.

Theorem 4.5 [Kempf 1978]. *Let G be a reductive group, acting on an affine variety X. Let χ be a character of G, and let $x \in X$ be a χ-unstable point. Then*:

(1) *$\Lambda^\chi(x)$ is not empty.*

(2) *For any $g \in G$, $\Lambda^\chi(g \cdot x) = g \Lambda^\chi(x) g^{-1}$, and $\mathcal{M}^\chi(g \cdot x) = \mathcal{M}^\chi(x)$.*

(3) *There is a parabolic subgroup $P(\chi, x)$ of G such that for all $\lambda \in \Lambda^\chi(x)$, $P(\lambda) = P(\chi, x)$, and such that any two elements of $\Lambda^\chi(x)$ are conjugate to each other by an element in $P(\chi, x)$.*

4B. ***The quiver setting.*** We now unpack what these machineries mean in the case of representation of quivers. For starters, let us fix an acyclic quiver Q, and a dimension vector $\boldsymbol{d} \in \mathbb{Z}^{Q_0}$. By $\mathrm{GL}(n)$ we mean the linear algebraic group of invertible $n \times n$ matrices with entries in k. Let the linear algebraic group

$$\mathrm{GL}(\boldsymbol{d}) := \prod_{v \in Q_0} \mathrm{GL}(\boldsymbol{d}_v)$$

act on the k-vector space

$$R(Q,\boldsymbol{d}) := \prod_{a\in Q_1} \operatorname{Hom}_k(k^{\boldsymbol{d}_{ta}}, k^{\boldsymbol{d}_{ha}})$$

via the following law:

$$(g\cdot\phi)_a = g_{ha}\circ\phi_a\circ(g_{ta})^{-1} \text{ for any } g\in G, \phi\in R(Q,\boldsymbol{d}).$$

In this way, the $\mathrm{GL}(\boldsymbol{d})$-orbits in $R(Q,\boldsymbol{d})$ correspond to the isomorphism classes of representations of Q of dimension $\boldsymbol{d}$. A weight $\theta:\mathbb{Z}^{Q_0}\to\mathbb{Z}$ defines a character $\chi_\theta:\mathrm{GL}(\boldsymbol{d})\to k^\times$ by

$$\chi_\theta(g) = \prod_{v\in Q_0} \det(g_v)^{\theta(v)} \text{ for any } g\in \mathrm{GL}(\boldsymbol{d}).$$

We fix a weight θ with $\theta(\boldsymbol{d})=0$.

Let M be a representation of Q of dimension $\boldsymbol{d}$. Since χ_θ-stability is constant on $\mathrm{GL}(\boldsymbol{d})$-orbits, different choices of bases for each M_v does not affect the χ_θ-stability of the corresponding elements of M in $R(Q,\boldsymbol{d})$. From now on we fix an identification $M_v\simeq\mathbb{R}^{\boldsymbol{d}_v}$ for each v, and still write the identification of M in $R(Q,\boldsymbol{d})$ as M.

We now recall the following relation between weighted filtrations of M, and the one parameter subgroups having limits at M, namely, the one parameter subgroups in C_M. Any one parameter subgroup $\lambda\in C_M$ induces a weighted filtration

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_s = M,$$

where λ acts on each quotient M_i/M_{i-1} with weight Γ_i. Moreover, the weights enjoy the following property: $\Gamma_1>\Gamma_2>\cdots>\Gamma_s$; see [King 1994].

Conversely, given a weighted filtration $0=M_0\subsetneq M_1\subsetneq\cdots\subsetneq M_s=M$ with weights $\Gamma_1>\cdots>\Gamma_s$, we may choose new bases for M at all vertices that are compatible with the filtration. Namely, choose a basis for M_1, then extends the basis to M_2, M_3, and so on. We then let $g_v\in\mathrm{GL}(\boldsymbol{d}_v)$ be the one parameter subgroup that acts on $(M_i/M_{i-1})_v$ by weight Γ_i. In this way, the one parameter subgroup $\lambda=\prod_{v\in Q_0} g_v$ of $\mathrm{GL}(\boldsymbol{d})$ induces the original filtration. Moreover, since $\theta(M)=0$, we have

$$\langle\chi_\theta,\lambda\rangle = \sum_{i=1}^{s}\Gamma_i\theta(M_i/M_{i-1}) = \sum_{i=1}^{s-1}(\Gamma_i-\Gamma_{i+1})\theta(M_i). \tag{4-1}$$

In particular, for any proper subrepresentation M' of M, one may form the filtration $0\subsetneq M'\subsetneq M$, and assign weights Γ_1,Γ_2 to M' and M respectively, where Γ_1 is any integer and $\Gamma_2=\Gamma_1-1$. It then follows from the above discussion and (4-1) that there is a one parameter subgroup λ with $\langle\chi_\theta,\lambda\rangle=\theta(M')$. In view of Theorem 4.3, we see that M is χ_θ-semistable if and only if $\theta(M')\le 0$ for any subrepresentation M' of M. This was the definition, Definition 2.5 we used for weight stability.

4C. ***From the Harder–Narasimhan filtration to maximally destabilizing one parameter subgroups.*** In this section, we address how to derive a maximally destabilizing one parameter subgroup of an unstable representation M of Q from its Harder–Narasimhan filtration. We need to set up appropriate weights and slope.

Let $\Theta, \kappa : \mathbb{Z}^{Q_0} \to \mathbb{Z}$ be two weights, and let $\mu = \Theta/\kappa$ be the associated slope function. Suppose $\dim M = \boldsymbol{d}$. Recall that we defined the weight $\theta_{\boldsymbol{d}}$ where

$$\theta_{\boldsymbol{d}}(N) := \kappa(\boldsymbol{d})\Theta(N) - \Theta(\boldsymbol{d})\kappa(N) \text{ for any representation } N.$$

With these we have that $\theta_{\boldsymbol{d}}(M) = 0$, and that M is μ-semistable if and only if it is $\chi_{\theta_{\boldsymbol{d}}}$-semistable Lemma 2.7.

We now define a norm $\|-\|$ on $\boldsymbol{\Gamma}(\mathrm{GL}(\boldsymbol{d}))$. This norm will depend on the weight κ. We first build the norm on the diagonal maximal torus $T \subset \mathrm{GL}(\boldsymbol{d})$. There is a natural identification

$$\boldsymbol{\Gamma}(T)_{\mathbb{R}} \simeq \bigoplus_{v \in Q_0} \mathbb{R}^{\boldsymbol{d}_v}.$$

We weight the standard norm on $\mathbb{R}^{\boldsymbol{d}_v}$ by $\kappa(v)$ for each v. More explicitly, if $\lambda \in \boldsymbol{\Gamma}(T)$ with $\lambda_v = (\lambda_{1,v}, \dots, \lambda_{\boldsymbol{d}_v,v})$, we set

$$\|\lambda\| = \Bigl(\sum_{v \in Q_0} \sum_{i=1}^{\boldsymbol{d}_v} \kappa(v)(\lambda_{i,v})^2\Bigr)^{1/2}. \tag{4-2}$$

This norm $\|-\|$ extends to the entire set $\Gamma(\mathrm{GL}(\boldsymbol{d}))$ and is invariant under conjugation. We refer the readers to page 58 in [Mumford et al. 1994] for a detailed discussion on the construction of norms on the set of one parameter subgroup of a reductive group.

Therefore, whenever $\lambda \in C_M$ (that is, $\lim_{t\to 0} \lambda(t) \cdot M$ exists), its norm can be expressed in terms of its weights and the filtration it induces: If $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_s = M$ is the filtration induced by λ with weights $\Gamma_1 > \cdots > \Gamma_s$, then

$$\|\lambda\| = \Bigl(\sum_{i=1}^{s} \sum_{v \in Q_0} \kappa(v)\Gamma_i^2 \dim(M_i/M_{i-1})_v\Bigr)^{1/2} = \Bigl(\sum_{i=1}^{s} \Gamma_i^2 \kappa(M_i/M_{i-1})\Bigr)^{1/2}. \tag{4-3}$$

We adopt the above norm to define (using Definition 4.4) one parameter subgroups that are $\chi_{\theta_{\boldsymbol{d}}}$-adapted to M.

Since all one parameter subgroups that are $\chi_{\theta_{\boldsymbol{d}}}$-adapted to M are in a full conjugacy class of their parabolic subgroup (Theorem 4.5), the filtrations induced by those one parameter subgroups are the same. In [Zamora 2014], such a filtration is named as the Kempf filtration of M. By Theorem 5.3 from [loc. cit.], it is also the Harder–Narasimhan filtration for M with respect to the slope μ. In addition, there is the following recipe for reverse engineering a maximally destabilizing one parameter subgroup from the Harder–Narasimhan filtration.

Theorem 4.6 [Zamora 2014, Theorem 4.1, Lemma 5.2]. *Let $\Theta, \kappa : \mathbb{Z}^{Q_0} \to \mathbb{Z}$ be two weights and let $\mu = \Theta/\kappa$ be the slope. Let M be a μ-unstable representation of dimension $\boldsymbol{d}$, and let*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$$

be the Harder–Narasimhan filtration. Set

$$u_i = \kappa(M)\mu(M_i/M_{i-1}) - \Theta(M) \textit{ for } i = 1, \dots, r.$$

Choose a basis for M_v for each vertex v compatible with the filtration, and let $T \subset \mathrm{GL}(\boldsymbol{d})$ be the maximal torus diagonal with respect to these bases. Define $\tilde{\lambda} \in \boldsymbol{\Gamma}(T)_{\mathbb{Q}} \simeq \bigoplus_{v \in Q_0} \mathbb{Q}^{\boldsymbol{d}_v}$ where for each i and v, the entries of $\tilde{\lambda}_v$ that correspond to $(M_i/M_{i-1})_v$ are u_i. Then the lattice points on the ray $\mathbb{Q}_{>0} \cdot \tilde{\lambda}$ are the one parameter subgroups in T that are $\chi_{\theta_{\boldsymbol{d}}}$-adapted to M. Moreover,

$$\mathcal{M}^{\chi_{\theta_{\boldsymbol{d}}}}(M) = \biggl(\sum_{i=1}^{r} (\kappa(M)\mu(M_i/M_{i-1}) - \Theta(M))^2 \kappa(M_i/M_{i-1})\biggr)^{1/2}.$$

Remark 4.7. In the case that $\Theta(M) = 0$ in the first place, one can take

$$u_i = \mu(M_i/M_{i-1}),$$

and

$$\mathcal{M}^{\chi_{\Theta}}(M) = \biggl(\sum_i \mu(M_i/M_{i-1})^2 \kappa(M_i/M_{i-1})\biggr)^{1/2} = \biggl(\sum_i \Theta(M_i/M_{i-1})\mu(M_i/M_{i-1})\biggr)^{1/2}.$$

Therefore, knowing the Harder–Narasimhan filtration of an unstable representation is equivalent to knowing its maximally destabilizing one parameter subgroups. A full treatment of Theorem B is now complete. An account of the correctness of the construction in Theorem 4.6 is given in the next section for interested readers.

4D. ***Maximizing Kempf function.*** Let M be a μ-unstable representation of Q of dimension $\boldsymbol{d}$ with the Harder–Narasimhan filtration

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M.$$

By Theorem 5.3 from [Zamora 2014], the filtration is the same as the Kempf filtration. Recall that C_M denotes the set of one parameter subgroups having limits at M. Let

$$f : C_M \backslash \{\boldsymbol{0}\} \to \mathbb{R}$$

be the function defined by

$$f(\lambda) = \frac{\langle \chi_{\theta_{\boldsymbol{d}}}, \lambda \rangle}{\|\lambda\|}.$$

To maximize this function, we can restrict the search range to the set of one parameter subgroups that induce the Kempf filtration, which is also the Harder–Narasimhan filtration.

Consider the inner product $(\,-\,,\,-\,) : \mathbb{R}^r \times \mathbb{R}^r \to \mathbb{R}$ defined by the matrix

$$\begin{pmatrix} \kappa(M_1) & & & 0 \\ & \kappa(M_2/M_1) & & \\ & & \ddots & \\ 0 & & & \kappa(M/M_{r-1}) \end{pmatrix}.$$

If λ is a one parameter subgroup that induces the Harder–Narasimhan filtration of M with the weight vector $\Gamma = (\Gamma_1, \dots, \Gamma_s)$, then upon using $\theta_{\boldsymbol{d}}$ as θ in (4-1), we derive that

$$\begin{aligned} \langle \chi_{\theta_{\boldsymbol{d}}}, \lambda \rangle &= \sum_i \Gamma_i \big(\kappa(M)\Theta(M_i/M_{i-1}) - \Theta(M)\kappa(M_i/M_{i-1})\big) \\ &= \sum_i \Gamma_i \kappa(M_i/M_{i-1})(\kappa(M)\mu(M_i/M_{i-1}) - \Theta(M)) \\ &= (\Gamma, u), \end{aligned} \tag{4-4}$$

where $u_i = \kappa(M)\mu(M_i/M_{i-1}) - \Theta(M)$. Moreover, (4-3) implies $\|\lambda\| = (\Gamma, \Gamma)^{1/2}$.

Letting $u = (u_1, \dots, u_r) \in \mathbb{R}^r$, we define the function

$$g_u : \mathbb{R}^r \backslash \{\mathbf{0}\} \to \mathbb{R}$$

where

$$g_u(x) = \frac{(x, u)}{\sqrt{(x, x)}}.$$

This function is called the Kempf function in [Zamora 2014]. We see that maximizing f among all one parameter subgroups inducing the Kempf filtration is equivalent to maximizing the Kempf function g_u on the open cone $C = \{x \in \mathbb{R}^r \mid x_1 > x_2 > \cdots > x_r\}$. By the Cauchy–Schwarz inequality, g_u attains global maximum at u. Since $\mu(M_1) > \mu(M_2/M_1) > \cdots > \mu(M/M_r)$, u is already in the cone C. Therefore, the one parameter subgroup constructed in Theorem 4.6 maximizes f.

5. A short example

In this example we construct an unstable representation of a bipartite quiver and compute the following:

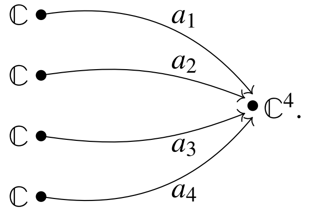
(1) Several witnesses to the discrepancy.

(2) The Harder–Narasimhan filtration.

(3) A maximally destabilizing one parameter subgroup.

We compare the results of (1), (2) with Theorem 3.3, and demonstrate that not all optimal subrepresentations occur in the Harder–Narasimhan filtration. For (3), we present two approaches. The first approach applies Theorem 4.6 to the Harder–Narasimhan filtration obtained in (2), and the second is a sketch of the brute force procedure that can be applied to any representation of any reductive group. By doing so we hope to give readers a sense of the hardness of finding Kempf's one parameter subgroups in general. The set up of this example is motivated by [Chindris and Kline 2021].

Set up. Let us consider the following representation M of the following bipartite quiver over the field $\mathbb{C}$ of complex numbers:



Label the four vertices on the left by x_1, x_2, x_3, x_4 from top to bottom. Label the single vertex on the right as y so that $M_{x_i} = \mathbb{C}$ for each $i = 1, \dots, 4$, and $M_y = \mathbb{C}^4$.

We set $M(a_1)(1) = e_2$, $M(a_2)(1) = e_1$, $M(a_3)(1) = 2e_1$, and $M(a_4)(1) = e_3$ in $\mathbb{C}^4$, where $e_1, \dots, e_4$ form the standard basis of $\mathbb{C}^4$. We let Θ and κ be two weights where $\Theta(x_i) = 4$, $\Theta(y) = -4$, and $\kappa(x_i) = \kappa(y) = 1$ for each i. It then follows that $\Theta(M) = 0$. We also let $\mu(-) = \Theta(-)/\kappa(-)$ be the corresponding slope.

We let $\mathrm{Sp}(e_1)$ be the largest subrepresentation M' of M such that $M'_y = \mathrm{Span}(e_1)$. Specifically,

$$\mathrm{Sp}(e_1)_{x_i} = \begin{cases} \mathbb{C} & \text{if } i = 2, 3, \\ 0 & \text{if } i = 1, 4, \end{cases}$$

and

$$\mathrm{Sp}(e_1)_y = \mathrm{Span}(e_1).$$

We define $\mathrm{Sp}(e_1, e_2)$, $\mathrm{Sp}(e_1, e_3)$, and $\mathrm{Sp}(e_1, e_2, e_3)$ similarly.

Witnesses to the discrepancy. We verify that the four subrepresentations $\mathrm{Sp}(e_1)$, $\mathrm{Sp}(e_1, e_2)$, $\mathrm{Sp}(e_1, e_3)$, $\mathrm{Sp}(e_1, e_2, e_3)$ are Θ-optimal in M with Θ value 4. For this, note that for any subrepresentation M' of M,

$$\Theta(M') \leq 4 \cdot (\#\{i \mid M'_{x_i} = \mathbb{C}\} - \dim(\mathrm{Span}(\{M(a_i)(1) \mid M'_{x_i} = \mathbb{C}\}))).$$

Therefore, for $\Theta(M')$ to be positive, M'_{x_2} and M'_{x_3} must be equal to $\mathbb{C}$. The only proper subrepresentations of M that are nonzero at x_2, x_3 with positive Θ values are exactly the four subrepresentations listed above. Since they all have the same Θ value 4, they are also Θ-optimal and $\mathrm{disc}(M, \Theta) = 4$.

The Harder–Narasimhan filtration. We verify that

$$0 \subsetneq \mathrm{Sp}(e_1) \subsetneq \mathrm{Sp}(e_1, e_2, e_3) \subsetneq M$$

is the Harder–Narasimhan filtration of M. For this, it is clear that $\mathrm{Sp}(e_1)$ is the only subrepresentation with the highest slope $4/3$. We may infer that $\mathrm{Sp}(e_1)$ is the scss subrepresentation of M. Moving on to $M/\mathrm{Sp}(e_1)$, since $\mathrm{Sp}(e_1)$ is Θ-optimal, we can infer $\mu(M'/\mathrm{Sp}(e_1)) \leq 0$ for any subrepresentation M' containing $\mathrm{Sp}(e_1)$. Since

$$\mu(\mathrm{Sp}(e_1, e_2)/\mathrm{Sp}(e_1)) = \mu(\mathrm{Sp}(e_1, e_3)/\mathrm{Sp}(e_1)) = \mu(\mathrm{Sp}(e_1, e_2, e_3)/\mathrm{Sp}(e_1)) = 0,$$

we infer that the quotient $\mathrm{Sp}(e_1, e_2, e_3)/\mathrm{Sp}(e_1)$ is the scss subrepresentation of $M/\mathrm{Sp}(e_1)$. The quotient $M/\mathrm{Sp}(e_1, e_2, e_3)$ is one dimensional on y and zero elsewhere. We conclude that $M/\mathrm{Sp}(e_1, e_2, e_3)$ is μ-semistable and that the filtration written above is the Harder–Narasimhan filtration of M.

Here we note that the two Θ-optimal subrepresentations $\mathrm{Sp}(e_1, e_2)$ and $\mathrm{Sp}(e_1, e_3)$ are not included in the filtration. We see in this example that not all optimal subrepresentations occur in the Harder–Narasimhan filtration. Also note that $\mathrm{Sp}(e_1)$ has the highest slope among all Θ-optimal subrepresentations. This agrees with the implications of Theorem 3.3 because $\mu(\mathrm{Sp}(e_1)) = 4/3 > 0 = \mu(\mathrm{Sp}(e_1, e_2, e_3)/\mathrm{Sp}(e_1))$. Namely, $\mathrm{Sp}(e_1)$ serves as M_l in the description of Theorem 3.3.

Maximal destabilizing one parameter subgroups. We now demonstrate a maximally destabilizing one parameter subgroup for M with respect to the weight Θ and the norm weighted by κ. The first thing to do is to reproduce the GIT set up introduced in Section 4B. To begin with, we have the vector space $\prod_{a\in Q_1}\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}, \mathbb{C}^4) \simeq \mathbb{C}^{4\times 4}$. Each column of a matrix in $\mathbb{C}^{4\times 4}$ defines a map from a left vertex to the right vertex. We let the first column define a map from x_1 to y, and so on. In this way, the group $G = (\mathbb{C}^\times)^4 \times \mathrm{GL}(4)$ acts on $\mathbb{C}^{4\times 4}$ via the rule

$$(t_1, t_2, t_3, t_4, A)\cdot U = A\cdot U\cdot \begin{pmatrix} t_1^{-1} & & & \\ & t_2^{-1} & & \\ & & t_3^{-1} & \\ & & & t_4^{-1} \end{pmatrix}$$

for all $(t_1, t_2, t_3, t_4, A) \in G$ and for all $U \in \mathbb{C}^{4\times 4}$. There is the diagonal torus $D \simeq (\mathbb{C}^\times)^4$ in $\mathrm{GL}(4)$. Let $T = (\mathbb{C}^\times)^4 \times D \subset G$ be the maximal torus in G. We then have $\boldsymbol{\Gamma}(T)_{\mathbb{Q}} \simeq \mathbb{Q}^8$. With the notations introduced in Theorem 4.6, we have

$$u_1 = \tfrac{4}{3},\quad u_2 = 0,\quad u_3 = -4$$

by Remark 4.7. The maximally destabilizing one parameter subgroups in T is then on the positive ray of the point

$$\big(\underbrace{0, \tfrac{4}{3}, \tfrac{4}{3}, 0}_{x_1,x_2,x_3,x_4}, \underbrace{\tfrac{4}{3}, 0, 0, -4}_{y}\big).$$

We now sketch a procedure using linear programming. Here we do not assume we know the Harder–Narasimhan filtration in the first place. Recall that Θ defines the character χ_Θ of G where

$$\chi_\Theta(t_1, t_2, t_3, t_4, A) = (t_1t_2t_3t_4)^4\cdot\det(A)^{-4}$$

for all $(t_1, t_2, t_3, t_4, A) \in G$. The representation M corresponds to the matrix:

$$\begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Let us continue to use M to represent the matrix.

If $\lambda(t) = (t^{a_1}, \dots, t^{a_8})$ is a one parameter subgroup in T, then

$$\lambda(t) \cdot M = \begin{pmatrix} 0 & t^{-a_2+a_5} & 2 \cdot t^{-a_3+a_5} & 0 \\ t^{-a_1+a_6} & 0 & 0 & 0 \\ 0 & 0 & 0 & t^{-a_4+a_7} \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

We see that $\lim_{t\to\infty} \lambda(t) \cdot M$ exists if and only if

$$\begin{aligned} -a_1 + a_6 &\geq 0, \\ -a_2 + a_5 &\geq 0, \\ -a_3 + a_5 &\geq 0, \\ -a_4 + a_7 &\geq 0. \end{aligned} \tag{5-1}$$

One also easily calculates that

$$\langle \chi_\Theta, \lambda \rangle = 4(a_1 + a_2 + a_3 + a_4) - 4(a_5 + a_6 + a_7 + a_8).$$

The norm on the set of one parameter subgroups of T is weighted by κ. In this case it is simply the standard norm. Therefore, to find one parameter subgroups in T that maximally destabilize M, we are maximizing the function

$$f = \frac{4(a_1 + a_2 + a_3 + a_4) - 4(a_5 + a_6 + a_7 + a_8)}{(a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2 + a_8^2)^{1/2}},$$

with the side constraints given by (5-1). With the help of SageMath, we calculated that f attains maximum on the positive ray of the point $\bigl(0, \frac{4}{3}, \frac{4}{3}, 0, \frac{4}{3}, 0, 0, -4\bigr)$.

Notice that the constraints depends only on the nonzero entries of M. That is, replacing the nonzero entries of M by any other nonzero scalars does not change the linear programming problem. The set of the positions of the nonzero entries of M is called the support of M.

We must be aware that up to this point, we are only calculating one parameter subgroups in T. In general, maximally destabilizing one parameter subgroups of an unstable point do not have to be in a particular maximal torus. To work with a particular maximal torus, one needs to enumerate all supports coming from the orbit of the unstable point, conduct linear programming for each support, and choose the maximum result. Often times the challenge is to determine the supports of points in the orbit. Beyond that the number of supports of points in the orbit can be quite large, leading to vast amount of linear programming required. As we can see, enumerating supports of $g \cdot M$ for all $g \in G$ in this relatively small example already gets tedious. We shall not continue this brute force procedure here, as the main point to illustrate the hardness of finding Kempf's one parameter subgroups in general, and to demonstrate the value of Theorem 4.6 is made.

Appendix: Algebraic complexity towards the stability of representations of quivers

In this section, we will demonstrate how algebraic complexity tools can be applied to computing the discrepancy, together with a witnesses, for a representation of an acyclic quiver.

Preliminaries. For starters, we let $\mathbb{F}$ be an infinite field of arbitrary characteristic. The space of $n \times n$ matrices over $\mathbb{F}$ is denoted $M(n, \mathbb{F})$. Let $\mathcal{B}$ be a subspace of $M(n, \mathbb{F})$. If U is a subspace of $\mathbb{F}^n$, we set

$$\mathcal{B}(U) = \sum_{B \in \mathcal{B}} BU,$$

where $\sum$ denote the sum of subspaces. We say U is a *c-shrunk subspace of $\mathcal{B}$* if

$$\dim U - \dim \mathcal{B}(U) \geq c.$$

We say U is a *shrunk subspace of $\mathcal{B}$* if U is a c-shrunk subspace of $\mathcal{B}$ for some $c \in \mathbb{Z}^+$. We define the *discrepancy of $\mathcal{B}$* as the integer

$$\operatorname{disc}(\mathcal{B}) = \max_{c \in \mathbb{N}} \{\exists \text{ a } c\text{-shrunk subspace of } \mathcal{B}\}.$$

Remark A.1. For any subspace $\mathcal{B} \subset M(n, \mathbb{F})$, if $c = \operatorname{disc}(\mathcal{B})$, it is shown in [Huszar 2021, Lemma 2.1], that the intersection of c-shrunk subspaces is again a c-shrunk subspace. Therefore, there is an unique minimal c-shrunk subspace of $\mathcal{B}$.

The following is a summary of various results from [Ivanyos et al. 2018] and [Ivanyos et al. 2015] .

Theorem A.2 [Ivanyos et al. 2018, Theorem 1.5; 2015, Proposition 7, Lemma 9]. *Let $\mathcal{B}$ be a matrix space in $M(n, \mathbb{F})$ with $\operatorname{disc}(\mathcal{B}) = c$ (a priori unknown). There exists a deterministic algorithm using $n^{O(1)}$ arithmetic operations over $\mathbb{F}$ that returns a c-shrunk subspace of $\mathcal{B}$. Moreover, the c-shrunk subspace produced by this algorithm is the minimal c-shrunk subspaces of $\mathcal{B}$.*

Remark A.3. The original Theorem 1.5 from [Ivanyos et al. 2018] deals with how field elements are represented in a computer, which is not the main concern of this paper. Personal communications with the authors of [loc. cit.] confirmed that in terms of the number of operations needed, there is nothing special about the field of rational numbers stated in the theorem in [loc. cit.]. Any field with large enough set of elements to work with will suffice.

We now follow the recipe of [Huszar 2021] to build a matrix space from a given representation of an acyclic quiver, and establish the connection between the discrepancy of the matrix space and that of the representation. Recall we wrote a quiver as $Q = (Q_0, Q_1, t, h)$. Multiple arrows between any two vertices are allowed. We fix a weight $\theta : Q_0 \to \mathbb{Z}$ and a representation W of Q of dimension $\boldsymbol{d}$ with $\theta(\boldsymbol{d}) = 0$. If $p = a_j a_{j-1} \cdots a_1$ is a path in Q, we let $W(p)$ denote the composition $W(a_j)W(a_{j-1}) \cdots W(a_1)$.

Let $x_1, \dots, x_n$ (resp. $y_1, \dots, y_m$) be the vertices of Q where θ takes positive values (resp. negative values). We then define

$$\begin{aligned}\theta_+(x_i) = \theta(x_i) \quad &(\text{resp. } \theta_-(y_j) = -\theta(y_j)),\\ N := \sum_i \theta_+(x_i)\boldsymbol{d}(x_i) &= \sum_j \theta_-(y_j)\boldsymbol{d}(y_j),\end{aligned}$$

and

$$M = \sum_j \theta_-(y_j) \quad (\text{resp. } M' = \sum_i \theta_+(x_i)).$$

For each $i \in [n]$ and each $j \in [m]$, we let

$$I_i^+ = \left\{ r \in \mathbb{N} \,\middle|\, \sum_{k=1}^{i-1} \theta_+(x_i) < r \leq \sum_{k=1}^{i} \theta_+(x_i) \right\},$$

and

$$I_j^- = \left\{ q \in \mathbb{N} \,\middle|\, \sum_{k=1}^{j-1} \theta_-(y_j) < q \leq \sum_{k=1}^{j} \theta_-(y_j) \right\}.$$

For each $q \in I_j^-$, $r \in I_i^+$, and each path p between x_i and x_j, we define the $M \times M'$ block matrix $A_{q,r}^{i,j,p}$ whose (q, r)-block is the $\boldsymbol{d}(y_j) \times \boldsymbol{d}(x_i)$ matrix representing $W(p) : \mathbb{R}^{d(x_i)} \to \mathbb{R}^{d(y_j)}$, and whose other blocks are zero block matrices of appropriate sizes. In this way, the same matrix representing $W(p)$ is placed in the various (q', r')-blocks of $M \times M'$ block matrices for $q' \in I_j^-$, and $r' \in I_i^+$. We set

$$\mathcal{A}_{W,\theta} = \operatorname{Span}(\{A_{q,r}^{i,j,p} \mid i \in [n], j \in [m], q \in I_j^-, r \in I_i^+, p \in \mathcal{P}_{i,j}\}) \subset M(N, \mathbb{F}).$$

where $\mathcal{P}_{i,j}$ is the collection of paths from x_i to y_j.

We have an immediate relation described by the

Lemma A.4. *For any representation* W, *we have* $\operatorname{disc}(W, \theta) \leq \operatorname{disc}(\mathcal{A}_{W,\theta})$.

Proof. Let $W' \subset W$ be a subrepresentation. Define $U = \bigoplus_i (W'_{x_i})^{\theta_+(x_i)}$. It then follows that

$$\begin{aligned}\theta(W') &= \sum_i \theta_+(x_i) W'_{x_i} - \sum_j \theta_-(y_j) W'_{y_j}\\ &= \dim U - \dim\Bigl(\bigoplus_j W_{y_j}^{\theta_-(y_j)}\Bigr)\\ &\leq \dim U - \dim\Bigl(\bigoplus_{j,q} \sum_i \sum_{p \in \mathcal{P}_{ij}} W(p)(W'_{x_i})\Bigr)\\ &= \dim U - \dim \mathcal{A}_{W,\theta}(U).\end{aligned}$$

This finishes the proof of the lemma. □

Relating the two discrepancies. In this section we relate better the two discrepancies $\operatorname{disc}(W, \theta)$, and $\operatorname{disc}(\mathcal{A}_{W,\theta})$. We will show that they are equal, and demonstrate how to translate a witness to one discrepancy into a witness to the other. For this we need to introduce a right action on $\bigoplus_i W_{x_i}^{\theta_+(x_i)}$ and on $\bigoplus_j W_{y_j}^{\theta_-(y_j)}$ by the paths of Q. For the following, homomorphisms and endomorphisms are taken in the category of representations of Q. In addition, we let $c = \operatorname{disc}(\mathcal{A}_{W,\theta})$ so that by a c-shrunk subspace of $\mathcal{A}_{W,\theta}$ we mean a subspace that witnesses $\operatorname{disc}(\mathcal{A}_{W\theta})$.

For any vertex $x \in Q_0$, we let P_x be the representation of Q where for each $y \in Q_0$, $(P_x)_y$ is the vector space with basis the paths from x to y. Here $(P_x)_x$ is one dimensional with basis the trivial path e_x. For any $a \in Q_1$, we define

$$P_x(a) : (P_x)_{ta} \to (P_x)_{ha}$$

by post composition.

For any representation V of Q, there is a natural identification $\operatorname{Hom}(P_x, V) \simeq V_x$. Letting

$$P_1 = \bigoplus_i P_{x_i}^{\theta_+(x_i)} \quad \left(\text{resp. } P_0 = \bigoplus_j P_{y_j}^{\theta_-(y_j)}\right),$$

we have

$$\operatorname{Hom}(P_1, W) \simeq \bigoplus_i W_{x_i}^{\theta_+(x_i)} \quad \left(\text{resp. } \operatorname{Hom}(P_0, W) \simeq \bigoplus_j W_{y_j}^{\theta_-(y_j)}\right).$$

Under the above identifications, a morphism $\varphi \in \operatorname{Hom}(P_0, P_1)$ induces a morphism $A(\varphi) : \bigoplus_i W_{x_i}^{\theta_+(x_i)} \to \bigoplus_j W_{y_j}^{\theta_-(y_j)}$ by precomposition. Moreover, if p is a path from x_i to y_j placed in the (q, r)-th component of $\operatorname{Hom}(P_0, P_1) \simeq \bigoplus_{i,j} P_{x_i}(y_j)^{\theta_-(y_j)\theta_+(x_i)}$, then the map it induces is precisely $A_{q,r}^{i,j,p}$. Therefore, for any subspace $U \subset \bigoplus_i W_{x_i}^{\theta_+(x_i)}$, $\mathcal{A}_{W,\theta}(U)$ is the same as the sum $\sum_\varphi A(\varphi)(U)$, taken over all $\varphi \in \operatorname{Hom}(P_0, P_1)$.

Similarly, $\operatorname{End}(P_1)$ (resp. $\operatorname{End}(P_0)$) induces a right action on $\bigoplus_i W_{x_i}^{\theta_+(x_i)}$ (resp. $\bigoplus_j W_{y_j}^{\theta_-(y_j)}$) by precomposition. We recall Remark A.1 that there is a unique minimal subspace that witnesses $\operatorname{disc}(\mathcal{A}_{W,\theta})$. Now we quote the

Lemma A.5 [Huszar 2021, Lemma 3.2]. *Let $U \subset \bigoplus_i W_{x_i}^{\theta_+(x_i)}$ be the minimal c-shrunk subspace of $\mathcal{A}_{W\theta}$. Then U (resp. $\sum_\varphi A(\varphi)(U)$) is a right* $\operatorname{End}(P_1)$ (*resp.* $\operatorname{End}(P_0)$)*-module. Namely, U (resp. $\sum_\varphi A(\varphi)(U)$) is closed under the right action of* $\operatorname{End}(P_1)$ (*resp.* $\operatorname{End}(P_0)$) *defined by precomposition.*

We now apply the lemma to establish the

Proposition A.6. *Let U be the minimal c-shrunk subspace of $\mathcal{A}_{W,\theta}$, and let $V = \sum_\varphi A(\varphi)(U)$. For each i, r (resp. j, q), let $\pi_{i,r} : \bigoplus_i W_{x_i}^{\theta_+(x_i)} \to W_{x_i}$ (resp. $\pi_{j,q} : \bigoplus_j W_{y_j}^{\theta_-(y_j)} \to W_{y_j}$) be the projection onto the (i, r)-th (resp. (j, q)-th) component. The following properties then hold*:

(1) *$U = \bigoplus_i (W'_{x_i})^{\theta_+(x_i)}$, where $W'_{x_i} = \pi_{i,r}(U) \subseteq W_{x_i}$ for any $r \in I_i^+$.*

(2) *$V = \bigoplus_j (W'_{y_j})^{\theta_-(y_j)}$, where $W'_{y_j} = \pi_{j,q}(V) = \sum_{i, p \in \mathcal{P}_{i,j}} W(p)(W'_{x_i}) \subseteq W_{y_j}$ for any $q \in I_j^-$.*

Proof. Let $u \in U$ and let p be a path from $x_{i'}$ to x_i in the (r', r)-th component of $\operatorname{End}(P_1) \simeq \bigoplus_{i,i'} (P_{x_{i'}})_{x_i}^{\theta_+(x_{i'})\theta_+(x_i)}$. The precomposition $u \circ p$ is then $W(p)(\pi_{i',r'}(u))$ placed in the r-th component of $W(x_i)^{\theta_+(x_i)}$. Since U is a right $\mathrm{End}(P_1)$-module, and the same path p can be placed in any (r', r)-th component of $\mathrm{End}(P_1)$, the image $W(p)(\pi_{i'r'}(u))$ when placed in the r-th component of $W(x_i)^{\sigma_+(x_i)}$, is still in U for any $r' \in I_{i'}^+$ and any $r \in I_i^+$. In particular, taking $i' = i$, we see that for any $r_1, r_2 \in I_i^+$, $\pi_{i,r_1}(u)$ when placed at the r_2-th component of $W_{x_i}^{\theta_+(x_i)}$, is still in U. Basically, we obtain

$$\pi_{i,r_1}(U) = \pi_{i,r_2}(U) \text{ for any } r_1, r_2 \in I_i^+ \quad \text{and} \quad U = \bigoplus_i (\pi_{i,r}(U))^{\theta_+(x_i)} \text{ for any r} \in I_i^+.$$

This establishes property (1).

Using the fact that V is a right $\mathrm{End}(P_0)$-module, we also get

$$V = \bigoplus_j (\pi_{j,q}(V))^{\theta_-(y_j)} \text{ for any q} \in I_j^-.$$

On the other hand, it is clear that

$$\begin{aligned}\sum_{\varphi} A(\varphi)(U) &= \bigoplus_{j,q} \Big(\sum_{i,p} \sum_r A_{q,r}^{i,j,p} \cdot \pi_{i,r}(U) \Big) \\ &= \bigoplus_{j,q} \Big(\sum_{i,p} \sum_r W(p)\pi_{i,r}(U) \Big) \\ &= \bigoplus_{j} \Big(\sum_{i,p \in \mathcal{P}_{i,j}} W(p)(W'_{x_i}) \Big)^{\theta_-(y_j)}\end{aligned}$$

This establishes property (2), finishing the proof of the proposition. □

Theorem A.7. *Let $U \subset M(N, \mathbb{F})$ be the minimal c-shrunk subspace of $\mathcal{A}_{W,\theta}$. Let $\pi_{i,r} : \bigoplus_i W_{x_i}^{\sigma_+(x_i)} \to W_{x_i}$ be the projection onto the (i, r)-th component. For each $i \in [n]$, set*

$$W'_{x_i} = \pi_{i,r}(U).$$

For each $j \in [m]$, set

$$W'_{y_j} = \sum_{i, p \in \mathcal{P}_{i,j}} W(p)(W_{x_i}).$$

For each $y \in Q_0$ with $\theta(y) = 0$, set

$$W'_y = \sum_{\theta(x) \neq 0} \Big(\sum_{p : x \to y} W(p)(W_x) \Big).$$

Then $\{W'_x\}_{x \in Q_0}$ defined this way yields a subrepresentation W' with $\theta(W') = c$. In this case, we actually have

$$\mathrm{disc}(W, \theta) = c.$$

Proof. We first verify that $\{W'_x\}_{x \in Q_0}$ forms a subrepresentation W' of W. We need to show that $W(a)(W'_{ta}) \subset W'_{ha}$ for all $a \in Q_1$. Due to the construction of W', it is more convenient to work with paths. We split the paths in Q into three major categories.

Case 1: The path starts at some $x_{i'}$. We consider three possibilities:

Case (1a) The path ends at some x_i.

Case (1b) The path ends at some y_j.

Case (1c) The path ends at some y.

For case (1a), let $p : x_{i'} \to x_i$ be a path. We have seen in the proof of Proposition A.6 that $W(p)(W_{x_{i'}})$, when placed in any r-th component of $W_{x_i}^{\theta_+(x_i)}$, is still in U. By Proposition A.6(1), $W(p)(W'_{x_{i'}}) \subset W'_{x_i}$. This finishes case (1a). Case (1b) follows from the description of W'_{y_j} in Proposition A.6. Case (1c) follows from the construction of W'_y.

Case 2: The path starts at some $y_{j'}$. Again we consider three possibilities:

Case (2a): The path ends at some x_i.

Case (2b): The path ends at some y_j.

Case (2c): The path ends at some y.

For case (2a), if there are no paths from any $x_{i'}$ into y_j, then W'_{y_j} is the zero subspace, which is a trivial scenario. If there are paths from some $x_{i'}$ into y_j, the case is covered by case (1a). Case (2b) can be established using the fact that V is an $\mathrm{End}(P_0)$-module like what we did for case (1a). Finally, case (2c) follows from the construction of W'_y as well.

Case 3: The path starts at some y'. We consider:

Case (3a): The path ends at some x_i.

Case (3b): The path ends at some y_j.

Case (3c): The path ends at some y.

If there are no paths from either $x_{i'}$ or $y_{j'}$ into y, then W'_y must be the zero subspace, which is a trivial scenario. If there is a path from some $x_{i'}$ or some $y_{j'}$ into y, case (3a) is covered by case (1a) and case (2a). Similarly case (3b) is covered by case (1b) and case (2b). Finally, case (3c) is covered by the construction of W'_y.

We have shown that $\{W'_x\}_{x\in Q_0}$ forms a subrepresentation W' of W. Next, note that

$$\theta(W') = \sum_i (\dim W'_{x_i}) \cdot \theta_+(x_i) - \sum_j (\dim W'_{y_j}) \cdot \theta_-(y_j) = \dim U - \dim \mathcal{A}_{W,\theta}(U)$$

by Proposition A.6. By Lemma A.4, it must be the case that $\theta(W') = \mathrm{disc}(W, \theta) = \mathrm{disc}(\mathcal{A}_{W,\theta})$. □

We are now able to establish the algorithm of Theorem 3.5, which returns the discrepancy, together with a witness for any representation of an acyclic quiver over an infinite field.

Corollary A.8. *Let Q be an acylcic quiver and let W be a representation as above. There is a deterministic algorithm that finds the discrepancy* $\mathrm{disc}(W, \theta)$, *together with a subrepresentation W' so that $\theta(W') =$*

$\operatorname{disc}(W,\theta)$. *If we set* $\Omega = \sum_{x\in Q_0}|\theta(x)|$, $K = \sum_{x\in Q_0}\dim W_x$, *and* P *as the number of paths in* Q, *then the algorithm has time complexity that is polynomial in* Ω, K, P.

Proof. We propose the following three steps to find the discrepancy of W, together with a witnessing subrepresentation. As step 1, we compute a basis for the matrix space

$$\mathcal{A}_{W,\theta} = \bigoplus_{i,j}\bigoplus_{q,r}\operatorname{Span}(A^{i,j,p}_{q,r} \mid p \in \mathcal{P}_{ij}),$$

where each $A^{i,j,p}_{q,r}$ is $W(p)$ placed in the (q,r)-block. If p has length l, then $W(p)$ involves $l-1$ multiplications of matrices of sizes taken from a subset of $\{\dim W_x\}_{x\in Q_0}$. Iterating through paths in increasing lengths, computing $W(p)$ for all $p \in \mathcal{P}_{i,j}$ has time complexity polynomial in K, and linear in P. We then sort out linearly independent size $\dim W(y_j) \times \dim W(x_i)$ matrices among $\{W(p) \mid p \in \mathcal{P}_{i,j}\}$, which has time complexity polynomial in K, P. Finally, we put these linearly independent matrices into appropriate (q,r)-blocks for all $q \in I^+_j$, $r \in I^+_i$, and for all i, j. There are $M \times M'$ blocks so the time complexity to compute a basis for $\mathcal{A}_{W,\theta}$ is polynomial in Ω, K, P.

As step 2, apply the algorithm of Theorem A.2 to obtain a basis of the minimal c-shrunk subspace U of $\mathcal{A}_{W,\theta}$. The time complexity is polynomial in N, which in turn is bounded by a polynomial in $\Omega \cdot K$.

As step 3, we apply Theorem A.7 to derive a basis for W'_x for each $x \in Q_0$. A spanning set for each W'_{x_i} is obtained by truncating suitable parts of the basis of U we obtained earlier. We can then trim this spanning set down to a basis within time complexity polynomial in $\dim W_{x_i}$ and N, which is bounded by a polynomial in Ω, K. Since there are at most Ω many x'_is, the time complexity to obtain bases for all W'_{x_i} is bounded by a polynomial in Ω, K. For W'_{y_j}, we can first compute $\sum_i \sum_{p\in P_{i,j}} W(p)(W'_{x_i})$. In this case, since each $W(p)$ is computed earlier, a spanning set of $W(p)(W'_{x_i})$ is obtained by multiplying $W(p)$ with the basis matrix of W'_{x_i}. Hence a spanning set for $W'(y_j)$ can be obtained within time complexity polynomial in K, P. Since there are at most $P \cdot \sum_i \dim W'_{x_i}$ vectors in the spanning set for each $W'(y_j)$, deriving a basis for W'_{y_j} has time complexity polynomial in K, P. Since the number of y_j is bounded by Ω, we may infer that computing bases for all W'_{y_j} has time complexity polynomial in Ω, K, P. Similarly, computing bases for all W'_y with $\theta(y) = 0$ has time complexity polynomial in Ω, K, P.

Since the three major steps are all within time complexity polynomial in Ω, K, P. The corollary is proved. □

Acknowledgements

The author would like to thank Calin Chindris for his support along the preparation of this paper. The discussion with him and questions raised by him offered many insights that fostered the results in the paper. The author also gives thanks to Alfonso Zamora, Alana Huszar, and Gábor Ivanyos, Youming Qiao for kindly answering the author's questions on certain results in the papers [Zamora 2014], [Huszar 2021], and [Ivanyos et al. 2018] respectively. Finally, the author thanks a referee for clarifying the complexity of the algorithms presented.

References

[Chindris and Kline 2021] C. Chindris and D. Kline, "Simultaneous robust subspace recovery and semi-stability of quiver representations", *J. Algebra* **577**:1 (2021), 210–236. MR Zbl

[Hille and de la Peña 2002] L. Hille and J. A. de la Peña, "Stable representations of quivers", *J. Pure Appl. Algebra* **172**:2-3 (2002), 205–224. MR Zbl

[Hoskins 2014] V. Hoskins, "Stratifications associated to reductive group actions on affine spaces", *Q. J. Math.* **65**:3 (2014), 1011–1047. MR Zbl

[Huszar 2021] A. Huszar, "Non-commutative rank and semi-stability of quiver representations", preprint, 2021. arXiv 2111.00039

[Ivanyos et al. 2015] G. Ivanyos, M. Karpinski, Y. Qiao, and M. Santha, "Generalized Wong sequences and their applications to Edmonds' problems", *J. Comput. System Sci.* **81**:7 (2015), 1373–1386. MR Zbl

[Ivanyos et al. 2018] G. Ivanyos, Y. Qiao, and K. V. Subrahmanyam, "Constructive non-commutative rank computation is in deterministic polynomial time", *Comput. Complexity* **27**:4 (2018), 561–593. MR Zbl

[Kempf 1978] G. R. Kempf, "Instability in invariant theory", *Ann. of Math.* (2) **108**:2 (1978), 299–316. MR Zbl

[King 1994] A. D. King, "Moduli of representations of finite-dimensional algebras", *Quart. J. Math. Oxford Ser.* (2) **45**:4 (= 180) (1994), 515–530. MR Zbl

[Mumford et al. 1994] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, 3rd ed., Ergebnisse der Math. (2) **34**, Springer, 1994. MR Zbl

[Zamora 2014] A. Zamora, "On the Harder–Narasimhan filtration for finite dimensional representations of quivers", *Geom. Dedicata* **170** (2014), 185–194. MR Zbl

Communicated by Victor Reiner
Received 2022-06-24 Revised 2023-01-16 Accepted 2023-03-20

ccheng@citadel.edu *University of Missouri, Columbia, MO, United States*

ALGEBRA AND NUMBER THEORY 18:2 (2024)
https://doi.org/10.2140/ant.2024.18.349

Sur les espaces homogènes de Borovoi–Kunyavskii

Nguyễn Mạnh Linh

Nous établissons le principe de Hasse et l'approximation faible pour certains espaces homogènes de SL_m à stabilisateur géométrique nilpotent de classe 2, construits par Borovoi et Kunyavskii. Ces espaces homogènes vérifient donc une conjecture de Colliot-Thélène concernant l'obstruction de Brauer–Manin pour les variétés géométriquement rationnellement connexes.

We establish the Hasse principle and the weak approximation property for certain homogeneous spaces of SL_m whose geometric stabilizer is of nilpotency class 2, which were constructed by Borovoi and Kunyavskii. These homogeneous spaces verify thus a conjecture of Colliot-Thélène on the Brauer–Manin obstruction for geometrically rationally connected varieties.

1. Introduction

1A. ***Intérêt du problème.*** Soit X une variété lisse définie sur un corps de nombres k. On dira que X est un contre-exemple au principe de Hasse si X possède des points locaux dans tous les complétés k_v de k mais $X(k) = \varnothing$. Manin [1971] a introduit une méthode générale pour l'étude des obstructions à l'existence de k-points sur X: à X on associe le groupe de Brauer non ramifié $\mathrm{Br}_{\mathrm{nr}}\, X$ et l'on considère l'*accouplement de Brauer–Manin*

$$\prod_v X(k_v) \times \mathrm{Br}_{\mathrm{nr}}\, X, \quad \langle (P_v)_v, A\rangle_{\mathrm{BM}} = \sum_v \mathrm{inv}_v(A(P_v)), \tag{1-1}$$

où v parcourt les places de k, et où $\mathrm{inv}_v : \mathrm{Br}\, k_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$ désigne l'invariant local. Notant $\mathrm{Br}_0\, X = \mathrm{Im}(\mathrm{Br}\, k \to \mathrm{Br}\, X)$, on voit par la loi de réciprocité globale que l'accouplement (1-1) se factorise par $(\mathrm{Br}_{\mathrm{nr}}\, X)/(\mathrm{Br}_0\, X)$.

MSC2020: 11R34, 14G05, 14G12.
Mots-clefs: Galois cohomology, lien, nonabelian cohomology, homogeneous spaces, rational points, Hasse principle, weak approximation, Brauer–Manin obstruction.

On plonge $X(k)$ diagonalement dans $\prod_v X(k_v)$. Alors l'adhérence de $X(k)$ (pour la topologie produit) est contenue dans l'ensemble (fermé) $\left(\prod_v X(k_v)\right)^{\mathrm{Br}}$ des familles de points locaux de X qui sont orthogonales à $\mathrm{Br}_{\mathrm{nr}} X$ par rapport à l'accouplement (1-1). Si $X(k) \neq \varnothing$, on dira que l'*obstruction de Brauer–Manin à l'approximation faible pour X est la seule* si $X(k)$ est dense dans $\left(\prod_v X(k_v)\right)^{\mathrm{Br}}$. On dira que l'*obstruction de Brauer–Manin au principe de Hasse est la seule* pour une classe $\mathscr{X}$ de variétés lisses sur k si pour toute variété $X \in \mathscr{X}$, $\left(\prod_v X(k_v)\right)^{\mathrm{Br}} \neq \varnothing$ entraîne $X(k) \neq \varnothing$. Notons que ces deux propriétés sont des invariants birationnels stables.

Une conjecture de Colliot-Thélène [Colliot-Thélène et Skorobogatov 2021, Conjecture 14.1.2] prédit que l'obstruction de Brauer–Manin au principe de Hasse et à l'approximation faible est la seule pour les espaces homogènes de groupes algébriques linéaires. À la suite du travail de Demarche et Lucchini Arteche [2019], le cas général se réduit au cas où le groupe ambiant est SL_m et où le stabilisateur géométrique est fini. On sait que cette conjecture vaut si le stabilisateur est abélien [Borovoi 1996, Theorem 2.2] : dans ce cas l'obstruction à l'existence de k-points sur X est en fait contrôlée par un morphisme $Б(X) \to \mathbb{Q}/\mathbb{Z}$, où $Б(X)$ est un sous-groupe de $(\mathrm{Br}_{\mathrm{nr}} X/\mathrm{Br}_0 X)$, c'est la *première obstruction de Brauer–Manin* de X. Dans le cas où le stabilisateur géométrique n'est pas abélien, on ne sait pas si le groupe $Б(X)$ est suffisant pour expliquer le défaut du principe de Hasse. Borovoi et Kunyavskii ont essayé [1997] de construire un espace homogène où l'obstruction par rapport à $Б(X)$ ne suffit pas, mais il s'avère que cette construction ne marche pas [Borovoi et Kunyavskii 2001]. Nous allons, dans ce texte, étudier leur construction (qu'on va appeler *espaces homogènes de Borovoi–Kunyavskii*), et notamment nous montrons que ces espaces homogènes vérifient toujours le principe de Hasse ainsi que l'approximation faible ; ils vérifient donc la conjecture de Colliot-Thélène mentionnée ci-dessus (en fait il n'y pas d'obstruction de Brauer–Manin pour ceux-ci).

Il est à noter qu'un résultat récent de Harpaz et Wittenberg [2020, théorème B] dit que la conjecture de Colliot-Thélène vaut si le stabilisateur géométrique est *hyper-résoluble* (en tant que groupe fini muni d'une action extérieure du groupe de Galois absolu). Cela n'est pas toujours le cas pour les espaces homogènes de Borovoi–Kunyavskii (voir le corollaire 1.3 ci-dessous), malgré le fait que les stabilisateurs de ceux-ci sont nilpotents (un groupe *abstrait* fini et nilpotent est toujours hyper-résoluble, mais ce n'est pas le cas pour les groupes algébriques finis).

1B. ***Notations et conventions.*** On va fixer dans ce texte quelques notations.

Si K est un corps parfait, $\overline{K}$ désigne une clôture algébrique de K et $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$ est le groupe de Galois absolu de K.

Soit K un corps de caractéristique nulle. Si F est un K-groupe fini (un schéma en groupes fini sur $\mathrm{Spec}\, K$), on l'identifiera au groupe abstrait $F(\overline{K})$ muni de l'action naturelle de Γ_K. On note aussi $\hat{F} = \mathrm{Hom}(F, \overline{K}^\times)$ le Γ_K-module des caractères de F.

Lorsque F est un groupe abstrait ou un schéma en groupes, on note $[F, F]$ son sous-groupe dérivé, $F^{\mathrm{ab}} = F/[F, F]$ son abélianisé, $Z(F)$ son centre, $\mathrm{Aut}(F)$ son groupe des automorphismes (en tant que groupe abstrait), $\mathrm{Int}(F) = F/Z(F)$ son groupe des automorphismes intérieurs, $\mathrm{int}(f) \in \mathrm{Int}(F)$

la conjugaison par un élément $f \in F$, et $\mathrm{Out}(F) = \mathrm{Aut}(F)/\mathrm{Int}(F)$ son groupe des automorphismes extérieurs. Si F est un groupe fini et Γ est un groupe profini, une action (resp. *action extérieure*) de Γ sur F est un morphisme *continu* (i.e., localement constant) de Γ dans $\mathrm{Aut}(F)$ (resp. dans $\mathrm{Out}(F)$).

Rappelons la notion de groupe fini hyper-résoluble au sens de Harpaz–Wittenberg [2020, définition 6.4]. Soit $\kappa : \Gamma \to \mathrm{Out}(F)$ une action extérieure d'un groupe profini Γ sur un groupe fini F. Un sous-groupe distingué G de F est dit stable sous κ si pour tout $\sigma \in \Gamma$, il existe un relevé $\phi \in \mathrm{Aut}(F)$ de $\kappa(\sigma)$ tel que $\phi(G) \subseteq G$ (dans ce cas, comme G est un sous-groupe distingué de F, tous les relevés de $\kappa(\sigma)$ vérifient cette propriété). On dit que F (muni de l'action extérieure κ) est hyper-résoluble s'il existe un entier n et une suite

$$\{1\} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

de sous-groupes distingués de F, stables sous κ, tels que F_i/F_{i-1} soit cyclique pour tout $i \in \{1, \dots, n\}$. Il est clair que dans ce cas, pour tout sous-groupe distingué G de F qui est stable sous κ, le quotient F/G muni de l'action extérieure de Γ induite par κ est également hyper-résoluble [1].

Les cohomologies utilisées seront cohomologie de groupes profinis, cohomologie galoisienne et cohomologie étale. On dispose aussi de la notion des H^0 et H^1 non abéliens. Le H^2 non abélien, défini dans [Flicker et al. 1998, § 1], sera mentionné dans le paragraphe 3A.

Si G est un groupe et H est un sous-groupe distingué de G, l'image d'un élément $\sigma \in G$ dans G/H sera notée $\bar{\sigma}$. Pour tout $r \geqslant 1$, l'image dans H^r d'un r-cocycle a de Z^r sera notée $[a]$.

Si G est un groupe abstrait et $P \subseteq G$, $\langle P\rangle$ désigne le sous-groupe de G (algébriquement) engendré par P. Si de plus G est supposé topologique, l'adhérence $\overline{\langle P\rangle}$ est le sous-groupe de G topologiquement engendré par P.

Soit k un corps de nombres. L'ensemble des places de k sera noté Ω_k. Si A est un Γ_k-module, r est un entier et $v \in \Omega_k$, on notera $\mathrm{loc}_v : \mathrm{H}^r(k, A) \to \mathrm{H}^r(k_v, A)$ le morphisme de localisation, et $\alpha_v = \mathrm{loc}_v(\alpha)$ pour tout $\alpha \in \mathrm{H}^r(k, A)$. De plus, on définit les sous-groupes

$$Ш^r_S(k, A) := \mathrm{Ker}\left(\mathrm{H}^r(k, A) \to \prod_{v \in \Omega_k \setminus S} \mathrm{H}^r(k_v, A)\right)$$

pour tout sous-ensemble fini $S \subseteq \Omega_k$, et

$$Ш^r_\omega(k, A) := \bigcup_S Ш^r_S(k, A), \qquad Ш^r(k, A) := Ш^r_\varnothing(k, A).$$

Soit X une variété lisse et géométriquement intègre sur un corps K de caractéristique nulle. Le groupe de Brauer de X est toujours le groupe de Brauer–Grothendieck $\mathrm{Br}\, X := \mathrm{H}^2(X, \mathbb{G}_m)$. Le groupe de Brauer non ramifié $\mathrm{Br}_{\mathrm{nr}}\, X$ est le groupe de Brauer de n'importe quelle variété propre et lisse contenant X comme un ouvert dense ; c'est naturellement un sous-groupe de $\mathrm{Br}\, X$, et c'est un invariant birationnel stable [Colliot-Thélène et Skorobogatov 2021, § 6.2]. Si K est un corps, le groupe de Brauer de K est alors $\mathrm{Br}\, K = \mathrm{H}^2(K, \mathbb{G}_m)$. Notons que $\mathrm{H}^2(K, \mu_n) = (\mathrm{Br}\, K)[n]$ pour tout entier n. Dans le cas où K est un corps

[1] Attention, κ n'induit pas forcément une action extérieure de Γ sur G.

p-adique ou $\mathbb{R}$ ou $\mathbb{C}$, $\mathrm{inv}_K : \mathrm{Br}\, K \hookrightarrow \mathbb{Q}/\mathbb{Z}$ désigne l'invariant local. Si k un corps de nombres et v est une place de k, on notera $\mathrm{inv}_v = \mathrm{inv}_{k_v}$.

Rappelons aussi l'interprétation cohomologique suivante de l'approximation faible, dont la preuve peut se trouver par exemple dans [Harari 2007, § 1.2].

Lemme 1.1. *Soient k un corps de nombres et F un k-groupe fini. On choisit un plongement $F \hookrightarrow \mathrm{SL}_m$ de k-groupes et l'on pose $X = F \backslash \mathrm{SL}_m$. Alors pour tout sous-ensemble fini $S \subseteq \Omega_k$, on a équivalence entre :*

1. *$X(k)$ est dense dans $\prod_{v \in S} X(k_v)$.*
2. *La restriction $\mathrm{H}^1(k, F) \to \prod_{v \in S} \mathrm{H}^1(k_v, F)$ est surjective.*

1C. *Énoncés des principaux théorèmes.* Soit k un corps de nombres. On rappelle la construction de Borovoi–Kunyavskii. On construit une extension centrale de k-groupes finis

$$0 \to Z \to F \to M \oplus M \to 0 \tag{1-2}$$

avec $Z = Z(F) = [F, F]$ (donc F est nilpotent de classe 2) et on considère les espaces homogènes X de SL_m à stabilisateur géométrique F. Dans le paragraphe 3, cette construction sera discutée en détail. Pour le stabilisateur F comme dans les théorèmes A et B ci-dessous, on verra dans le paragraphe 4 qu'il n'y a pas d'obstruction de Brauer–Manin pour ces espaces homogènes X : leurs groupes de Brauer non ramifiés sont réduits aux constantes (proposition 5.4).

Voici les principaux résultats de ce texte.

Théorème A. *Soient A un groupe abélien fini, k un corps de nombres contenant $\mu_{\exp(A)}$, L/k une extension finie galoisienne, $M = \mathrm{Ind}_{\Gamma_k}^{\Gamma_L} A$, $j : A \otimes A \hookrightarrow M \otimes M$ l'inclusion canonique, Z le conoyau de j et $\phi : M \otimes M \to Z$ la projection. On définit l'application biadditive*

$$\Phi : (M \oplus M) \times (M \oplus M) \to Z, \quad \Phi((x, y), (x', y')) = \phi(x \otimes y'),$$

vue comme 2-cocycle normalisé sur $M \oplus M$ à coefficients dans Z (muni de l'action triviale de $M \oplus M$) et soit F le produit croisé $Z \times_\Phi (M \oplus M)$, muni de l'action coordonnée par coordonnée de Γ_k. Alors les espaces homogènes de SL_m *de lien de Springer* $\mathrm{lien}(F)$ *(voir paragraphe 3A pour la définition du lien de Springer d'un espace homogène) vérifient le principe de Hasse.*

Théorème B. *Avec les mêmes hypothèses du théorème A, soit X un espace homogène de* SL_m *de lien de Springer* $\mathrm{lien}(F)$. *Si $X(k) \neq \varnothing$, alors X vérifie l'approximation faible.*

Les théorèmes A et B seront démontrés dans les paragraphes 5C et 5D. Leurs preuves reposent sur des calculs cohomologiques : comme $M = \mathrm{Ind}_{\Gamma_k}^{\Gamma_L} A$, on peut utiliser le lemme de Shapiro pour passer de $\mathrm{H}^r(k, M)$ à $\mathrm{H}^r(L, A)$. La compatibilité avec l'isomorphisme de Shapiro de certaines applications sera donc nécessaire, et nous allons en discuter au paragraphe 2.

Pour toute extension K de k, la flèche connectante $\Delta : \mathrm{H}^1(K, M \oplus M) \to \mathrm{H}^2(K, Z)$ induite par l'extension centrale (1-2) s'exprime en termes de cup-produits (voir lemme 3.8). Cette observation importante nous permet de réduire le problème des points rationnels sur X aux calculs cohomologiques.

L’argument clé sera le théorème 5.5, qui est lui-même une application d’un « lemme arithmétique », les propositions 5.1 et 5.2 du paragraphe 5A. Ces propositions sont des généralisations de [Serre 1970, chapitre III, §2.2, théorème 4], qui décrivent une propriété globale du symbole de Hilbert, et dont les démonstrations reposent sur la dualité de Poitou–Tate.

Montrons que le stabilisateur des espaces homogènes de Borovoi–Kunyavskii comme dans l’énoncé du théorème A n’est pas toujours hyper-résoluble au sens de Harpaz–Wittenberg.

Lemme 1.2. *Soit $\mathfrak{g}$ le groupe cyclique $\langle g : g^3 = 1\rangle$ et soit $M = (\mathbb{Z}/2)[\mathfrak{g}] = \bigoplus_{i=0}^{2}(\mathbb{Z}/2)e_i$. Alors le quotient $\overline{M} = M/(e_0 + e_1 + e_2)$ est un $\mathfrak{g}$-module simple mais pas un groupe cyclique.*

Démonstration. Le groupe $\overline{M}$ est bien un $\mathfrak{g}$-module puisque $e_0 + e_1 + e_2 \in M$ est fixé par $\mathfrak{g}$. Il est d’ordre 4 et d’exposant 2 donc non cyclique. Montrons qu’il est un $\mathfrak{g}$-module simple. Soit $N \subseteq \overline{M}$ un sous-groupe $\mathfrak{g}$-stable et supposons $N \neq 0$. Soit $x \in N \setminus \{0\}$ et affirmons que x n’est pas fixé par $\mathfrak{g}$. En effet, on peut écrire $x = \overline{a_1e_1 + a_2e_2}$, où $a_1, a_2 \in \mathbb{Z}/2$. Alors ${}^{g}x = \overline{a_1e_0 + a_2e_1}$. Si ${}^{g}x = x$, alors il existe $b \in \mathbb{Z}/2$ tel que $a_1e_0 + a_2e_1 = a_1e_1 + a_2e_2 + b(e_0 + e_1 + e_2)$, d’où

$$a_1 = b, \quad a_2 = a_1 + b, \quad a_2 + b = 0,$$

et donc $a_1 = a_2 = 0$, ou $x = 0$. Cette contradiction montre qu’en fait on a ${}^{g}x \neq x$. On en déduit que N contient quatre éléments deux à deux distincts, à savoir 0, x, ${}^{g}x$ et ${}^{g^2}x$. Comme $\overline{M}$ est d’ordre 4, on voit que $N = \overline{M}$, ce qui montre que $\overline{M}$ n’a pas de sous-groupe $\mathfrak{g}$-stable non trivial. □

Corollaire 1.3. *Soit L/k une extension galoisienne de degré 3 de corps de nombres et $M = \mathrm{Ind}_{\Gamma_k}^{\Gamma_L} \mu_2$. De M, on construit le k-groupe fini F comme dans l’énoncé du théorème A. Alors F n’est pas hyper-résoluble (en tant que groupe fini muni de l’action extérieure de Γ_k).*

Démonstration. En effet, si F était hyper-résoluble, alors $M \oplus M = F/Z$ serait un Γ_k-module hyper-résoluble. On en déduirait que ce serait aussi le cas pour M et le quotient $\overline{M}$ comme dans le lemme 1.2. Mais $\overline{M}$ est un Γ_k-module simple non cyclique, donc non hyper-résoluble. Ainsi, F n’est pas hyper-résoluble. □

2. Compatibilité avec les isomorphismes de Shapiro

Dans cette section, G est un groupe profini et H est un sous-groupe ouvert, distingué de G.

Soit r un entier. On rappelle que si A est un groupe abélien muni de l’action triviale de H, le groupe $\mathrm{Z}^r(H, A)$ des r-cocycles $H^r \to A$ est muni de l’action suivante de G :

$${}^{\sigma}a_{\tau_1,\dots,\tau_r} = a_{\sigma^{-1}\tau_1\sigma,\dots,\sigma^{-1}\tau_r\sigma} \quad \forall \sigma \in G,\ \forall a \in \mathrm{Z}^r(H, A),\ \forall \tau_1, \dots, \tau_r \in H.$$

Cette action induit une action de G sur le groupe $\mathrm{H}^r(H, A)$. Le groupe H agit trivialement sur $\mathrm{H}^r(H, A)$ puisque les automorphismes intérieurs de H induisent l’identité. On obtient ainsi une action de G/H sur $\mathrm{H}^r(H, A)$. Pour le reste de cette section, soit $M = \mathrm{Ind}_G^H A$ (voir [Serre 1994, chapitre I, §2.5] pour la notion de module induit). Alors M est un G-module discret dont le groupe abélien sous-jacent est celui des applications $G/H \to A$, et dont l'action de G est donnée par la formule

$$^{\sigma}f(g) = f(g\bar{\sigma}) \quad \forall \sigma \in G,\ \forall f \in M,\ \forall g \in G/H.$$

Pour tout $r \geqslant 1$, on dispose d'un morphisme

$$\mathrm{sh} : \mathrm{Z}^r(G, M) \to \mathrm{Z}^r(H, A)$$

qui à chaque r-cocycle $a : G^r \to M$ associe le r-cocycle

$$H^r \to A, \quad (\sigma_1, \ldots, \sigma_r) \mapsto a_{\sigma_1,\ldots,\sigma_r}(1).$$

Le lemme de Shapiro affirme que sh induit un isomorphisme $\mathrm{sh} : \mathrm{H}^r(G, M) \to \mathrm{H}^r(H, A)$. Le but de cette section est de donner quelques résultats de compatibilité des isomorphismes de Shapiro avec certaines applications.

2A. ***Quasi-inverses aux applications de Shapiro.*** On fixe une section (ensembliste) $u : G/H \to G$ avec $u(1) = 1$. Pour tous $g \in G/H$ et $\sigma \in G$, posons $\gamma(g, \sigma) := u(g)\sigma u(g\bar{\sigma})^{-1}$. Alors $\gamma(g, \sigma) \in H$ puisque son image dans G/H est $g\bar{\sigma}(g\bar{\sigma})^{-1} = 1$. L'application $\gamma : G/H \times G \to H$ est continue. Elle vérifie une « condition de cocycle » :

$$\gamma(g, \sigma\tau) = \gamma(g, \sigma)\gamma(g\bar{\sigma}, \tau) \quad \forall g \in G/H,\ \forall \sigma, \tau \in G. \tag{2-1}$$

Les résultats suivants décrivent des morphismes $\mathrm{Z}^r(H, A) \to \mathrm{Z}^r(G, M)$ pour $r = 1, 2$, qui induisent des inverses de sh au niveau de la cohomologie. Ils sont inspirés par [Naidu 2007, Lemma 2.1, Lemma 2.2].

Lemme 2.1. *Soit $a \in \mathrm{H}^1(H, A)$, vu comme morphisme continu $H \to A$. Soit $x : G \to M$ l'application continue définie par*

$$x_\sigma(g) = a_{\gamma(g,\sigma)} \quad \forall \sigma \in G,\ \forall g \in G/H.$$

Alors x est un 1-cocycle. De plus, pour tous $\sigma \in H$ et $g \in G/H$, on a $x_\sigma(g) = {}^{u(g)^{-1}}a_\sigma$. En particulier, $\mathrm{sh}(x) = a$.

Démonstration. Pour tous $g \in G/H$ et $\sigma, \tau \in G$, au vu de (2-1), on a

$$x_{\sigma\tau}(g) = a_{\gamma(g,\sigma\tau)} = a_{\gamma(g,\sigma)\gamma(g\bar{\sigma},\tau)} = a_{\gamma(g,\sigma)} + a_{\gamma(g\bar{\sigma},\tau)} = x_\sigma(g) + x_\tau(g\bar{\sigma}) = x_\sigma(g) + {}^{\sigma}x_\tau(g),$$

d'où $x_{\sigma\tau} = x_\sigma + {}^{\sigma}x_\tau$, donc x est bien un 1-cocycle.

Soient $\sigma \in H$ et $g \in G/H$. Alors $\gamma(g, \sigma) = u(g)\sigma u(g\bar{\sigma})^{-1} = u(g)\sigma u(g)^{-1}$, d'où

$$x_\sigma(g) = a_{u(g)\sigma u(g)^{-1}} = {}^{u(g)^{-1}}a_\sigma.$$

En particulier, $x_\sigma(1) = a_\sigma$ puisque $u(1) = 1$ et donc $\mathrm{sh}(x) = a$. □

Lemme 2.2. *Soit $a \in \mathrm{Z}^2(H, A)$. Soit $x : G \times G \to M$ l'application continue définie par*

$$x_{\sigma,\tau}(g) = a_{\gamma(g,\sigma),\gamma(g\bar{\sigma},\tau)} \quad \forall \sigma, \tau \in G,\ \forall g \in G/H.$$

Alors x est un 2-cocycle. De plus, pour tous $\sigma, \tau \in H$ et $g \in G/H$, on a $x_{\sigma,\tau}(g) = {}^{u(g)^{-1}}a_{\sigma,\tau}$. En particulier, $\mathrm{sh}(x) = a$.

Démonstration. Pour tous $g \in G/H$ et $\sigma, \tau, \upsilon \in G$, on a

$$\begin{aligned} &{}^{\sigma}x_{\tau,\upsilon}(g) - x_{\sigma\tau,\upsilon}(g) + x_{\sigma,\tau\upsilon}(g) - x_{\sigma,\tau}(g) \\ &\qquad = x_{\tau,\upsilon}(g\bar{\sigma}) - x_{\sigma\tau,\upsilon}(g) + x_{\sigma,\tau\upsilon}(g) - x_{\sigma,\tau}(g) \\ &\qquad = a_{\gamma(g\bar{\sigma},\tau),\gamma(g\overline{\sigma\tau},\upsilon)} - a_{\gamma(g,\sigma\tau),\gamma(g\overline{\sigma\tau},\upsilon)} + a_{\gamma(g,\sigma),\gamma(g\bar{\sigma},\tau\upsilon)} - a_{\gamma(g,\sigma),\gamma(g\bar{\sigma},\tau)} \\ &\qquad \overset{(2\text{-}1)}{=} a_{\gamma(g\bar{\sigma},\tau),\gamma(g\overline{\sigma\tau},\upsilon)} - a_{\gamma(g,\sigma)\gamma(g\bar{\sigma},\tau),\gamma(g\overline{\sigma\tau},\upsilon)} + a_{\gamma(g,\sigma),\gamma(g\bar{\sigma},\tau)\gamma(g\overline{\sigma\tau},\upsilon)} - a_{\gamma(g,\sigma),\gamma(g\bar{\sigma},\tau)} \\ &\qquad = 0, \end{aligned}$$

où la dernière égalité découle du fait que a est un 2-cocycle. De là, ${}^{\sigma}x_{\tau,\upsilon} - x_{\sigma\tau,\upsilon} + x_{\sigma,\tau\upsilon} - x_{\sigma,\tau} = 0$ et donc x est bien un 2-cocycle.

Soient $\sigma, \tau \in H$ et $g \in G/H$. Alors $\gamma(g,\sigma) = u(g)\sigma u(g\bar{\sigma})^{-1} = u(g)\sigma u(g)^{-1}$ et $\gamma(g\bar{\sigma},\tau) = u(g\bar{\sigma})\tau u(g\overline{\sigma\tau})^{-1} = u(g)\tau u(g)^{-1}$, d'où

$$x_{\sigma,\tau}(g) = a_{u(g)\sigma u(g)^{-1},u(g)\tau u(g)^{-1}} = {}^{u(g)^{-1}}a_{\sigma,\tau}.$$

En particulier, $x_{\sigma,\tau}(1) = a_{\sigma,\tau}$ puisque $u(1) = 1$ et donc $\mathrm{sh}(x) = a$. □

2B. *Description globale.* À partir de ce paragraphe, on identifie $M \otimes M$ au groupe des applications $G/H \times G/H \to A \otimes A$, muni de l'action de G définie par

$${}^{\sigma}f(g,h) = f(g\bar{\sigma}, h\bar{\sigma}) \quad \forall \sigma \in G,\ \forall f \in M \otimes M,\ \forall g, h \in G/H.$$

Alors pour tous $f_1, f_2 \in M$, l'élément $f_1 \otimes f_2 \in M \otimes M$ est donné par

$$(f_1 \otimes f_2)(g,h) = f_1(g) \otimes f_2(h) \quad \forall g, h \in G/H.$$

Pour tout $g \in G/H$, on définit le morphisme

$$\omega_g : M \otimes M \to \mathrm{Ind}_G^H(A \otimes A) = \{G/H \to A \otimes A\}, \quad \omega_g(f)(h) = f(gh, h). \tag{2-2}$$

On vérifie sans peine que ω_g est G-équivariant. Soit $\omega = (\omega_g)_{g \in G/H} : M \otimes M \to (\mathrm{Ind}_G^H(A \otimes A))^{[G:H]}$. Explicitons la composée $\mathrm{sh}' = \mathrm{sh}^{[G:H]} \circ \omega_* : \mathrm{Z}^r(G, M \otimes M) \to \mathrm{Z}^r(H, A \otimes A)^{[G:H]}$ pour tout $r \geqslant 1$.

Lemme 2.3. *Soit $r \geqslant 1$.*

1. *ω est un isomorphisme de G-modules* (*donc* $\mathrm{sh}' : \mathrm{H}^r(G, M \otimes M) \to \mathrm{H}^r(H, A \otimes A)^{[G:H]}$ *est un isomorphisme*).

2. *Soit $x \in \mathrm{Z}^r(G, M \otimes M)$. Pour tout $g \in G/H$, soit $a_g \in \mathrm{Z}^r(H, A \otimes A)$ le r-cocycle $(\sigma_1, \dots, \sigma_r) \mapsto x_{\sigma_1,\dots,\sigma_r}(g, 1)$. Alors $\mathrm{sh}'(x) = (a_g)_{g \in G/H}$.*

Démonstration. 1. Montrons l'injectivité de ω. Soit $f \in M \otimes M$ tel que $\omega(f) = 0$. Alors

$$f(g, h) = f(gh^{-1}h, h) = \omega_{gh^{-1}}(f)(h) = 0$$

pour tous $g, h \in G/H$, d'où $f = 0$.

Montrons maintenant que ω est surjectif. Soit alors $(f_g)_{g \in G/H}$ une famille d'applications $G/H \to A \otimes A$. On définit l'élément $f \in M \otimes M$ par

$$f(g, h) = f_{gh^{-1}}(h) \quad \forall g, h \in G/H.$$

Pour tous $g, h \in G/H$, on a $\omega_g(f)(h) = f(gh, h) = f_{ghh^{-1}}(h) = f_g(h)$, d'où $\omega_g(f) = f_g$ et donc $\omega(f) = (f_g)_{g \in G/H}$.

2. Pour tous $\sigma_1, \dots, \sigma_r \in H$ et $g \in G/H$, on a

$$((\omega_g)_* x)_{\sigma_1,\dots,\sigma_r}(1) = \omega_g(x_{\sigma_1,\dots,\sigma_r})(1) = x_{\sigma_1,\dots,\sigma_r}(g, 1) = (a_g)_{\sigma_1,\dots,\sigma_r},$$

donc $\mathrm{sh}((\omega_g)_* x) = a_g$, d'où $\mathrm{sh}'(x) = (\mathrm{sh}((\omega_g)_* x))_{g \in G/H} = (a_g)_{g \in G/H}$. □

Décrivons l'application $\mathrm{H}^1(H, A) \times \mathrm{H}^1(H, A) \to \mathrm{H}^2(H, A \otimes A)^{[G:H]}$ associée au cup-produit

$$\cup : \mathrm{H}^1(G, M) \times \mathrm{H}^1(G, M) \to \mathrm{H}^2(G, M \otimes M).$$

Lemme 2.4. *On a un diagramme commutatif, où les flèches verticales sont des isomorphismes :*

$$\begin{tikzcd}
\mathrm{H}^1(H, A) \times \mathrm{H}^1(H, A) \arrow[r, "(a,b) \mapsto ({}^{g^{-1}}a \cup b)_{g \in G/H}"] & \mathrm{H}^2(H, A \otimes A)^{[G:H]} \\
\mathrm{H}^1(G, M) \times \mathrm{H}^1(G, M) \arrow[u, "\mathrm{sh}"', "\mathrm{sh}"] \arrow[r, "\cup"] & \mathrm{H}^2(G, M \otimes M) \arrow[u, "\mathrm{sh}'"']
\end{tikzcd}$$

Démonstration. Soient $a, b \in \mathrm{H}^1(H, A)$, vus comme morphismes continus $H \to A$. Soient $x, y : G \to M$ les 1-cocycles représentant les classes $\mathrm{sh}^{-1}(a), \mathrm{sh}^{-1}(b) \in \mathrm{H}^1(G, M)$ respectivement, qui sont construits dans le lemme 2.1. Alors l'on a $x_\sigma(g) = {}^{u(g)^{-1}}a_\sigma$ et $y_\sigma(g) = {}^{u(g)^{-1}}b_\sigma$ pour tous $\sigma \in H$ et $g \in G/H$ (où $u(g) \in G$ désigne un relevé de g).

Regardons le cup-produit $x \cup y \in \mathrm{Z}^2(G, M \otimes M)$. Pour tous $g \in G/H$ et $\sigma, \tau \in H$, on a

$$(x \cup y)_{\sigma,\tau}(g, 1) = (x_\sigma \otimes {}^\sigma y_\tau)(g, 1) = (x_\sigma \otimes y_\tau)(g, 1) = x_\sigma(g) \otimes y_\tau(1) = {}^{u(g)^{-1}}a_\sigma \otimes b_\tau = ({}^{u(g)^{-1}}a \cup b)_{\sigma,\tau}.$$

Par le lemme 2.3, on a $\mathrm{sh}'(x \cup y) = ({}^{u(g)^{-1}}a \cup b)_{g \in G/H}$ dans $\mathrm{Z}^2(H, A \otimes A)^{[G:H]}$, ce qui implique que $\mathrm{sh}'([x] \cup [y]) = ({}^{g^{-1}}a \cup b)_{g \in G/H}$ dans $\mathrm{H}^2(G, A \otimes A)^{[G:H]}$, d'où le lemme. □

Lemme 2.5. *On munit A de l'action triviale de G. Soit $j : A \otimes A \hookrightarrow M \otimes M$ l'inclusion G-équivariante qui à tout $m \in A \otimes A$ associe l'application*

$$G/H \times G/H \to A \otimes A, \quad (g, h) \mapsto m.$$

Soit $r \geqslant 1$ et soit $\mathrm{res} : \mathrm{Z}^r(G, A \otimes A) \to \mathrm{Z}^r(H, A \otimes A)$ le morphisme de restriction. Alors l'on dispose d'un diagramme commutatif, où la flèche verticale est un isomorphisme :

$$\begin{tikzcd}
\mathrm{H}^r(G, A \otimes A) \arrow[r, "{(\mathrm{res},\ldots,\mathrm{res})}"] \arrow[dr, "j_*"'] & \mathrm{H}^r(H, A \otimes A)^{[G:H]} \\
& \mathrm{H}^r(G, M \otimes M) \arrow[u, "\mathrm{sh}'"']
\end{tikzcd}$$

Démonstration. Soit $x \in \mathrm{Z}^r(G, A \otimes A)$. Alors $(j_* x)_{\sigma_1,\ldots,\sigma_r}(g, 1) = j(x_{\sigma_1,\ldots,\sigma_r})(g, 1) = x_{\sigma_1,\ldots,\sigma_r}$ pour tous $\sigma_1, \ldots, \sigma_r \in H$ et $g \in G/H$. Par le lemme 2.3, on a $\mathrm{sh}'(j_* x) = (\mathrm{res}(x), \ldots, \mathrm{res}(x))$ dans $\mathrm{Z}^r(H, A \otimes A)^{[G:H]}$ et donc $\mathrm{sh}'(j_*[x]) = (\mathrm{res}([x]), \ldots, \mathrm{res}([x]))$ dans $\mathrm{H}^r(H, A \otimes A)^{[G:H]}$. □

2C. ***Description locale.*** Dans ce paragraphe et celui qui le suit, on prend $G = \Gamma_k$ et $H = \Gamma_L$, où L/k est une extension finie galoisienne de corps de nombres. Posons $\mathfrak{g} = \mathrm{Gal}(L/k) = \Gamma_k/\Gamma_L$. A est toujours groupe abélien muni de l'action triviale de Γ_L et $M = \mathrm{Ind}_{\Gamma_k}^{\Gamma_L} A$.

On fixe une place v de k, une place w de L divisant v et une extension de w à $\bar{k}$ (d'où une inclusion $\Gamma_{k_v} \subseteq \Gamma_k$ avec $\Gamma_{L_w} = \Gamma_{k_v} \cap \Gamma_L$). Soit $\mathfrak{g}_v = \mathrm{Gal}(L_w/k_v) = \Gamma_{k_v}/\Gamma_{L_w} \subseteq \mathfrak{g}$ le groupe de décomposition de $w|v$. On choisit un système de représentants $\mathscr{E}_v$ des classes à gauche de $\mathfrak{g}$ suivant $\mathfrak{g}_v$ et l'on pose $e_v = |\mathscr{E}_v| = [\mathfrak{g} : \mathfrak{g}_v]$. Alors toute place de L divisant v est de la forme sw pour un unique $s \in \mathscr{E}_v$.

Posons $M_v = \mathrm{Ind}_{\Gamma_{k_v}}^{\Gamma_{L_w}} A = \{\mathfrak{g}_v \to A\}$. Pour tout $s \in \mathscr{E}_v$, soit $\varsigma_s : M \to M_v$ le morphisme Γ_{k_v}-équivariant défini par

$$\varsigma_s(f)(h) = f(sh) \quad \forall f \in M,\ \forall h \in \mathfrak{g}_v.$$

Soit $\varsigma = (\varsigma_s)_{s \in \mathscr{E}_v} : M \to M_v^{e_v}$ et soit $\mathrm{sh}_v = \mathrm{sh}^{e_v} \circ \varsigma_* : \mathrm{Z}^r(k_v, M) \to \mathrm{Z}^r(L_w, A)^{e_v}$ pour tout $r \geqslant 1$.

Lemme 2.6. *ς est un isomorphisme de Γ_{k_v}-modules* (*donc* $\mathrm{sh}_v : \mathrm{H}^r(k_v, M) \to \mathrm{H}^r(L_w, A)^{e_v}$ *est un isomorphisme pour tout* $r \geqslant 1$).

Démonstration. Montrons l'injectivité de ς. Soit $f \in M$ tel que $\varsigma(f) = 0$. Pour tout $g \in \mathfrak{g}$, on peut écrire $g = sh$, où $s \in \mathscr{E}_v$ et $h \in \mathfrak{g}_v$. Alors $f(g) = f(sh) = \varsigma_s(f)(h) = 0$, d'où $f = 0$.

Montrons maintenant que ς est surjectif. Soit alors $(f_s)_{s \in \mathscr{E}_v}$ une famille d'éléments de M_v. On définit l'élément $f \in M$ comme suit. Pour tout $g \in \mathfrak{g}$, il existe un unique $s \in \mathscr{E}_v$ et un unique $h \in \mathfrak{g}_v$ tel que $g = sh$. On définit $f(g) = f_s(h)$. Alors l'on a $\varsigma_s(f)(h) = f(sh) = f_s(h)$ pour tous $s \in \mathscr{E}_v$ et $h \in \mathfrak{g}$, d'où $\varsigma_s(f) = f_s$ et donc $\varsigma(f) = (f_s)_{s \in \mathscr{E}_v}$. □

Par le lemme 2.6, on dispose d'un isomorphisme

$$\varsigma \otimes \varsigma = (\varsigma_s \otimes \varsigma_t)_{s,t \in \mathscr{E}_v} : M \otimes M \to M_v^{e_v} \otimes M_v^{e_v} = (M_v \otimes M_v)^{e_v^2}$$

de Γ_{k_v}-modules. Notons que pour tous $s, t \in \mathscr{E}_v$, $f_1, f_2 \in M$ et $h_1, h_2 \in \mathfrak{g}_v$, on a

$$\begin{aligned}(\varsigma_s \otimes \varsigma_t)(f_1 \otimes f_2)(h_1, h_2) = (\varsigma_s(f_1) \otimes \varsigma_t(f_2))(h_1, h_2) &= \varsigma_s(f_1)(h_1) \otimes \varsigma_t(f_2)(h_2)\\ &= f_1(sh_1) \otimes f_2(th_2) = (f_1 \otimes f_2)(sh_1, th_2).\end{aligned}$$

Mais comme $M \otimes M$ est engendré (en tant que groupe abélien) par les éléments de la forme $f_1 \otimes f_2$ (où $f_1, f_2 \in M$), on voit que

$$(\varsigma_s \otimes \varsigma_t)(f)(h_1, h_2) = f(sh_1, th_2) \quad \forall s, t \in \mathscr{E}_v,\ \forall f \in M \otimes M,\ \forall h_1, h_2 \in \mathfrak{g}_v. \tag{2-3}$$

Par le lemme 2.3 (appliqué aux groupes profinis $\Gamma_{L_w} \subseteq \Gamma_{k_v}$ et au Γ_{k_v}-module M_v), la composée

$$\mathrm{sh}'_v = (\mathrm{sh}')^{e_v^2} \circ (\varsigma \otimes \varsigma)_* : \mathrm{Z}^r(k_v, M \otimes M) \to \mathrm{Z}^r(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|}$$

induit un isomorphisme $\mathrm{H}^r(k_v, M \otimes M) \to \mathrm{H}^r(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|}$ pour tout $r \geqslant 1$.

Explicitons maintenant l'application $\mathrm{H}^1(L_w, A)^{e_v} \times \mathrm{H}^1(L_w, A)^{e_v} \to \mathrm{H}^2(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|}$ associée au cup-produit $\cup : \mathrm{H}^1(k_v, M) \times \mathrm{H}^1(k_v, M) \to \mathrm{H}^2(k_v, M \otimes M)$.

Lemme 2.7. *On a un diagramme commutatif, où les flèches verticales sont des isomorphismes* :

$$\begin{tikzcd}
\mathrm{H}^1(L_w, A)^{e_v} \times \mathrm{H}^1(L_w, A)^{e_v} \arrow[rr, "((a_s)_{s\in\mathscr{E}_v}{,}(b_s)_{s\in\mathscr{E}_v})\mapsto({}^{h^{-1}}a_s\cup b_t)_{h\in\mathfrak{g}_v{,}s{,}t\in\mathscr{E}_v}"] & & \mathrm{H}^2(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|} \\
\mathrm{H}^1(k_v, M) \times \mathrm{H}^1(k_v, M) \arrow[u, "\mathrm{sh}_v \quad \mathrm{sh}_v"'] \arrow[rr, "\cup"] & & \mathrm{H}^2(k_v, M \otimes M) \arrow[u, "\mathrm{sh}'_v"']
\end{tikzcd}$$

Démonstration. Puisque $\mathrm{sh}_v = \mathrm{sh}^{e_v} \circ \varsigma_*$ et $\mathrm{sh}'_v = (\mathrm{sh}')^{e_v^2} \circ (\varsigma \otimes \varsigma)_*$, il suffit de montrer que les deux petits carrés du diagramme suivant sont commutatifs :

$$\begin{tikzcd}
\mathrm{H}^1(L_w, A)^{e_v} \times \mathrm{H}^1(L_w, A)^{e_v} \arrow[rr, "((a_s)_{s\in\mathscr{E}_v}{,}(b_s)_{s\in\mathscr{E}_v})\mapsto({}^{h^{-1}}a_s\cup b_t)_{h\in\mathfrak{g}_v{,}s{,}t\in\mathscr{E}_v}"] & & \mathrm{H}^2(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|} \\
\mathrm{H}^1(k_v, M_v)^{e_v} \times \mathrm{H}^1(k_v, M_v)^{e_v} \arrow[u, "\mathrm{sh}^{e_v} \quad \mathrm{sh}^{e_v}"'] \arrow[rr, "((x_s)_{s\in\mathscr{E}_v}{,}(y_s)_{s\in\mathscr{E}_v})\mapsto(x_s\cup y_t)_{s{,}t\in\mathscr{E}_v}"] & & \mathrm{H}^2(k_v, M_v \otimes M_v)^{e_v^2}. \arrow[u, "(\mathrm{sh}')^{e_v^2}"'] \\
\mathrm{H}^1(k_v, M) \times \mathrm{H}^1(k_v, M) \arrow[u, "\varsigma_* \quad \varsigma_*"'] \arrow[rr, "\cup"] & & \mathrm{H}^2(k_v, M \otimes M) \arrow[u, "(\varsigma\otimes\varsigma)_*"']
\end{tikzcd} \tag{2-4}$$

Par le lemme 2.4, le diagramme

$$\begin{tikzcd}
\mathrm{H}^1(L_w, A) \times \mathrm{H}^1(L_w, A) \arrow[r, "(a{,}b)\mapsto({}^{h^{-1}}a\cup b)_{h\in\mathfrak{g}_v}"] & \mathrm{H}^2(L_w, A \otimes A)^{|\mathfrak{g}_v|} \\
\mathrm{H}^1(k_v, M_v) \times \mathrm{H}^1(k_v, M_v) \arrow[u, "\mathrm{sh} \quad \mathrm{sh}"'] \arrow[r, "\cup"] & \mathrm{H}^2(k_v, M_v \otimes M_v) \arrow[u, "\mathrm{sh}'"']
\end{tikzcd}$$

est commutatif, d'où la commutativité du carré du haut de (2-4). Le carré du bas de (2-4) commute tout simplement par fonctorialité du cup-produit. □

Le résultat suivant est une version locale du lemme 2.5.

Lemme 2.8. *On munit A de l'action triviale de Γ_k. Soit $j : A \otimes A \hookrightarrow M \otimes M$ l'inclusion Γ_k-équivariante qui à tout $m \in A \otimes A$ associe l'application*

$$\mathfrak{g} \times \mathfrak{g} \to A \otimes A, \quad (g, h) \mapsto m.$$

Soit $r \geqslant 1$ et soit $\mathrm{res} : \mathrm{Z}^r(k_v, A \otimes A) \to \mathrm{Z}^r(L_w, A \otimes A)$ *le morphisme de restriction. Alors l'on dispose d'un diagramme commutatif, où la flèche verticale est un isomorphisme :*

$$\begin{tikzcd}
\mathrm{H}^r(k_v, A \otimes A) \arrow[r, "(\mathrm{res},\dots,\mathrm{res})"] \arrow[dr, "j_*"] & \mathrm{H}^r(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|} \\
& \mathrm{H}^r(k_v, M \otimes M) \arrow[u, "\mathrm{sh}'_v"']
\end{tikzcd}$$

Démonstration. Soit $x \in \mathrm{Z}^r(k_v, A \otimes A)$. Pour tous $s, t \in \mathscr{E}_v$, $\sigma_1, \dots, \sigma_r \in \Gamma_{L_w}$ et $h \in \mathfrak{g}_v$, on a

$$((\varsigma_s \otimes \varsigma_t)_* j_* x)_{\sigma_1,\dots,\sigma_r}(h, 1) = (\varsigma_s \otimes \varsigma_t)(j(x_{\sigma_1,\dots,\sigma_r}))(h, 1) \overset{(2\text{-}3)}{=} j(x_{\sigma_1,\dots,\sigma_r})(sh, t) = x_{\sigma_1,\dots,\sigma_r} = \mathrm{res}(x)_{\sigma_1,\dots,\sigma_r},$$

d'où $\mathrm{sh}'((\varsigma_s \otimes \varsigma_t)_* j_* x) = (\mathrm{res}(x), \dots, \mathrm{res}(x)) \in \mathrm{Z}^r(L_w, A \otimes A)^{|\mathfrak{g}_v|}$ pour tous $s, t \in \mathscr{E}_v$ en vertu du lemme 2.3. Ainsi, on a $\mathrm{sh}'_v(j_* x) = (\mathrm{sh}')^{e_v^2}((\varsigma \otimes \varsigma)_* j_* x) = (\mathrm{res}(x), \dots, \mathrm{res}(x))$ dans $\mathrm{Z}^r(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|}$, ou $\mathrm{sh}'_v(j_*[x]) = (\mathrm{res}([x]), \dots, \mathrm{res}([x]))$ dans $\mathrm{H}^r(L_w, A \otimes A)^{e_v^2|\mathfrak{g}_v|}$, ce qui achève la démonstration. □

2D. ***Description des localisations.*** On garde les notations du paragraphe précédent. Rappelons qu'on a des isomorphismes

$$\mathrm{sh} : \mathrm{H}^1(k, M) \to \mathrm{H}^1(L, A) \quad \text{et} \quad \mathrm{sh}_v = \mathrm{sh}^{e_v} \otimes \varsigma_* : \mathrm{H}^1(k_v, M) \to \mathrm{H}^1(L_w, A)^{e_v}.$$

Décrivons le morphisme $\mathrm{H}^1(L, A) \to \mathrm{H}^1(L_w, A)^{e_v}$ associé au morphisme de localisation

$$\mathrm{loc}_v : \mathrm{H}^1(k, M) \to \mathrm{H}^1(k_v, M).$$

Lemme 2.9. *On a un diagramme commutatif, où les flèches verticales sont des isomorphismes :*

$$\begin{tikzcd}
\mathrm{H}^1(L, A) \arrow[r, "a \mapsto ((^{s^{-1}}a)_w)_{s \in \mathscr{E}_v}"] & \mathrm{H}^1(L_w, A)^{e_v} \\
\mathrm{H}^1(k, M) \arrow[u, "\mathrm{sh}"'] \arrow[r, "\mathrm{loc}_v"] & \mathrm{H}^1(k_v, M) \arrow[u, "\mathrm{sh}_v"']
\end{tikzcd}$$

Démonstration. Soit $a \in \mathrm{H}^1(L, A)$, vu comme morphisme continu $\Gamma_L \to A$. Soit $x : \Gamma_k \to M$ le 1-cocycle représentant la classe $\mathrm{sh}^{-1}(a) \in \mathrm{H}^1(k, M)$ construit dans le lemme 2.1. Alors l'on a $x_\sigma(g) = {}^{u(g)^{-1}}a_\sigma$ pour tous $\sigma \in \Gamma_L$ et $g \in \mathfrak{g}$ (où $u(g) \in \Gamma_k$ désigne un relevé de g).

Étudions le localisé $x_v : \Gamma_{k_v} \to M$. Pour tous $s \in \mathscr{E}_v$ et $\sigma \in \Gamma_{L_w}$, on a

$$((\varsigma_s)_* x_v)_\sigma(1) = \varsigma_s((x_v)_\sigma)(1) = (x_v)_\sigma(s) = x_\sigma(s) = {}^{u(s)^{-1}}a_\sigma = (({}^{u(s)^{-1}}a)_w)_\sigma.$$

Ainsi, $\mathrm{sh}((\varsigma_s)_* x_v) = ({}^{u(s)^{-1}}a)_w$ dans $\mathrm{Z}^1(L_w, A)$, d'où $\mathrm{sh}_v(x_v) = ((\varsigma_s)_* x_v)_{s \in \mathscr{E}_v} = (({}^{u(s)^{-1}}a)_w)_{s \in \mathscr{E}_v}$ dans $\mathrm{Z}^1(L_w, A)^{e_v}$, ou $\mathrm{sh}_v([x_v]) = (({}^{s^{-1}}a)_w)_{s \in \mathscr{E}_v}$ dans $\mathrm{H}^1(L_w, A)^{e_v}$. □

Rappelons maintenant qu'on a des isomorphismes

$$\mathrm{sh}' : \mathrm{H}^2(k, M \otimes M) \to \mathrm{H}^2(L, A \otimes A)^{|\mathfrak{g}|} \quad \text{et} \quad \mathrm{sh}'_v = (\mathrm{sh}')^{e_v^2} \circ (\varsigma \otimes \varsigma)_* : \mathrm{H}^2(k_v, M \otimes M) \to \mathrm{H}^2(L_w, A \otimes A)^{e_v^2 |\mathfrak{g}_v|}.$$

Décrivons le morphisme $\mathrm{H}^2(L, A \otimes A)^{|\mathfrak{g}|} \to \mathrm{H}^2(L_w, A \otimes A)^{e_v^2 |\mathfrak{g}_v|}$ associé au morphisme de localisation

$$\mathrm{loc}_v : \mathrm{H}^2(k, M \otimes M) \to \mathrm{H}^2(k_v, M \otimes M).$$

Lemme 2.10. *On a un diagramme commutatif, où les flèches verticales sont des isomorphismes* :

$$\begin{tikzcd}
\mathrm{H}^2(L, A \otimes A)^{|\mathfrak{g}|} \arrow[r, "(\alpha_g)_{g \in \mathfrak{g}} \mapsto (({}^{t^{-1}}\alpha_{sht^{-1}})_w)_{h \in \mathfrak{g}_v, s, t \in \mathscr{E}_v}"] & \mathrm{H}^2(L_w, A \otimes A)^{e_v^2 |\mathfrak{g}_v|} \\
\mathrm{H}^2(k, M \otimes M) \arrow[u, "\mathrm{sh}'"'] \arrow[r, "\mathrm{loc}_v"] & \mathrm{H}^2(k_v, M \otimes M) \arrow[u, "\mathrm{sh}'_v"']
\end{tikzcd}$$

Démonstration. Soit $(a_g)_{g \in \mathfrak{g}}$ une famille de 2-cocycles $\Gamma_L \times \Gamma_L \to A \otimes A$. Pour tout $g \in \mathfrak{g}$, on note $x_g : \Gamma_k \times \Gamma_k \to \mathrm{Ind}_{\Gamma_k}^{\Gamma_L}(A \otimes A) = \{\mathfrak{g} \to A \otimes A\}$ le 2-cocycle construit dans le lemme 2.2 (appliqué au $A \otimes A$ au lieu de A), de sorte que $\mathrm{sh}(x_g) = a_g$ et que

$$(x_g)_{\sigma,\tau}(h) = {}^{u(h)^{-1}}(a_g)_{\sigma,\tau} \quad \forall \sigma, \tau \in \Gamma_L,\ \forall h \in \mathfrak{g}, \tag{2-5}$$

où $u(h) \in \Gamma_k$ désigne un relevé de h.

Reprenons les notations $\omega_g : M \otimes M \to \mathrm{Ind}_{\Gamma_k}^{\Gamma_L}(A \otimes A)$ et

$$\omega = (\omega_g)_{g \in \mathfrak{g}} : M \otimes M \to (\mathrm{Ind}_{\Gamma_k}^{\Gamma_L}(A \otimes A))^{|\mathfrak{g}|}$$

au début du paragraphe 2B. Par le lemme 2.3, il existe un 2-cocycle $y \in \mathrm{Z}^2(k, M \otimes M)$ tel que $x_g = (\omega_g)_* y$ pour tout $g \in \mathfrak{g}$. Alors $\mathrm{sh}'(y) = (\mathrm{sh}((\omega_g)_* y))_{g \in \mathfrak{g}} = (\mathrm{sh}(x_g))_{g \in \mathfrak{g}} = (a_g)_{g \in \mathfrak{g}} \in \mathrm{Z}^2(L, A \otimes A)^{|\mathfrak{g}|}$.

Étudions le localisé $y_v \in \mathrm{Z}^2(k_v, M \otimes M)$. Pour tous $s, t \in \mathscr{E}_v$, $h \in \mathfrak{g}_v$ et $\sigma, \tau \in \Gamma_{L_w}$, on a

$$\begin{aligned}
((\varsigma_s \otimes \varsigma_t)_* y_v)_{\sigma,\tau}(h, 1) = (\varsigma_s \otimes \varsigma_t)((y_v)_{\sigma,\tau})(h, 1) = (\varsigma_s \otimes \varsigma_t)(y_{\sigma,\tau})(h, 1) &\overset{\text{(2-3)}}{=} y_{\sigma,\tau}(sh, t) \\
= y_{\sigma,\tau}(sht^{-1}t, t) \overset{\text{(2-2)}}{=} \omega_{sht^{-1}}(y_{\sigma,\tau})(t) = ((\omega_{sht^{-1}})_* y)_{\sigma,\tau}(t)& \\
= (x_{sht^{-1}})_{\sigma,\tau}(t) \overset{\text{(2-5)}}{=} {}^{u(t)^{-1}}(a_{sht^{-1}})_{\sigma,\tau} = ({}^{u(t)^{-1}}(a_{sht^{-1}})_w)_{\sigma,\tau}&,
\end{aligned}$$

d'où $\mathrm{sh}'((\varsigma_s \otimes \varsigma_t)_* y_v) = ({}^{u(t)^{-1}}(a_{sht^{-1}})_w)_{h \in \mathfrak{g}_v}$ dans $\mathrm{Z}^2(L_w, A \otimes A)^{|\mathfrak{g}_v|}$ par le lemme 2.3. Ainsi

$$\mathrm{sh}'_v(y_v) = (\mathrm{sh}'((\varsigma_s \otimes \varsigma_t)_* y_v))_{s,t \in \mathscr{E}_v} = (({}^{u(t)^{-1}}(a_{sht^{-1}}))_w)_{h \in \mathfrak{g}_v, s, t \in \mathscr{E}_v}$$

dans $\mathrm{Z}^2(L_w, A\otimes A)^{e_v^2|\mathfrak{g}_v|}$, ou $\mathrm{sh}'_v([y_v]) = ((^{t^{-1}}[a_{sht^{-1}}])_w)_{h\in\mathfrak{g}_v, s,t\in\mathscr{E}_v}$ dans $\mathrm{H}^2(L_w, A\otimes A)^{e_v^2|\mathfrak{g}_v|}$. Cette égalité établit le résultat voulu. □

3. La construction de Borovoi–Kunyavskii

3A. $\mathbf{H}^2$ *non abélien et espaces homogènes.* Soit K un corps de caractéristique nulle. Pour étudier les K-espaces homogènes de SL_m (qui peut ne pas avoir de K-point), il convient d'introduire la notion de 2-cohomologie non abélienne. Nous allons utiliser sa version concrète en termes de cocycles [Flicker et al. 1998, §1].

Seuls les K-liens dont le $\overline{K}$-groupe sous-adjacent est fini (c'est donc simplement un groupe abstrait fini) seront pris en considération. Un *K-lien* (*fini*) $L = (F, \kappa)$ est alors la donnée d'un groupe fini F muni d'une action extérieure $\kappa : \Gamma_K \to \mathrm{Out}(F)$. Si F est un K-groupe — i.e., si une action (continue) $\rho : \Gamma_K \to \mathrm{Aut}(F)$ est donnée — on lui associe son K-lien canonique $\mathrm{lien}(F)$.

Soit $L = (F, \kappa)$ un K-lien. Un *2-cocycle à coefficients dans* L est un couple (ρ, u) où $\rho : \Gamma_K \to \mathrm{Aut}(F)$ et $u : \Gamma_K \times \Gamma_K \to F$ sont des applications continues telles que :

1. ρ_σ relève κ_σ pour tout $\sigma \in \Gamma_K$.
2. $\rho_{\sigma\tau} = \mathrm{int}(u_{\sigma,\tau}) \circ \rho_\sigma \circ \rho_\tau$ pour tous $\sigma, \tau \in \Gamma_K$.
3. $u_{\sigma,\tau\upsilon}\rho_\sigma(u_{\tau,\upsilon}) = u_{\sigma\tau,\upsilon}u_{\sigma,\tau}$ pour tous $\sigma, \tau, \upsilon \in \Gamma_K$.

Notons $\mathrm{Z}^2(K, L)$ l'ensemble des 2-cocycles à coefficients dans L. Deux tels 2-cocycles (ρ, u) et (ρ', u') sont dits *cohomologues* s'il existe une application continue $c : \Gamma_K \to F$ telle que :

1. $\rho'_\sigma = \mathrm{int}(c_\sigma) \circ \rho_\sigma$ pour tout $\sigma \in \Gamma_K$.
2. $u'_{\sigma,\tau} = c_{\sigma\tau}u_{\sigma,\tau}\rho_\sigma(c_\tau)^{-1}c_\sigma^{-1}$ pour tous $\sigma, \tau \in \Gamma_K$.

Alors « être cohomologues » est une relation d'équivalence sur $\mathrm{Z}^2(K, L)$. On appelle *ensemble de 2-cohomologie galoisienne à coefficients dans* L le quotient $\mathrm{Z}^2(K, L)$ par cette relation, et on le note $\mathrm{H}^2(K, L)$. Si F est un K-groupe, on note $\mathrm{H}^2(K, F) := \mathrm{H}^2(K, \mathrm{lien}(F))$. Dans le cas où F est un Γ_K-module, $\mathrm{H}^2(K, F)$ est le groupe de 2-cohomologie galoisienne usuel.

Soit $L = (F, \kappa)$ un K-lien. Une classe $\eta \in \mathrm{H}^2(K, L)$ est dite *neutre* si elle est représentée par un 2-cocycle de la forme $(\rho, 1)$. Dans ce cas, $\rho : \Gamma_K \to \mathrm{Aut}(F)$ est une action continue de Γ_K sur F relevant κ et donc η correspond à une K-forme F' ; on note $\eta = n(F')$. L'ensemble $\mathrm{H}^2(K, L)$ peut ne pas avoir de classe neutre, et elle peut également en posséder plusieurs. Si F est un K-groupe et $\rho : \Gamma_K \to F$ désigne l'action de Γ_K, l'ensemble $\mathrm{H}^2(K, F)$ a une classe neutre privilégiée $\eta_0 = [(\rho, 1)] = n(F)$. Si F est un Γ_K-module, la seule classe neutre du groupe $\mathrm{H}^2(K, F)$ est 0.

Soit $L = (F, \kappa)$ un K-lien et soit $Z = Z(F)$. Comme Z est commutatif et caractéristique dans F, l'action extérieure de Γ_K sur F induit une action sur Z, i.e., Z est naturellement un Γ_K-module. Dans le cas où l'ensemble $\mathrm{H}^2(K, L)$ est non vide, c'est un espace principal homogène du groupe abélien $\mathrm{H}^2(K, Z)$, l'action étant définie par

$$[\beta] \cdot [(\rho, u)] := [(\rho, \beta u)],$$

où β (resp. (ρ, u)) est un 2-cocycle à coefficients dans Z (resp. dans L) [Borovoi 1993, Lemma 1.9].

Soit X un K-espace homogène d'un K-groupe algébrique G à stabilisateur géométrique fini F. Alors F n'est pas a priori muni d'une action, mais seulement d'une action extérieure de Γ_K. On peut donc définir le *lien de Springer* L_X de X. Plus concrètement, soit $x \in X(\overline{K})$ un point géométrique et soit $F \subseteq G(\overline{K})$ son stabilisateur. Pour tout $\sigma \in \Gamma_K$, écrivons ${}^\sigma x = x \cdot g_\sigma$, où $g_\sigma \in \mathrm{SL}_m(\overline{K})$ est unique modulo multiplication à gauche par un élément de F. On peut choisir les g_σ de sorte que l'application $\sigma \mapsto g_\sigma$ est continue. On définit

$$\rho_\sigma : F \to F, \quad \rho_\sigma(f) = g_\sigma {}^\sigma f g_\sigma^{-1}.$$

Alors $\rho : \Gamma_K \to \mathrm{Aut}(F)$ est continue et la composée $\kappa : \Gamma_K \xrightarrow{\rho} \mathrm{Aut}(F) \to \mathrm{Out}(F)$ est une action extérieure. On vérifie que le K-lien $L_X = (F, \kappa)$ ne dépend pas du choix de x et des g_σ ; c'est le lien de Springer de X. De plus, si l'on note $u_{\sigma,\tau} := g_{\sigma\tau} {}^\sigma g_\tau^{-1} g_\sigma^{-1}$ pour tous $\sigma, \tau \in \Gamma_K$, alors (ρ, u) est un 2-cocycle à coefficients dans L_X. On définit la *classe de Springer* de X comme étant $\eta_X := [(\rho, u)] \in \mathrm{H}^2(K, L_X)$. Elle est neutre si et seulement si X est dominé par un K-torseur sous G [Borovoi 1993, §7.6]. En particulier, si $\mathrm{H}^1(K, G) = 1$ (par exemple, c'est le cas pour $G = \mathrm{GL}_m$ ou $G = \mathrm{SL}_m$ par une variante du théorème 90 de Hilbert), alors η_X est neutre si et seulement si $X(K) \neq \varnothing$.

Lemme 3.1. *Soit L un K-lien et soit $\eta \in \mathrm{H}^2(K, L)$. Alors il existe un entier m et un espace homogène X de* SL_m *de lien de Springer L et de classe de Springer η. Deux tels espaces homogènes sont K-stablement birationnels.*

Démonstration. On pourra consulter [Demarche et Lucchini Arteche 2019, corollaires 3.3 et 3.5]. □

Remarque 3.2. Soit F un K-groupe fini et $Z = Z(F)$. À partir de chaque classe $\eta \in \mathrm{H}^2(K, Z)$, Borovoi et Kunyavskii [1997, §2] ont construit explicitement un espace homogène X de SL_m de lien de Springer $\mathrm{lien}(F)$. Notant $\eta_0 = n(F) \in \mathrm{H}^2(K, F)$ la classe neutre privilégiée, alors la classe de Springer de X est $\eta \cdot \eta_0$ [Harari et Skorobogatov 2002, Lemma 5.3]. Puisque $\mathrm{H}^2(K, Z)$ agit transitivement sur $\mathrm{H}^2(K, F)$, cette construction-là donne tous les espaces homogènes de SL_m de lien de Springer $\mathrm{lien}(F)$, à équivalence birationnelle stable près.

Proposition 3.3. *Soient F un K-groupe fini, $Z = Z(F)$ et $\eta_0 \in \mathrm{H}^2(K, F)$ la classe neutre privilégiée. On note $\Delta : \mathrm{H}^1(K, F/Z) \to \mathrm{H}^2(K, Z)$ l'application connectante induite par l'extension centrale*

$$1 \to Z \to F \to F/Z \to 1$$

(*cf.* [Serre 1962, chapitre VII, annexe, proposition 2]). *Soit $\beta \in \mathrm{H}^2(K, Z)$ et soit X un espace homogène de* SL_m *de lien de Springer* $\mathrm{lien}(F)$ *et de classe de Springer $\eta_X = \beta \cdot \eta_0 \in \mathrm{H}^2(K, F)$. Alors $X(K) \neq \varnothing$ si et seulement s'il existe $\alpha \in \mathrm{H}^1(K, F/Z)$ tel que $\beta = \Delta(\alpha)$. Dans ce cas, X est K-isomorphe à ${}_{\mathfrak{a}}F \backslash \mathrm{SL}_m$, où $\mathfrak{a} : \Gamma_K \to F/Z$ est n'importe quel* 1*-cocycle représentant α. Ici, ${}_{\mathfrak{a}}F$ désigne la K-forme de F tordue par $\mathfrak{a}$, c'est-à-dire que son action de Galois $\cdot_{\mathfrak{a}} : \Gamma_k \times {}_{\mathfrak{a}}F \to {}_{\mathfrak{a}}F$ est donnée par*

$$\sigma \cdot_{\mathfrak{a}} f = \tilde{\mathfrak{a}}_\sigma {}^\sigma f \tilde{\mathfrak{a}}_\sigma^{-1} \quad \forall \sigma \in \Gamma_k,\ \forall f \in F,$$

où $\tilde{\mathfrak{a}}_\sigma \in F$ *est un relevé quelconque de* $\mathfrak{a}_\sigma$.

Démonstration. Par [Borovoi 1993, Lemma 2.4 et Lemma 2.5], η_X est neutre si et seulement s'il existe un 1-cocycle $\mathfrak{a} : \Gamma_K \to F/Z$ tel que $\eta_X = n({}_{\mathfrak{a}}F) = \Delta([\mathfrak{a}]) \cdot \eta_0$. Cette égalité équivaut à $\Delta([\mathfrak{a}]) = \beta$ puisque l'action de $\mathrm{H}^2(K, Z)$ sur $\mathrm{H}^2(K, F)$ est libre. Dans ce cas, X est k-stablement birationnel à ${}_{\mathfrak{a}}F\backslash \mathrm{SL}_{m'}$, donc X possède un K-point dont le stabilisateur est K-isomorphe à ${}_{\mathfrak{a}}F$, i.e., $X \simeq {}_{\mathfrak{a}}F\backslash \mathrm{SL}_m$. □

Remarque 3.4. Lorsque $K = k$ est un corps de nombres, F est un k-groupe fini et $Z = Z(F) = [F, F]$, Harari et Skorobogatov ont utilisé une « théorie de la descente non abélienne » pour démontrer le fait suivant : si X est un k-espace homogène de SL_m de lien de Springer lien(F) et de classe de Springer $\eta \cdot \eta_0$, où $\eta \in Ш^2(k, Z)$, alors X possède un point adélique orthogonal à $\mathrm{Br}_1 X := \mathrm{Ker}(\mathrm{Br}\, X \to \mathrm{Br}\, \overline{X})$ [Harari et Skorobogatov 2002, Proposition 5.5]. Ils ont soulevé la question si l'on peut en déduire l'existence de contre-exemples au principe de Hasse non expliqués par l'obstruction de Brauer–Manin algébrique (cf. loc. cit., Remark 5.6). Dans ce texte, nous y donnons une réponse partielle : c'est impossible pour les données de k et de F comme dans l'énoncé du théorème A.

3B. ***Construction du stabilisateur.*** Soit K un corps de caractéristique nulle. Soient M et Z des Γ_K-modules finis et $\phi : M \otimes M \to Z$ un morphisme Γ_K-équivariant. On dira que ϕ est *non dégénéré* s'il possède les propriétés suivantes :

1. Si $x \in M$ est tel que $\phi(x \otimes y) = 0$ pour tout $y \in M$, alors $x = 0$.
2. Si $y \in M$ est tel que $\phi(x \otimes y) = 0$ pour tout $x \in M$, alors $y = 0$.

On munit Z de l'action triviale de $M \oplus M$. Posons

$$\Phi : (M \oplus M) \times (M \oplus M) \to Z, \quad \Phi((x, y), (x', y')) = \phi(x \otimes y'). \tag{3-1}$$

Alors Φ est biadditive, donc c'est un 2-cocycle *normalisé* ($\Phi(a, 0) = \Phi(0, a) = 0$ pour tout $a \in M \oplus M$). Soit F le produit croisé $Z \times_\Phi (M \oplus M)$, c'est-à-dire que $F = Z \times (M \oplus M)$ comme ensemble et la loi de composition sur F est donnée par la formule

$$(z, a)(z', a') = (z + z' + \Phi(a, a'), a + a') \quad \forall z, z' \in Z,\ \forall a, a' \in M \oplus M. \tag{3-2}$$

En particulier, $(z, a) = (z, 0)(0, a) = (0, a)(z, 0)$. De plus, comme

$$(0, a)(0, -a) = (\Phi(a, -a), 0) = (-\Phi(a, a), 0) = (\Phi(a, a), 0)^{-1},$$

on a $(0, a)^{-1} = (\Phi(a, a), 0)(0, -a) = (\Phi(a, a), -a)$ et donc

$$(z, a)^{-1} = (z, 0)^{-1}(0, a)^{-1} = (-z, 0)(\Phi(a, a), -a) = (\Phi(a, a) - z, -a). \tag{3-3}$$

On obtient une extension *centrale* de groupes *abstraits* :

$$0 \to Z \to F \to M \oplus M \to 0. \tag{3-4}$$

Lemme 3.5. *Soient* M, Z, ϕ, Φ, F *comme ci-dessus. Soient* $z, z' \in Z$ *et* $a, a' \in M \oplus M$.

1. *On a* $(z, a)(z', a')(z, a)^{-1} = (z' + \Phi(a, a') - \Phi(a', a), a')$.
2. *Le commutateur* $[(z, a), (z', a')] = (\Phi(a, a') - \Phi(a', a), 0)$.
3. *Si* ϕ *est surjectif*, $Z = [F, F]$.

Démonstration. 1. On a

$$\begin{aligned}(z, a)(z', a')(z, a)^{-1} &= (z, 0)(0, a)(z', a')(0, a)^{-1}(z, 0)^{-1} \\ &= (0, a)(z', a')(0, a)^{-1} && (Z \text{ central dans } F) \\ &= (z' + \Phi(a, a'), a + a')(\Phi(a, a), -a) && (\text{par (3-2) et (3-3)}) \\ &= (z' + \Phi(a, a') + \Phi(a, a) + \Phi(a + a', -a), a + a' - a) && (\text{par (3-2)}) \\ &= (z' + \Phi(a, a') - \Phi(a', a), a').\end{aligned}$$

2. On a

$$\begin{aligned}[(z, a), (z', a')] &= [(z, 0)(0, a), (z', 0)(0, a')] \\ &= [(0, a), (0, a')] && (Z \text{ central dans } F) \\ &= (0, a)(0, a')(0, a)^{-1}(0, a')^{-1} \\ &= (\Phi(a, a') - \Phi(a', a), a')(\Phi(a', a'), -a') && (\text{par 1. et (3-3)}) \\ &= (\Phi(a, a') - \Phi(a', a) + \Phi(a', a') + \Phi(a', -a'), a' - a') && (\text{par (3-2)}) \\ &= (\Phi(a, a') - \Phi(a', a), 0).\end{aligned}$$

3. Comme $F/Z = M \oplus M$ est commutatif, on a toujours que $[F, F] \subseteq Z$. De plus,

$$\phi(x \otimes y) = \phi(x \otimes y) - \phi(0, 0) = \Phi((x, 0), (0, y)) - \Phi((0, y), (x, 0))$$

pour tous $x, y \in M$, d'où

$$(\phi(x \otimes y), 0) = (\Phi((x, 0), (0, y)) - \Phi((0, y), (x, 0)), 0) = [(0, (x, 0)), (0, (0, y))] \in [F, F]$$

par le deuxième point. Ainsi, on aura $Z = Z \times \{0\} \subseteq [F, F]$ dès que ϕ est surjectif. □

Lemme 3.6. *Soient* M, Z, ϕ, Φ, F *comme ci-dessus. Si* ϕ *est non dégénéré*, $Z = Z(F)$.

Démonstration. Comme Z est centrale dans F, il reste à montrer que $Z(F) \subseteq Z$. Supposons $(z, a) \in Z(F)$, où $z \in Z$ et $a = (x, y) \in M \oplus M$. En vertu du lemme 3.5, on a

$$(0, 0) = [(z, a), (0, a')] = (\Phi(a, a') - \Phi(a', a), 0) = (\phi(x \otimes y') - \phi(x' \otimes y), 0)$$

pour tout $a' = (x', y') \in M \oplus M$. En choisissant $x' = 0$, on obtient

$$\phi(x \otimes y') = 0 \quad \forall y' \in M,$$

d'où $x = 0$ puisque ϕ est non dégénéré. De même, $y = 0$, d'où $a = 0$ et donc $(z, a) = (z, 0) \in Z$. □

Finalement, on munit F d'une action de Γ_K qui est compatible avec celles sur Z et sur $M \oplus M$; alors (3-4) devient une extension centrale de K-groupes finis. Dans ce texte, on se concentre principalement sur l'action *coordonnée par coordonnée*, c'est-à-dire

$$^{\sigma}(z, a) = ({}^{\sigma}z, {}^{\sigma}a)$$

pour tous $\sigma \in \Gamma_K$, $z \in Z$ et $a \in A$. De (3-2), on voit que cette action est bien compatible avec la loi de composition sur F puisque Φ est Γ_K-équivariant.

Définition 3.7. On appelle *espace homogène de Borovoi–Kunyavskii* tout espace homogène de SL_m dont les stabilisateurs géométriques F sont de la forme du groupe du milieu de (3-4), avec $Z = Z(F) = [F, F]$.

Rappelons que la condition $Z = Z(F) = [F, F]$ se garantit lorsque ϕ est surjectif et non dégénéré (lemmes 3.5 et 3.6).

3C. ***Quelques calculs avec des cocycles.*** Soit K un corps de caractéristique nulle. Soient M et Z des Γ_K-modules finis et $\phi : M \otimes M \to Z$ un morphisme Γ_K-équivariant. On définit l'application biadditive $\Phi : (M \oplus M) \times (M \oplus M) \to Z$ par (3-1) et l'on pose $F = Z \times_{\Phi} (M \oplus M)$, muni de l'action coordonnée par coordonnée de Γ_K.

Si $x, y : \Gamma_K \to M$ sont des 1-cochaînes, on notera $x \otimes y : \Gamma_K \to M \otimes M$ la 1-cochaîne $\sigma \mapsto x_\sigma \otimes y_\sigma$. On considérera le cup-produit des cochaînes à coefficients dans M induit par l'accouplement $\otimes : M \times M \to M \otimes M$. Pour la preuve du théorème 5.6 (c'est-à-dire du théorème A), au vu de la proposition 3.3, il conviendra de décrire l'application connectante $\Delta : \mathrm{H}^1(K, M \oplus M) \to \mathrm{H}^2(K, Z)$ induite par (3-4).

Lemme 3.8. *Avec les notations ci-dessus, on a les résultats suivants.*

1. *Soit* $\mathfrak{a} = (\mathfrak{x}, \mathfrak{y}) : \Gamma_K \to M \oplus M$ *un* 1*-cocycle* (*i.e.*, $\mathfrak{x}$ *et* $\mathfrak{y}$ *sont des* 1*-cocycles*), *et soit* ${}_{\mathfrak{a}}F$ *la* K*-forme de* F *tordue par* $\mathfrak{a}$ (*cf. proposition 3.3*). *Soient* $z : \Gamma_K \to Z$, $a = (x, y) : \Gamma_K \to M \oplus M$ *des* 1*-cochaînes, et* $f = (z, a) : \Gamma_K \to {}_{\mathfrak{a}}F$. *Alors* f *est un cocycle si et seulement si* :
   — *a est un cocycle* (*i.e.*, *x et y sont des cocycles*).
   — $\mathrm{d}z + \phi_*(\mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y})) = 0$.
2. *Notons* $\Delta : \mathrm{H}^1(K, M \oplus M) \to \mathrm{H}^2(K, Z)$ *l'application connectante induite par* (3-4) (*cf.* [Serre 1962, chapitre VII, annexe, proposition 2]). *Alors* $\Delta([a]) = \phi_*[x \cup y]$ *pour tout* 1*-cocycle* $a = (x, y) : \Gamma_K \to M \oplus M$.

Démonstration. On note toujours $\cdot_{\mathfrak{a}}$ l'action de Γ_K sur F tordue par $\mathfrak{a}$. Alors

$$\sigma \cdot_{\mathfrak{a}} (\zeta, \alpha) = (0, \mathfrak{a}_\sigma)^{\sigma}(\zeta, \alpha)(0, \mathfrak{a}_\sigma)^{-1} = (0, \mathfrak{a}_\sigma)({}^{\sigma}\zeta, {}^{\sigma}\alpha)(0, \mathfrak{a}_\sigma)^{-1} = ({}^{\sigma}\zeta + \Phi(\mathfrak{a}_\sigma, {}^{\sigma}\alpha) - \Phi({}^{\sigma}\alpha, \mathfrak{a}_\sigma), {}^{\sigma}\alpha) \tag{3-5}$$

pour tous $(\zeta, \alpha) \in F$ et $\sigma \in \Gamma_K$, en vertu du lemme 3.5.

1. Le morphisme ${}_{\mathfrak{a}}F \to M \oplus M$ étant la deuxième projection, on voit que a est forcément un 1-cocycle dès que f l'est. Soient $\sigma, \tau \in \Gamma_K$. Sous la condition que a est un cocycle, on a

$$\begin{aligned}
&(0, a_\sigma)(\sigma \cdot_{\mathfrak{a}} (z_\tau, a_\tau))(0, a_{\sigma\tau})^{-1} \\
&\quad = (0, a_\sigma)(\sigma \cdot_{\mathfrak{a}} (z_\tau, a_\tau))(\Phi(a_{\sigma\tau}, a_{\sigma\tau}), -a_{\sigma\tau}) && \text{(par (3-3))} \\
&\quad = (0, a_\sigma)({}^\sigma z_\tau + \Phi(\mathfrak{a}_\sigma, {}^\sigma a_\tau) - \Phi({}^\sigma a_\tau, \mathfrak{a}_\sigma), {}^\sigma a_\tau)(\Phi(a_{\sigma\tau}, a_{\sigma\tau}), -a_{\sigma\tau}) && \text{(par (3-5))} \\
&\quad = ({}^\sigma z_\tau + \Phi(\mathfrak{a}_\sigma, {}^\sigma a_\tau) - \Phi({}^\sigma a_\tau, \mathfrak{a}_\sigma) + \Phi(a_\sigma, {}^\sigma a_\tau), a_\sigma + {}^\sigma a_\tau)(\Phi(a_{\sigma\tau}, a_{\sigma\tau}), -a_{\sigma\tau}) && \text{(par (3-2))} \\
&\quad = ({}^\sigma z_\tau + \Phi(\mathfrak{a}_\sigma, {}^\sigma a_\tau) - \Phi({}^\sigma a_\tau, \mathfrak{a}_\sigma) + \Phi(a_\sigma, {}^\sigma a_\tau), a_{\sigma\tau})(\Phi(a_{\sigma\tau}, a_{\sigma\tau}), -a_{\sigma\tau}) \\
&\quad = ({}^\sigma z_\tau + \Phi(\mathfrak{a}_\sigma, {}^\sigma a_\tau) - \Phi({}^\sigma a_\tau, \mathfrak{a}_\sigma) + \Phi(a_\sigma, {}^\sigma a_\tau) + \Phi(a_{\sigma\tau}, a_{\sigma\tau}) - \Phi(a_{\sigma\tau}, a_{\sigma\tau}), 0) && \text{(par (3-2))} \\
&\quad = ({}^\sigma z_\tau + \Phi(\mathfrak{a}_\sigma, {}^\sigma a_\tau) - \Phi({}^\sigma a_\tau, \mathfrak{a}_\sigma) + \Phi(a_\sigma, {}^\sigma a_\tau), 0),
\end{aligned}$$

d'où

$$\begin{aligned}
f_\sigma(\sigma \cdot_{\mathfrak{a}} f_\tau) f_{\sigma\tau}^{-1} &= (z_\sigma, a_\sigma)(\sigma \cdot_{\mathfrak{a}} (z_\tau, a_\tau))(z_{\sigma\tau}, a_{\sigma\tau})^{-1} \\
&= (z_\sigma, 0)(0, a_\sigma)(\sigma \cdot_{\mathfrak{a}} (z_\tau, a_\tau))(0, a_{\sigma\tau})^{-1}(z_{\sigma\tau}, 0)^{-1} \\
&= (z_\sigma, 0)({}^\sigma z_\tau + \Phi(\mathfrak{a}_\sigma, {}^\sigma a_\tau) - \Phi({}^\sigma a_\tau, \mathfrak{a}_\sigma) + \Phi(a_\sigma, {}^\sigma a_\tau), 0)(-z_{\sigma\tau}, 0) \\
&= (z_\sigma + {}^\sigma z_\tau - z_{\sigma\tau} + \Phi(\mathfrak{a}_\sigma, {}^\sigma a_\tau) - \Phi({}^\sigma a_\tau, \mathfrak{a}_\sigma) + \Phi(a_\sigma, {}^\sigma a_\tau), 0) \\
&= (z_\sigma + {}^\sigma z_\tau - z_{\sigma\tau} + \phi(\mathfrak{x}_\sigma \otimes {}^\sigma y_\tau - {}^\sigma x_\tau \otimes \mathfrak{y}_\sigma + x_\sigma \otimes {}^\sigma y_\tau), 0) \\
&= ((\mathrm{d}z)_{\sigma,\tau} + \phi(\mathfrak{x} \cup y)_{\sigma,\tau} - {}^\sigma x_\tau \otimes \mathfrak{y}_\sigma + (x \cup y)_{\sigma,\tau}, 0).
\end{aligned}$$

Notons de plus que

$$x_{\sigma\tau} \otimes \mathfrak{y}_{\sigma\tau} = (x_\sigma + {}^\sigma x_\tau) \otimes (\mathfrak{y}_\sigma + {}^\sigma \mathfrak{y}_\tau) = x_\sigma \otimes \mathfrak{y}_\sigma + {}^\sigma x_\tau \otimes \mathfrak{y}_\sigma + x_\sigma \otimes {}^\sigma \mathfrak{y}_\tau + {}^\sigma x_\tau \otimes {}^\sigma \mathfrak{y}_\tau,$$

d'où $-{}^\sigma x_\tau \otimes \mathfrak{y}_\sigma = x_\sigma \otimes {}^\sigma \mathfrak{y}_\tau + (x_\sigma \otimes \mathfrak{y}_\sigma + {}^\sigma(x_\tau \otimes \mathfrak{y}_\tau) - x_{\sigma\tau} \otimes \mathfrak{y}_{\sigma\tau}) = (x \cup \mathfrak{y})_{\sigma,\tau} + \mathrm{d}(x \otimes \mathfrak{y})_{\sigma,\tau}$ et donc on a

$$f_\sigma(\sigma \cdot_{\mathfrak{a}} f_\tau) f_{\sigma\tau}^{-1} = ((\mathrm{d}z)_{\sigma,\tau} + \phi((\mathfrak{x} \cup y)_{\sigma,\tau} + (x \cup \mathfrak{y})_{\sigma,\tau} + \mathrm{d}(x \otimes \mathfrak{y})_{\sigma,\tau} + (x \cup y)_{\sigma,\tau}), 0) \tag{3-6}$$

De (3-6), on voit que f est un cocycle si et seulement si a l'est et

$$\mathrm{d}z + \phi_*(\mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y})) = 0,$$

d'où le premier point du lemme.

2. Soit $a = (x, y) : \Gamma_K \to M \oplus M$ un 1-cocycle. On considère la 1-cochaîne $f = (0, a) : \Gamma_K \to F$ relevant a. Alors

$$f_\sigma {}^\sigma f_\tau f_{\sigma\tau}^{-1} = (\phi((x \cup y)_{\sigma,\tau}), 0)$$

pour tous $\sigma, \tau \in \Gamma_K$, au vu de (3-6). Par définition de Δ, on a bien $\Delta([a]) = \phi_*[x \cup y]$. □

Le lemme suivant sera utilisé dans la preuve du théorème 5.8 (c'est-à-dire du théorème B).

Lemme 3.9. *Gardons les notations au début du paragraphe, et soit* $\mathfrak{a} = (\mathfrak{x}, \mathfrak{y}) : \Gamma_K \to M \oplus M$ *un* 1*-cocycle. Soient* $f = (z, a)$ *et* $f' = (z', a')$ *des* 1*-cocycles* $\Gamma_K \to {}_{\mathfrak{a}}F$ *(cf. proposition 3.3), où* $a = (x, y)$ *et* $a' = (x', y')$ *(voir lemme 3.8). On suppose que* $\alpha = (\xi, \eta) \in M \oplus M$ *est un élément satisfaisant* $a' = a + \mathrm{d}\alpha$ *et l'on considère la* 1*-cochaîne*

$$c := z' - z + \phi_*(-(x + \mathfrak{x}) \cup \eta + \xi \cup (y' + \mathfrak{y}) + \mathrm{d}\xi \otimes \mathfrak{y}) : \Gamma_K \to Z.$$

1. c est un cocycle.

2. Si c est un cobord, f et f′ sont cohomologues.

3. Supposons ϕ *surjectif. Écrivons* $z = \phi_*\varepsilon$ *et* $z' = \phi_*\varepsilon'$*, où* $\varepsilon, \varepsilon' : \Gamma_K \to M \otimes M$ *sont des* 1*-cochaînes. Alors on peut écrire*

$$\mathrm{d}\varepsilon + \mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y}) = j_*\lambda \quad \textit{et} \quad \mathrm{d}\varepsilon' + \mathfrak{x} \cup y' + x' \cup \mathfrak{y} + x' \cup y' + \mathrm{d}(x' \otimes \mathfrak{y}) = j_*\lambda',$$

où $j : \operatorname{Ker}\phi \hookrightarrow M \otimes M$ *est l'inclusion et où* $\lambda, \lambda' : \Gamma_K \times \Gamma_K \to \operatorname{Ker}\phi$ *sont des* 2*-cocycles. De plus, si* $\delta : \mathrm{H}^1(K, Z) \to \mathrm{H}^2(K, \operatorname{Ker}\phi)$ *désigne le morphisme connectant induit par la suite exacte*

$$0 \to \operatorname{Ker}\phi \xrightarrow{j} M \otimes M \xrightarrow{\phi} Z \to 0,$$

alors $\delta([c]) = [\lambda' - \lambda]$.

Démonstration. 1. Par l'hypothèse, $x' = x + \mathrm{d}\xi$ et $y' = y + \mathrm{d}\eta$. Comme f et f' sont des cocycles, on a

$$\mathrm{d}z = -\phi_*(\mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y}))$$

et

$$\begin{aligned}\mathrm{d}z' &= -\phi_*(\mathfrak{x} \cup y' + x' \cup \mathfrak{y} + x' \cup y' + \mathrm{d}(x' \otimes \mathfrak{y}))\\ &= -\phi_*(\mathfrak{x} \cup (y + \mathrm{d}\eta) + (x + \mathrm{d}\xi) \cup \mathfrak{y} + (x + \mathrm{d}\xi) \cup (y + \mathrm{d}\eta) + \mathrm{d}((x + \mathrm{d}\xi) \otimes \mathfrak{y}))\end{aligned}$$

par le lemme 3.8. D'où

$$\begin{aligned}\mathrm{d}z' - \mathrm{d}z &= -\phi_*(\mathfrak{x} \cup \mathrm{d}\eta + \mathrm{d}\xi \cup \mathfrak{y} + x \cup \mathrm{d}\eta + \mathrm{d}\xi \cup y + \mathrm{d}\xi \cup \mathrm{d}\eta + \mathrm{d}(\mathrm{d}\xi \otimes \mathfrak{y}))\\ &= -\phi_*((x + \mathfrak{x}) \cup \mathrm{d}\eta + \mathrm{d}\xi \cup (y + \mathfrak{y} + \mathrm{d}\eta) + \mathrm{d}(\mathrm{d}\xi \otimes \mathfrak{y}))\\ &= -\phi_*((x + \mathfrak{x}) \cup \mathrm{d}\eta + \mathrm{d}\xi \cup (y' + \mathfrak{y}) + \mathrm{d}(\mathrm{d}\xi \otimes \mathfrak{y})).\end{aligned}$$

Notant que x, $\mathfrak{x}$, y' et $\mathfrak{y}$ sont des cocycles, on en déduit que

$$\begin{aligned}\mathrm{d}c &= \mathrm{d}(z' - z + \phi_*(-(x + \mathfrak{x}) \cup \eta + \xi \cup (y' + \mathfrak{y}) + \mathrm{d}\xi \otimes \mathfrak{y}))\\ &= \mathrm{d}z' - \mathrm{d}z + \phi_*((x + \mathfrak{x}) \cup \mathrm{d}\eta + \mathrm{d}\xi \cup (y' + \mathfrak{y}) + \mathrm{d}(\mathrm{d}\xi \otimes \eta))\\ &= 0,\end{aligned}$$

donc c est bien un cocycle.

2. Écrivons $c = \mathrm{d}\zeta$ avec $\zeta \in Z$. Pour tout $\sigma \in \Gamma_K$, on a

$$a'_\sigma + \alpha = a_\sigma + {}^\sigma\alpha \tag{3-7}$$

puisque $a' = a + \mathrm{d}\alpha$ et

$$c + z + \phi_*((x + \mathfrak{x}) \cup \eta - \xi \cup (y' + \mathfrak{y}) - \mathrm{d}\xi \otimes \mathfrak{y}) = z' \tag{3-8}$$

par définition de c. Calculons

$$\begin{aligned}
&(\zeta, \alpha)^{-1} f_\sigma(\sigma \cdot_{\mathfrak{a}} (\zeta, \alpha)) \\
&\quad = (\Phi(\alpha, \alpha) - \zeta, -\alpha)(z_\sigma, a_\sigma)(\sigma \cdot_{\mathfrak{a}} (\zeta, \alpha)) && \text{(par (3-3))} \\
&\quad = (\Phi(\alpha, \alpha) - \zeta, -\alpha)(z_\sigma, a_\sigma)({}^\sigma\zeta + \Phi(\mathfrak{a}_\sigma, {}^\sigma\alpha) - \Phi({}^\sigma\alpha, \mathfrak{a}_\sigma), {}^\sigma\alpha) && \text{(par (3-5))} \\
&\quad = (\Phi(\alpha, \alpha) - \zeta, -\alpha)(z_\sigma + {}^\sigma\zeta + \Phi(\mathfrak{a}_\sigma, {}^\sigma\alpha) - \Phi({}^\sigma\alpha, \mathfrak{a}_\sigma) + \Phi(a_\sigma, {}^\sigma\alpha), a_\sigma + {}^\sigma\alpha) && \text{(par (3-2))} \\
&\quad = (\Phi(\alpha, \alpha) - \zeta, -\alpha)(z_\sigma + {}^\sigma\zeta + \Phi(a_\sigma + \mathfrak{a}_\sigma, {}^\sigma\alpha) - \Phi({}^\sigma\alpha, \mathfrak{a}_\sigma), a'_\sigma + \alpha) && \text{(par (3-7))} \\
&\quad = (\Phi(\alpha, \alpha) - \zeta + z_\sigma + {}^\sigma\zeta + \Phi(a_\sigma + \mathfrak{a}_\sigma, {}^\sigma\alpha) - \Phi({}^\sigma\alpha, \mathfrak{a}_\sigma) - \Phi(\alpha, a'_\sigma + \alpha), a'_\sigma) && \text{(par (3-2))} \\
&\quad = ({}^\sigma\zeta - \zeta + z_\sigma + \Phi(a_\sigma + \mathfrak{a}_\sigma, {}^\sigma\alpha) - \Phi({}^\sigma\alpha, \mathfrak{a}_\sigma) - \Phi(\alpha, a'_\sigma), a'_\sigma) \\
&\quad = (c_\sigma + z_\sigma + \phi((x_\sigma + \mathfrak{x}_\sigma) \otimes {}^\sigma\eta - {}^\sigma\xi \otimes \mathfrak{y}_\sigma - \xi \otimes y'_\sigma), a'_\sigma) && \text{(car } c = \mathrm{d}\zeta) \\
&\quad = (c_\sigma + z_\sigma + \phi((x_\sigma + \mathfrak{x}_\sigma) \otimes {}^\sigma\eta - \xi \otimes (y'_\sigma + \mathfrak{y}_\sigma) - ({}^\sigma\xi - \xi) \otimes \mathfrak{y}_\sigma), a'_\sigma) \\
&\quad = (z'_\sigma, a'_\sigma) && \text{(par (3-8))} \\
&\quad = f'_\sigma.
\end{aligned}$$

Cette égalité signifie que f et f' sont cohomologues.

3. Comme f est un cocycle, on a

$$\phi_*(\mathrm{d}\varepsilon + \mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y})) = \mathrm{d}z + \phi_*(\mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y})) = 0$$

par le lemme 3.8. Donc on peut écrire

$$\mathrm{d}\varepsilon + \mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y}) = j_*\lambda \tag{3-9}$$

pour une 2-cochaîne $\lambda : \Gamma_K \times \Gamma_K \to \operatorname{Ker}\phi$. Le membre de gauche de (3-9) étant un cocycle, il en va de même pour λ puisque j est injectif. De même, on a

$$\mathrm{d}\varepsilon' + \mathfrak{x} \cup y' + x' \cup \mathfrak{y} + x' \cup y' + \mathrm{d}(x' \otimes \mathfrak{y}) = j_*\lambda' \tag{3-10}$$

pour un 2-cocycle $\lambda' : \Gamma_K \times \Gamma_K \to \operatorname{Ker}\phi$. Considérons maintenant la 1-cochaîne

$$e := \varepsilon' - \varepsilon - (x + \mathfrak{x}) \cup \eta + \xi \cup (y' + \mathfrak{y}) + \mathrm{d}\xi \otimes \mathfrak{y} : \Gamma_K \to M \otimes M.$$

Alors $\phi_* e = c$. Calculons le cobord

$$\begin{aligned} \mathrm{d}e &= \mathrm{d}\varepsilon' - \mathrm{d}\varepsilon + (x + \mathfrak{x}) \cup \mathrm{d}\eta + \mathrm{d}\xi \cup (y' + \mathfrak{y}) + \mathrm{d}(\mathrm{d}\xi \otimes \mathfrak{y}) \\ &= \mathrm{d}\varepsilon' - \mathrm{d}\varepsilon + (x + \mathfrak{x}) \cup (y' - y) + (x' - x) \cup (y' + \mathfrak{y}) + \mathrm{d}((x' - x) \otimes \mathfrak{y}) \\ &= (\mathrm{d}\varepsilon' + \mathfrak{x} \cup y' + x' \cup \mathfrak{y} + x' \cup y' + \mathrm{d}(x' \otimes \mathfrak{y})) - (\mathrm{d}\varepsilon + \mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y})) \\ &= j_*(\lambda' - \lambda), \end{aligned}$$

où la dernière égalité vient de (3-9) et (3-10). Par définition de δ, on a $\delta([c]) = [\lambda' - \lambda]$. □

4. Calculs des groupes de Brauer

4A. *Généralités.* Soit K un corps de caractéristique nulle et soit X un K-espace homogène de SL_m. Rappelons d'abord quelques groupes associés à X.

— Soit $\overline{X} = X \times_K \overline{K}$, alors $\operatorname{Br} \overline{X}$ est le *groupe de Brauer géométrique* de X.

— $\operatorname{Br}_1 X = \operatorname{Ker}(\operatorname{Br} X \to \operatorname{Br} \overline{X})$ est le *groupe de Brauer algébrique* de X et

$$\operatorname{Br}_{\mathrm{nr},1} X = \operatorname{Br}_1 X \cap \operatorname{Br}_{\mathrm{nr}} X$$

est sa *partie non ramifiée.*

— $\operatorname{Br}_0 X = \operatorname{Im}(\operatorname{Br} K \to \operatorname{Br} X) \subseteq \operatorname{Br}_{\mathrm{nr},1} X$ est le *sous-groupe des éléments constants* de $\operatorname{Br} X$.

— $\operatorname{Br}_a X = (\operatorname{Br}_1 X)/(\operatorname{Br}_0 X)$ est le *groupe de Brauer arithmétique* de X et

$$\operatorname{Br}_{\mathrm{nr},a} X = (\operatorname{Br}_{\mathrm{nr},1})/(\operatorname{Br}_0 X)$$

est sa partie non ramifiée.

— Lorsque $K = k$ est un corps de nombres, on note $X_v = X \times_k k_v$ pour toute place v de k. On définit les groupes

$$\text{Б}(X) = \operatorname{Ker}\Big(\operatorname{Br}_a X \to \prod_{v \in \Omega_k} \operatorname{Br}_a X_v\Big) = \{\alpha \in \operatorname{Br}_a X : \forall v \in \Omega_k, \alpha_v = 0\}$$

et

$$\text{Б}_\omega(X) = \{\alpha \in \operatorname{Br}_a X : \alpha_v = 0 \text{ pour presque tout } v \in \Omega_k\}.$$

Notons F le stabilisateur géométrique de X, qu'on suppose fini. Alors F est muni d'une action extérieure de Γ_K (cf. paragraphe 3A), ce qui induit une action de Γ_K sur $F^{\mathrm{ab}} = F/[F, F]$. Les groupes $\operatorname{Br}_a X$, $\text{Б}(X)$ et $\text{Б}_\omega(X)$ s'expriment en termes de F^{ab} ; c'est un argument classique qui se trouve par exemple dans [Skorobogatov 2001, Theorem 4.1.1].

Rappelons que $\hat{-}$ désigne le foncteur de dual de Cartier.

Proposition 4.1. *Soit K un corps de caractéristique nulle satisfaisant $\mathrm{H}^3(K, \overline{K}^\times) = 0$ et soit X un K-espace homogène de SL_m à stabilisateur géométrique F. On munit $\hat{F} = \operatorname{Hom}(F, \overline{K}^\times)$ de l'action de Γ_K induite par son action extérieure sur F.*

1. On a $\operatorname{Br}_a X = \mathrm{H}^1(K, \hat{F})$.

2. *Si $K = k$ est un corps de nombres, $Б(X) = Ш^1(k, \hat{F})$ et $Б_\omega(X) = Ш^1_\omega(k, \hat{F})$.*

Appliquons maintenant la proposition 4.1 aux espaces homogènes de Borovoi–Kunyavskii.

Corollaire 4.2. *Soient k un corps de nombres, M et Z des Γ_k-modules finis, et $\phi : M \otimes M \to Z$ un morphisme Γ_k-équivariant. À partir de ϕ, on construit l'extension*

$$0 \to Z \to F \to M \oplus M \to 0$$

de groupes abstraits comme dans le paragraphe 3B. Supposons $Z = Z(F) = [F, F]$. Si X est un espace homogène de SL_m à stabilisateur géométrique F (muni de n'importe quelle action extérieure de Γ_k compatible avec celles sur Z et sur $M \oplus M$, pas nécessairement celle induite par l'action coordonnée par coordonnée), alors $Б(X) = Ш^1(k, \hat{M})^2$ et $Б_\omega(X) = Ш^1_\omega(k, \hat{M})^2$.

Démonstration. Puisque $Z = [F, F]$, $F^{\mathrm{ab}} = F/Z = M \oplus M$ et donc $\hat{F} = \hat{F}^{\mathrm{ab}} = \hat{M} \oplus \hat{M}$. Ainsi, la proposition 4.1 donne $Б(X) = Ш^1(k, \hat{F}) = Ш^1(k, \hat{M})^2$ et $Б_\omega(X) = Ш^1_\omega(k, \hat{F}) = Ш^1_\omega(k, \hat{M})^2$. □

4B. *Étude de la flèche* $\mathbf{H}^1(K, F) \to \mathbf{H}^1(K, F^{\mathrm{ab}})$. Soit X un espace homogène de Borovoi–Kunyavskii sur un corps de nombres k. Afin de calculer le sous-groupe $\mathrm{Br}_{\mathrm{nr},a} X$ de $\mathrm{Br}_a X$, on va utiliser la formule de Demarche. Il faudra étudier l'image de la flèche $\mathrm{H}^1(k_v, F) \to \mathrm{H}^1(k_v, F^{\mathrm{ab}})$ (cette image n'est pas forcément un sous-groupe de $\mathrm{H}^1(k_v, F^{\mathrm{ab}})$) pour presque toute place v de k.

On se donne alors un corps p-adique K et un K-groupe fini F. Dans le cas où F est un K-groupe constant, Demarche [2010, §3] a donné une description assez explicite du sous-groupe de $\mathrm{H}^1(K, F^{\mathrm{ab}})$ engendré par l'image de la flèche $\mathrm{H}^1(K, F) \to \mathrm{H}^1(K, F^{\mathrm{ab}})$. Nous allons adapter son argument pour le cas où F est un K-groupe *non ramifié*, c'est-à-dire que l'action du sous-groupe d'inertie de Γ_K sur F est trivial.

On note respectivement K_{nr} et K_{mr} l'extension maximale non ramifiée et modérément ramifiée de K. Soit q le cardinal du corps résiduel de K. Notons $\pi : F \to F^{\mathrm{ab}}$ la projection. Posons $\Gamma = \mathrm{Gal}(K_{\mathrm{mr}}/K) = \overline{\langle \sigma, \tau : \sigma\tau\sigma^{-1} = \tau^q \rangle}$. Par l'hypothèse que F est non ramifié, τ agit trivialement sur F. Étudions la flèche $\pi_* : \mathrm{H}^1(\Gamma, F) \to \mathrm{H}^1(\Gamma, F^{\mathrm{ab}})$.

Soit $f : \Gamma \to F$ un cocycle. Comme τ agit trivialement sur F, on a

$$f(\tau)^q = f(\tau^q) = f(\sigma\tau\sigma^{-1}) = f(\sigma)\,{}^{\sigma}\!f(\tau)\,{}^{\sigma\tau}\!f(\sigma^{-1}) = f(\sigma)\,{}^{\sigma}\!f(\tau)\,{}^{\sigma}\!f(\sigma^{-1}).$$

Comme $1 = f(1) = f(\sigma\sigma^{-1}) = f(\sigma)\,{}^{\sigma}\!f(\sigma^{-1})$, on obtient ${}^{\sigma}\!f(\sigma^{-1}) = f(\sigma)^{-1}$ et donc

$$f(\tau)^q = f(\sigma)\,{}^{\sigma}\!f(\tau) f(\sigma)^{-1}.$$

Inversement, soient $a, b \in F$ tels que $a\,{}^{\sigma}b a^{-1} = b^q$. Alors il existe un unique cocycle $f : \Gamma \to F$ tel que $f(\sigma) = a$ et $f(\tau) = b$.

Définition 4.3. On appelle *q-relevable* tout élément $\bar{b} \in F^{\mathrm{ab}}$ ayant un relevé $b \in F$ tel que b^q soit conjugué à ${}^{\sigma}b$ (en particulier, ${}^{\sigma}\bar{b} = \bar{b}^q$).

L'inverse d'un élément q-relevable est encore q-relevable.

Si $f, g : \Gamma \to F^{\mathrm{ab}}$ sont deux cocycles cohomologues, alors $f(\tau) = g(\tau)$ (car l'action de τ sur F est triviale), donc $f(\tau)$ est q-relevable si et seulement si $g(\tau)$ l'est aussi.

On note $I(F)$ l'image de la flèche $\pi_* : \mathrm{H}^1(\Gamma, F) \to \mathrm{H}^1(\Gamma, F^{\mathrm{ab}})$, et $J(F)$ le sous-ensemble de $\mathrm{H}^1(\Gamma, F^{\mathrm{ab}})$ formé des classes des cocycles f tels que $f(\tau)$ soit q-relevable. Alors c'est évident que $I(F) \subseteq J(F)$, et que $J(F)$ est stable par l'inversion.

Lemme 4.4. *Les sous-groupes de* $\mathrm{H}^1(\Gamma, F^{\mathrm{ab}})$ *engendrés par* $I(F)$ *et par* $J(F)$ *coïncident.*

Démonstration. Soit $f : \Gamma \to F^{\mathrm{ab}}$ un cocycle tel que $[f] \in J(F)$. Il existe un relevé $b \in F$ de $f(\tau)$ et un élément $a \in F$ tel que $a^{\sigma}ba^{-1} = b^q$. Soit $\tilde{f}_1 : \Gamma \to F^{\mathrm{ab}}$ le cocycle déterminé par $\tilde{f}_1(\sigma) = a$ et $\tilde{f}_1(\tau) = b$. Posons $f_1 = \pi \circ \tilde{f}_1$, alors $f_1(\sigma) = \pi(a)$ et $f_1(\tau) = f(\tau)$.

Soit $a' \in F$ un relevé de $\pi(a)^{-1} f(\sigma)$. Soit $\tilde{f}_2 : \Gamma \to F$ le cocycle déterminé par $\tilde{f}_2(\sigma) = a'$ et $\tilde{f}_2(\tau) = 1$. Posons $f_2 = \pi \circ \tilde{f}_2$, alors $f_1(\sigma) f_2(\sigma) = f(\sigma)$ et $f_1(\tau) f_2(\tau) = f(\tau)$, donc $[f] = [f_1] + [f_2] \in \mathrm{H}^1(\Gamma, F^{\mathrm{ab}})$. Comme $[f_1], [f_2] \in I(F)$, $[f]$ appartient au sous-groupe engendré par $I(F)$. □

Proposition 4.5. *Soit K un corps p-adique et notons q le cardinal du corps résiduel de K. Soit $\sigma \in$* $\mathrm{Gal}(K_{\mathrm{mr}}/K)$ *un relevé de l'automorphisme de Frobenius. Soit F un K-groupe fini non ramifié de cardinal $|F| < p$. Alors on a équivalence entre* :

1. $\mathrm{H}^1(K, F^{\mathrm{ab}})$ *est engendré par l'image de la flèche* $\mathrm{H}^1(K, F) \to \mathrm{H}^1(K, F^{\mathrm{ab}})$.
2. *Le sous-groupe* $\{a \in F^{\mathrm{ab}} : {}^{\sigma}a = a^q\}$ *de* F^{ab} *est engendré par les éléments q-relevables.*

Démonstration. Pour tout cocycle $f : \Gamma_K \to F$, l'ensemble $\{\upsilon \in \Gamma_K : f(\upsilon) = 1\}$ est un sous-groupe ouvert de Γ_K. Il correspond à une extension finie L/K. On vérifie sans peine que pour tous $\upsilon, \upsilon' \in \Gamma_K$, $f(\upsilon') = f(\upsilon)$ équivaut à $\upsilon' \in \upsilon\Gamma_L$. En particulier, $[L : K] = [\Gamma_K : \Gamma_L] \le |F| < p$, donc L/K est modérément ramifiée. Ainsi, tout cocycle $\Gamma_K \to F$ se factorise par un cocycle $\mathrm{Gal}(K_{\mathrm{mr}}/K) \to F$ et il en va de même pour F^{ab}. Donc le premier point équivaut à dire que $\mathrm{H}^1(\mathrm{Gal}(K_{\mathrm{mr}}/K), F^{\mathrm{ab}})$ est engendré par l'image $I(F)$ de la flèche $\mathrm{H}^1(\mathrm{Gal}(K_{\mathrm{mr}}/K), F) \to \mathrm{H}^1(\mathrm{Gal}(K_{\mathrm{mr}}/K), F^{\mathrm{ab}})$.

Soit τ un générateur topologique de $\mathrm{Gal}(K_{\mathrm{mr}}/K_{\mathrm{nr}})$, de sorte que $\sigma\tau\sigma^{-1} = \tau^q$.

Supposons 1. Soit $a \in F^{\mathrm{ab}}$ satisfaisant ${}^{\sigma}a = a^q$. Alors on peut définir un cocycle

$$f : \mathrm{Gal}(K_{\mathrm{mr}}/K) \to F^{\mathrm{ab}}$$

par $f(\sigma) = 1$ et $f(\tau) = a$. Comme $I(F) \subseteq J(F)$, on peut écrire $[f] = [f_1] + \cdots + [f_r]$, où $[f_i] \in J(F)$, c'est-à-dire que chacun des $f_i(\tau)$ est q-relevable. Or τ agit trivialement sur F^{ab}, donc $a = f(\tau) = f_1(\tau) \cdots f_r(\tau)$, d'où 2.

Supposons 2. Soit $f : \mathrm{Gal}(K_{\mathrm{mr}}/K) \to F^{\mathrm{ab}}$ un cocycle. Alors ${}^{\sigma}f(\tau) = f(\tau)^q$ et donc $f(\tau) = \bar{b}_1 \cdots \bar{b}_r$, où chaque $\bar{b}_i \in F^{\mathrm{ab}}$ est q-relevable. Définissons les cocycles $f_i : \mathrm{Gal}(K_{\mathrm{mr}}/K) \to F^{\mathrm{ab}}$ par

$$\begin{aligned} &f_1(\sigma) = f(\sigma), \quad && f_1(\tau) = \bar{b}_1, \\ &f_i(\sigma) = 1, && f_i(\tau) = \bar{b}_i, \quad i = 2, \ldots, r. \end{aligned}$$

Alors $[f_i] \in J(F)$ et $[f] = [f_1] + \cdots + [f_r]$, donc $[f]$ appartient au sous-groupe engendré par $J(F)$. Par le lemme 4.4, $[f]$ appartient au sous-groupe engendré par l'image de $\mathrm{H}^1(\mathrm{Gal}(K_{\mathrm{mr}}/K), F) \to \mathrm{H}^1(\mathrm{Gal}(K_{\mathrm{mr}}/K), F^{\mathrm{ab}})$, d'où 1. □

4C. ***Groupe de Brauer arithmétique.*** Nous allons maintenant combiner l'analyse du paragraphe 4B avec la formule de Demarche pour calculer le groupe de Brauer arithmétique non ramifié d'un espace homogène de Borovoi–Kunyavskii.

Rappelons d'abord la dualité locale de Tate (voir par exemple [Harari 2017, chapitre 10]). Soit K un corps p-adique K et soit A un Γ_K-module fini, alors l'accouplement

$$\mathrm{H}^1(K, \hat{A}) \times \mathrm{H}^1(K, A) \to \mathbb{Q}/\mathbb{Z}, \quad (\alpha, a) \mapsto \mathrm{inv}_K(\alpha \cup a)$$

est une dualité parfaite de groupes abéliens finis.

Proposition 4.6. *Soient k un corps de nombres, M et Z des Γ_k-modules finis, et $\phi : M \otimes M \to Z$ un morphisme Γ_k-équivariant. À partir de ϕ, on construit l'extension*

$$0 \to Z \to F \to M \oplus M \to 0$$

de groupes abstraits comme dans le paragraphe 3B. Supposons $Z = Z(F) = [F, F]$.

1. *On munit F de l'action coordonnée par coordonnée de Γ_k. Alors le groupe $\mathrm{H}^1(k_v, F^{\mathrm{ab}})$ est engendré par l'image de la flèche $\mathrm{H}^1(k_v, F) \to \mathrm{H}^1(k_v, F^{\mathrm{ab}})$ pour presque tout $v \in \Omega_k$.*
2. *Soit X est un espace homogène de SL_m à stabilisateur géométrique F, muni de l'action extérieure de Γ_k induite par l'action coordonnée par coordonnée. Alors $\mathrm{Br}_{\mathrm{nr},a} X = Б_\omega(X) = Ш^1_\omega(k, \hat{M})^2$.*

Démonstration. 1. Soit L/k une extension finie galoisienne déployant F. Soit v une place de k qui est non ramifiée dans L/k, et qui divise un nombre premier impair $p > |F|$. On va démontrer que $\mathrm{H}^1(k_v, F^{\mathrm{ab}})$ est engendré par l'image de la flèche $\mathrm{H}^1(k_v, F) \to \mathrm{H}^1(k_v, F^{\mathrm{ab}})$. Au vu de la proposition 4.5, il suffit de démontrer que tout élément $a \in F^{\mathrm{ab}}$ satisfaisant ${}^{\sigma}a = qa$ est q-relevable, où q est le cardinal du corps résiduel de k_v et où $\sigma \in \mathrm{Gal}(k_{v,\mathrm{mr}}/k_v)$ est un relevé de l'automorphisme de Frobenius. Notons que $F^{\mathrm{ab}} = F/[F, F] = F/Z = M \oplus M$.

Rappelons de (3-1) qu'on dispose d'une application biadditive

$$\Phi : (M \oplus M) \times (M \oplus M) \to Z, \quad ((x, y), (x', y')) \mapsto \phi(x \otimes y').$$

Soit $a = (x, y) \in M \oplus M$ tel que ${}^{\sigma}a = qa$ et montrons que a est q-relevable. Considérons alors le relevé $(0, a) \in F$ de a. On va démontrer que $(0, a)^q$ est conjugué à ${}^{\sigma}(0, a) = (0, qa)$. À l'aide de (3-2), on peut calculer

$$(0, a)^q = \bigl(\tfrac{1}{2}q(q-1)\Phi(a, a), qa\bigr) \tag{4-1}$$

par récurrence. Soit $a' = \bigl(\frac{1}{2}(q+1)x, y\bigr)$. Alors

$$\Phi(qa, a') = \phi(qx \otimes y) = q\Phi(a, a) \quad \text{et} \quad \Phi(a', qa) = \phi\bigl(\tfrac{1}{2}(q+1)x \otimes qy\bigr) = \tfrac{1}{2}q(q+1)\Phi(a, a). \tag{4-2}$$

On a

$$\begin{aligned}(0,a')(0,qa)(0,a')^{-1} &= (\Phi(a',qa)-\Phi(qa,a'),qa) && \text{(par le lemme 3.5)}\\ &= \big(\tfrac{1}{2}q(q+1)\Phi(a,a)-q\Phi(a,a),qa\big) && \text{(par (4-2))}\\ &= \big(\tfrac{1}{2}q(q-1)\Phi(a,a),qa\big)\\ &= (0,a)^q && \text{(par (4-1)),}\end{aligned}$$

donc $(0,a)^q$ est bien conjugué à $(0,qa)={}^{\sigma}(0,a)$, d'où a est q-relevable. Cela nous permet de conclure que $\mathrm{H}^1(k_v,F^{\mathrm{ab}})$ est engendré par l'image de $\mathrm{H}^1(k_v,F)\to\mathrm{H}^1(k_v,F^{\mathrm{ab}})$ pour presque toute place v de k.

2. Rappelons que $\mathrm{Br}_a X=\mathrm{H}^1(k,\hat{F})=\mathrm{H}^1(k,\hat{M})^2$ et que $\mathrm{Br}_a X_v=\mathrm{H}^1(k_v,\hat{F})=\mathrm{H}^1(k_v,\hat{M})^2$ pour toute place v de k ; cf. proposition 4.1. Soit $\eta_0\in\mathrm{H}^2(k,F)$ la classe neutre privilégiée (où F est muni de l'action coordonnée par coordonnée de Γ_k). Alors il existe une unique classe $\beta\in\mathrm{H}^2(k,Z)$ telle que la classe de Springer de X vaut $\eta_X=\beta\cdot\eta_0$ (cf. paragraphe 3A). Pour presque tout $v\in\Omega_k$, on a $\beta_v=0\in\mathrm{H}^2(k_v,Z)$, donc $\mathrm{loc}_v(\eta_X)=\mathrm{loc}_v(\eta_0)$, ou X_v est k_v-isomorphe à $F\backslash\mathrm{SL}_m$ (voir proposition 3.3). Par la formule de Demarche [2010, théorème 1], un élément $\alpha\in\mathrm{Br}_a X$ appartient à $\mathrm{Br}_{\mathrm{nr},a} X$ si et seulement si pour presque tout $v\in\Omega_k$, l'image de α_v dans $\mathrm{H}^1(k_v,\hat{F})$ est orthogonale à l'image de $\mathrm{H}^1(k_v,F)\to\mathrm{H}^1(k_v,F^{\mathrm{ab}})$. Par dualité locale de Tate, cette dernière propriété signifie que $\alpha_v=0$ pour presque tout $v\in\Omega_k$, i.e., que $\alpha\in\text{Б}_\omega(X)$. Ainsi, $\mathrm{Br}_{\mathrm{nr},a} X=\text{Б}_\omega(X)=\text{Ш}^1_\omega(k,\hat{F})=\text{Ш}^1_\omega(k,\hat{M})^2$. □

4D. ***Groupe de Brauer géométrique.*** Dans ce paragraphe, soit K un corps *algébriquement clos* de caractéristique nulle. Pour calculer le groupe de Brauer géométrique non ramifié des espaces homogènes de Borovoi–Kunyavskii, on rappelle la formule suivante de Bogomolov [1987, §3].

Proposition 4.7. *Soit F un groupe fini, vu comme K-groupe. On choisit un plongement $F\hookrightarrow\mathrm{SL}_m$ de K-groupes et l'on pose $X=F\backslash\mathrm{SL}_m$. Alors*

$$\mathrm{Br}_{\mathrm{nr}} X=B_0(F):=\mathrm{Ker}\Big(\mathrm{H}^2(F,\mathbb{Q}/\mathbb{Z})\to\prod_A\mathrm{H}^2(A,\mathbb{Q}/\mathbb{Z})\Big),$$

où A parcourt les sous-groupes abéliens de F.

Lorsque F est nilpotent de classe 2, on dispose d'un morphisme

$$\lambda_F:\bigwedge^2 F^{\mathrm{ab}}\to Z,\quad \lambda(a\wedge b)=[\tilde{a},\tilde{b}],\tag{4-3}$$

où $Z=Z(F)$ et où $\tilde{a},\tilde{b}\in F$ sont des relevés respectifs de $a,b\in F^{\mathrm{ab}}$. Si de plus $Z=[F,F]$, c'est-à-dire que λ_F est surjectif (par exemple, pour les espaces homogènes de Borovoi–Kunyavskii), le groupe $B_0(F)$ a la description explicite en [Bogomolov 1987, Lemma 5.1]. (En fait, l'énoncé dans loc. cit. demande que F soit un p-groupe, mais sa démonstration vaut pour F de cardinal quelconque.) Un énoncé similaire se trouve dans [Moravec 2012, §5]. On rappellera la preuve pour la commodité du lecteur.

Lemme 4.8. *Soit F un groupe fini vérifiant $Z(F)=[F,F]$. Notons $Z=Z(F)$ et $\lambda=\lambda_F$ le morphisme surjectif défini par* (4-3). *Alors $B_0(F)=\mathrm{Hom}(S/S_\lambda,\mathbb{Q}/\mathbb{Z})$, où $S=\mathrm{Ker}\,\lambda$ et où S_λ est le sous-groupe de S engendré par $S\cap\{a\wedge b:a,b\in F^{\mathrm{ab}}\}$.*

Démonstration. La première étape est de montrer que $B_0(F)$ est inclus dans l'image du morphisme d'inflation $\pi^* : \mathrm{H}^2(F^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(F, \mathbb{Q}/\mathbb{Z})$ (où $\pi : F \to F^{\mathrm{ab}}$ désigne la projection). C'est le lemme 3.5 dans [Bogomolov 1987] : dans la suite spectrale de Hochschild–Serre $\mathrm{H}^p(F^{\mathrm{ab}}, \mathrm{H}^q(Z, \mathbb{Q}/\mathbb{Z})) \Rightarrow \mathrm{H}^{p+q}(F, \mathbb{Q}/\mathbb{Z})$, le groupe $\mathrm{H}^2(F, \mathbb{Q}/\mathbb{Z})$ admet une filtration $E_0 \subseteq E_1 \subseteq E_2$, où $E_0 \subseteq \mathrm{H}^2(F, \mathbb{Q}/\mathbb{Z})$ est l'image de π^*, où $E_1/E_0 \subseteq \mathrm{H}^1(F^{\mathrm{ab}}, \mathrm{H}^1(Z, \mathbb{Q}/\mathbb{Z}))$, et où $E_2/E_1 \subseteq \mathrm{H}^2(Z, \mathbb{Q}/\mathbb{Z})$. Pour tout $\alpha \in B_0(F)$, son image (par restriction) dans $\mathrm{H}^2(Z, \mathbb{Q}/\mathbb{Z})$ est nulle, on peut alors considérer son image β dans $\mathrm{H}^1(F^{\mathrm{ab}}, \mathrm{H}^1(Z, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}(F^{\mathrm{ab}}, \mathrm{Hom}(Z, \mathbb{Q}/\mathbb{Z}))$. Il suffit de montrer que $\beta = 0$. En effet, soit $C \subseteq F^{\mathrm{ab}}$ n'importe quel sous-groupe cyclique. On dispose de la suite spectrale de Hochschild–Serre $\mathrm{H}^p(C, \mathrm{H}^q(Z, \mathbb{Q}/\mathbb{Z})) \Rightarrow \mathrm{H}^{p+q}(\pi^{-1}(C), \mathbb{Q}/\mathbb{Z})$, d'où une filtration $\tilde{E}_0 \subseteq \tilde{E}_1 \subseteq \tilde{E}_2$ compatible avec celle mentionnée ci-dessus. Le sous-groupe $\pi^{-1}(C) \subseteq F$ est abélien (c'est une extension centrale du groupe cyclique C). La classe α étant dans $B_0(F)$, elle se restreint à $0 \in \mathrm{H}^2(\pi^{-1}(C), \mathbb{Q}/\mathbb{Z})$, donc on a $\beta|_C = 0 \in \mathrm{H}^1(C, \mathrm{H}^1(Z, \mathbb{Q}/\mathbb{Z}))$. Cela implique que $\beta = 0$, ou $\alpha \in E_0 = \mathrm{Im}\,\pi^*$.

La deuxième étape est de décrire $\mathrm{Im}\,\pi^*$. Il est connu qu'on a un isomorphisme

$$\mathrm{H}^2(F^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}\Big(\bigwedge^2 F^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}\Big) \tag{4-4}$$

qui à la classe $[E]$ de toute extension centrale $0 \to \mathbb{Q}/\mathbb{Z} \to E \to F^{\mathrm{ab}} \to 0$ associe le morphisme $\lambda_E : \bigwedge^2 F^{\mathrm{ab}} \to \mathbb{Q}/\mathbb{Z}$ défini par (4-3). Si $\pi^*[E] = 0 \in \mathrm{H}^2(F, \mathbb{Q}/\mathbb{Z})$, la projection $\pi : F \to F^{\mathrm{ab}}$ se relève en un morphisme $\rho : F \to E$. Dans ce cas, ρ induit un morphisme $\chi : Z \to \mathbb{Q}/\mathbb{Z}$ satisfaisant $\lambda_E = \chi \circ \lambda$. Inversement, supposons qu'il existe un morphisme $\chi : Z \to \mathbb{Q}/\mathbb{Z}$ tel que $\lambda_E = \chi \circ \lambda$, alors $[E] = \chi_*[F]$, où $\chi_* : \mathrm{H}^2(F^{\mathrm{ab}}, Z) \to \mathrm{H}^2(F^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z})$ est le morphisme induit par χ. Or $\pi^*[F] = 0 \in \mathrm{H}^2(F, Z)$, donc $\pi^*[E] = 0 \in \mathrm{H}^2(F, \mathbb{Q}/\mathbb{Z})$ puisque les opérateurs π^* et χ_* commutent. On en déduit que sous l'identification de (4-4), $\mathrm{Ker}\,\pi^*$ correspond au sous-groupe $\mathrm{Hom}(Z, \mathbb{Q}/\mathbb{Z}) \subseteq \mathrm{Hom}\big(\bigwedge^2 F^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}\big)$ (l'inclusion étant induite par la surjection λ). On conclut que $\mathrm{Im}\,\pi^* = \mathrm{Hom}(S, \mathbb{Q}/\mathbb{Z})$.

Soit maintenant $0 \to \mathbb{Q}/\mathbb{Z} \to E \to F^{\mathrm{ab}} \to 0$ une extension centrale et $\chi : S \to \mathbb{Q}/\mathbb{Z}$ la restriction de λ_E. Soient $a, b \in F^{\mathrm{ab}}$ tels que $a \wedge b \in S$, et relevons-les respectivement en $\tilde{a}, \tilde{b} \in F$. Comme $a \wedge b \in S$, la formule (4-3) implique que $\tilde{a}$ et $\tilde{b}$ commutent, donc le sous-groupe $\langle \tilde{a}, \tilde{b} \rangle \subseteq F$ est abélien. Si $[E] \in B_0(F)$, la composée $\bigwedge^2 \langle \tilde{a}, \tilde{b} \rangle \to \bigwedge^2 F^{\mathrm{ab}} \xrightarrow{\lambda_E} \mathbb{Q}/\mathbb{Z}$ est nulle, donc en particulier $\chi(a \wedge b) = \lambda_E(a \wedge b) = 0$. Ainsi, $[E] \in B_0(F)$ implique $\chi|_{S_\lambda} = 0$. Inversement, supposons $\chi|_{S_\lambda} = 0$. Soit $A \subseteq F$ un sous-groupe abélien. Pour tous $\tilde{a}, \tilde{b} \in A$, on a $\lambda(a \wedge b) = 0$ (où $a = \pi(\tilde{a})$ et $b = \pi(\tilde{b})$), donc $a \wedge b \in S_\lambda$, d'où $\lambda_E(a \wedge b) = \chi(a \wedge b) = 0$. La composée $\bigwedge^2 A \to \bigwedge^2 F^{\mathrm{ab}} \xrightarrow{\lambda_E} \mathbb{Q}/\mathbb{Z}$ est nulle, donc $[E] \mapsto 0 \in \mathrm{H}^2(A, \mathbb{Q}/\mathbb{Z})$. On en déduit que $[E] \in B_0(F)$. Ainsi

$$B_0(F) = \mathrm{Ker}(\mathrm{Hom}(S, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(S_\lambda, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}(S/S_\lambda, \mathbb{Q}/\mathbb{Z}). \qquad \square$$

Proposition 4.9. *Soient M et Z des groupes abéliens, $\phi : M \otimes M \to Z$ un morphisme, à partir desquels on construit une extension*

$$0 \to Z \to F \to M \oplus M \to 0$$

de groupes abstraits comme dans le paragraphe 3B, vue comme extension de K-groupes finis. Supposons $Z = Z(F) = [F, F]$, soit $F \hookrightarrow \mathrm{SL}_m$ un plongement de K-groupes et notons $X = F\backslash \mathrm{SL}_m$. Alors $\mathrm{Br}_{\mathrm{nr}} X = \mathrm{Hom}((\mathrm{Ker}\,\phi)/H, \mathbb{Q}/\mathbb{Z})$, *où H est le sous-groupe $\langle x \otimes y : x, y \in M, \phi(x \otimes y) = 0\rangle$ de $M \otimes M$.*

Démonstration. Sous l'identification $\bigwedge^2(M \oplus M) = \big(\bigwedge^2 M\big) \oplus (M \otimes M) \oplus \big(\bigwedge^2 M\big)$, on a

$$(x, y) \wedge (x', y') = (x \wedge x', x \otimes y', y \wedge y')$$

pour tous $x, y, x', y' \in M$. Soit $\lambda = \lambda_F : \bigwedge^2(M \oplus M) \to Z$ le morphisme défini par (4-3). On note $\Phi : (M \oplus M) \times (M \oplus M) \to Z$ l'application biadditive définie par (3-1). Par le lemme 3.5, on a

$$\begin{aligned}
&\lambda(x \wedge y, 0, 0) = \lambda((x, 0) \wedge (y, 0)) = \Phi((x, 0), (y, 0)) - \Phi((y, 0), (x, 0)) = \phi(x \otimes 0) - \phi(y \otimes 0) = 0,\\
&\lambda(0, x \otimes y, 0) = \lambda((x, 0) \wedge (0, y)) = \Phi((x, 0), (0, y)) - \Phi((0, y), (x, 0)) = \phi(x \otimes y) - \phi(0 \otimes 0)\\
&\qquad\qquad = \phi(x \otimes y),\\
&\lambda(0, 0, x \wedge y) = \lambda((0, x) \wedge (0, y)) = \Phi((0, x), (0, y)) - \Phi((0, y), (0, x)) = \phi(0 \otimes y) - \phi(0 \otimes x) = 0.
\end{aligned}$$

On en déduit que $\lambda(\gamma_1, \gamma_2, \gamma_3) = \phi(\gamma_2)$ pour tous $\gamma_1, \gamma_3 \in \bigwedge^2 M$ et $\gamma_2 \in M \otimes M$, d'où $S = \mathrm{Ker}\,\lambda = \bigwedge^2(M \oplus M) = \big(\bigwedge^2 M\big) \oplus (\mathrm{Ker}\,\phi) \oplus \big(\bigwedge^2 M\big)$, au vu des notations du lemme 4.8.

Nous affirmons que $S_\lambda = \bigwedge^2(M \oplus M) = \big(\bigwedge^2 M\big) \oplus H \oplus \big(\bigwedge^2 M\big)$. En effet, soient $x, y, x', y' \in M$. Alors $\lambda((x, y) \wedge (x', y')) = \lambda'(x \wedge x', x \otimes y', y \wedge y') = \phi(x \otimes y')$, donc $(x, y) \wedge (x', y') \in S$ si et seulement si $\phi(x \otimes y') = 0$. Dans ce cas, $x \otimes y' \in H$ par définition, d'où $S_\lambda \subseteq \big(\bigwedge^2 M\big) \oplus H \oplus \big(\bigwedge^2 M\big)$. Inversement :

— $\big(\bigwedge^2 M\big) \oplus \{0\} \oplus \{0\} \subseteq S_\lambda$ puisque $(x \wedge y, 0, 0) = (x, 0) \wedge (y, 0) \in S$ pour tous $x, y \in M$.

— $\{0\} \oplus \{0\} \oplus \big(\bigwedge^2 M\big) \subseteq S_\lambda$ puisque $(0, 0, x \wedge y) = (0, x) \wedge (0, y) \in S$ pour tous $x, y \in M$.

— $\{0\} \oplus H \oplus \{0\} \subseteq S_\lambda$ puisque $(0, x \otimes y, 0) = (x, 0) \wedge (0, y) \in S$ pour tous $x, y \in M$ tels que $\phi(x \otimes y) = 0$.

Ces propriétés impliquent que $S_\lambda = \big(\bigwedge^2 M\big) \oplus H \oplus \big(\bigwedge^2 M\big)$ comme voulu. Finalement, $S/S_\lambda = (\mathrm{Ker}\,\phi)/H$ et donc la proposition 4.7 donne $\mathrm{Br}_{\mathrm{nr}} X = B_0(F) = \mathrm{Hom}(S/S_\lambda, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}((\mathrm{Ker}\,\phi)/H, \mathbb{Q}/\mathbb{Z})$. □

5. Les principaux résultats

5A. *Un lemme arithmétique.* Pour établir les principaux résultats de ce texte, une propriété globale du symbole de Hilbert est nécessaire. On propose la généralisation suivante de [Serre 1970, chapitre III, §2.2, théorème 4].

Proposition 5.1 (« Lemme arithmétique » pour les groupes cycliques). *Soient k un corps de nombres, n un entier et $(a_i)_{i \in I}$ une famille finie d'éléments de $\mathrm{H}^1(k, \mathbb{Z}/n)$. Soit $(\lambda_i)_{i \in I} \in (\mathrm{Br}\,k)^{|I|}$ remplissant la condition suivante : pour tout $v \in \Omega_k$, il existe $c_v \in \mathrm{H}^1(k_v, \mu_n)$ tel que $(a_i)_v \cup c_v = (\lambda_i)_v$ pour tout $i \in I$. Alors pour tout sous-ensemble fini $S \subseteq \Omega_k$, il existe $b \in \mathrm{H}^1(k, \mu_n)$ tel que :*

1. *$a_i \cup b = \lambda_i$ pour tout $i \in I$.*
2. *$b_v = c_v$ pour tout $v \in S$.*

La preuve de la proposition 5.1 repose sur des théorèmes de dualité arithmétique. Pour les détails de la théorie de la dualité arithmétique, on pourra consulter [Harari 2017, chapitre 17]. Rappelons alors quelques notations. Soit k un corps de nombres et soit A un Γ_k-module fini. Pour toute place finie v de k telle que A soit un Γ_{k_v}-module non ramifié, on note $\mathrm{H}^1_{\mathrm{nr}}(k_v, A)$ l'image de la flèche d'inflation $\mathrm{H}^1(\mathrm{Gal}(k_{v,\mathrm{nr}}/k_v), A) \to \mathrm{H}^1(k_v, A)$. Notons $\mathbb{P}^1(k, A)$ le produit restreint $\prod'_{v\in\Omega_k} \mathrm{H}^1(k_v, A)$ par rapport aux sous-groupes $\mathrm{H}^1_{\mathrm{nr}}(k_v, A)$. On dispose d'une application diagonale de $\mathrm{H}^1(k, A)$ dans $\mathbb{P}^1(k, A)$. En rassemblant les dualités locales de Tate entre $\mathrm{H}^1(k_v, A)$ et $\mathrm{H}^1(k_v, \hat{A})$, on obtient un accouplement parfait de groupes abéliens localement compacts

$$\mathbb{P}^1(k, A) \times \mathbb{P}^1(k, \hat{A}) \to \mathbb{Q}/\mathbb{Z}, \quad ((a_v)_{v\in\Omega_k}, (b_v)_{v\in\Omega_k}) \mapsto \sum_{v\in\Omega_k} \mathrm{inv}_v(a_v \cup b_v).$$

Démonstration de la proposition 5.1. Calculons le sous-groupe

$$P = \mathrm{Im}(\mathrm{H}^1(k, \mathbb{Z}/n) \to \mathbb{P}^1(k, \mathbb{Z}/n)) \cap \left(\prod_{v\in S} \mathrm{H}^1(k_v, \mathbb{Z}/n) \times \prod_{v\in\Omega_k\setminus S} \langle (a_i)_v : i \in I\rangle \right)$$

de $\mathbb{P}^1(k, \mathbb{Z}/n)$. Soit alors $a \in \mathrm{H}^1(k, \mathbb{Z}/n)$ tel que pour tout $v \notin S$, a_v soit une combinaison linéaire des $(a_i)_v$, $i \in I$. On voit les a_i et a comme des morphismes continus $\Gamma_k \to \mathbb{Z}/n$; alors il existe un quotient G de Γ_k, qui est fini, abélien et de n-torsion, par lequel ces morphismes se factorisent. Notons $a'_i, a' \in \mathrm{Hom}(G, \mathbb{Z}/n)$ les morphismes induits respectifs. La condition sur a et le théorème de Chebotarev impliquent que $a'|_H \in \langle a'_i|_H : i \in I\rangle$ pour tout sous-groupe cyclique H de G. En appliquant cette condition à chaque sous-groupe cyclique de $\bigcap_{i\in I} \mathrm{Ker}(a'_i)$, on voit que a' s'annule sur $\bigcap_{i\in I} \mathrm{Ker}(a'_i)$. Au vu de l'accouplement parfait entre G et $\mathrm{Hom}(G, \mathbb{Z}/n)$, a' est orthogonal à $\bigcap_{i\in I} \mathrm{Ker}(a'_i)$, qui est l'orthogonal de $\langle a'_i : i \in I\rangle$, ainsi $a' \in \langle a'_i : i \in I\rangle$. Il s'ensuit que $a \in \langle a_i : i \in I\rangle$ et on conclut que $P = \langle ((a_i)_v)_{v\in\Omega_k} : i \in I\rangle$.

Lorsque $v \in \Omega_k \setminus S$ est une place telle que $(\lambda_i)_v = 0$ pour tout $i \in I$, on peut supposer que $c_v = 0$. Cela implique que $(c_v)_{v\in\Omega_k} \in \bigoplus_{v\in\Omega_k} \mathrm{H}^1(k_v, \mu_n) \subseteq \mathbb{P}^1(k, \mu_n)$. Au vu de l'accouplement parfait entre $\mathbb{P}^1(k, \mathbb{Z}/n)$ et $\mathbb{P}^1(k, \mu_n)$, la loi de réciprocité globale implique que $(c_v)_{v\in\Omega_k}$ est orthogonal à $((a_i)_v)_{v\in\Omega_k}$ pour tout $i \in I$, i.e., il est orthogonal à P. Or l'orthogonal de $\mathrm{Im}(\mathrm{H}^1(k, \mathbb{Z}/n) \to \mathbb{P}^1(k, \mathbb{Z}/n))$ est $\mathrm{Im}(\mathrm{H}^1(k, \mu_n) \to \mathbb{P}^1(k, \mu_n))$ (c'est l'exactitude au 5^{e} terme de la suite exacte à neuf termes de Poitou–Tate, cf. [Harari 2017, théorème 17.13]), donc

$$P^\perp = \mathrm{Im}(\mathrm{H}^1(k, \mu_n) \to \mathbb{P}^1(k, \mu_n)) + \prod_{v\in S} \{0\} \times \prod'_{v\in\Omega_k\setminus S} \langle (a_i)_v : i \in I\rangle^\perp,$$

donc il existe $b \in \mathrm{H}^1(k, \mu_n)$ satisfaisant les conditions suivantes :

1. Pour tout $v \in S$, $b_v - c_v = 0$ pour tout $v \in S$.
2. Pour tout $v \notin S$, $b_v - c_v$ est orthogonal aux $(a_i)_v$, $i \in I$.

On a ainsi que $(a_i \cup b)_v = (a_i)_v \cup c_v = (\lambda_i)_v$ pour tous $i \in I$ et $v \in \Omega_k$ (d'où $a_i \cup b = \lambda_i$ par la loi de réciprocité globale) et que $b_v = c_v$ pour tout $v \in S$. La proposition est finalement démontrée. □

La proposition 5.1 se généralise en la proposition 5.2 ci-dessous. Afin de la démontrer, remarquons le fait suivant : soient m et n deux entiers, soit $d = \mathrm{PGCD}(m, n)$, et soit K un corps de caractéristique nulle.

Alors l'on dispose d'un diagramme commutatif de Γ_K-modules, dont les flèches horizontales sont des isomorphismes :

$$\begin{tikzcd}
\mathbb{Z}/m \otimes \mu_n \arrow[r, "\simeq"] \arrow[d, "\iota_n^m \otimes \mathrm{id}"] & \mu_d \arrow[d, hook] \\
\mathbb{Z}/n \otimes \mu_n \arrow[r, "\simeq"] & \mu_n
\end{tikzcd}$$

et dont le morphisme ι_n^m est la composée

$$\mathbb{Z}/m \twoheadrightarrow \mathbb{Z}/d \hookrightarrow \mathbb{Z}/n. \tag{5-1}$$

Il s'ensuit qu'il y a un diagramme commutatif

$$\begin{tikzcd}
\mathrm{H}^1(K, \mathbb{Z}/m) \times \mathrm{H}^1(K, \mu_n) \arrow[r, "\cup"] \arrow[d, "(\iota_n^m)_*"] \arrow[d, phantom, shift left=8, "\Vert"] & (\mathrm{Br}\, K)[d] \arrow[d, hook] \\
\mathrm{H}^1(K, \mathbb{Z}/n) \times \mathrm{H}^1(K, \mu_n) \arrow[r, "\cup"] & (\mathrm{Br}\, K)[n]
\end{tikzcd} \tag{5-2}$$

D'ailleurs, dans le cas où K contient $\mu_{\mathrm{PPCM}(m,n)}$ (un générateur duquel sera fixé), on dispose d'un diagramme commutatif de Γ_K-modules, à lignes exactes :

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}/m \arrow[r] \arrow[d, two heads] & \overline{K}^\times \arrow[r, "(-)^m"] \arrow[d, "(-)^{m/d}"] & \overline{K}^\times \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathbb{Z}/d \arrow[r] \arrow[d, hook] & \overline{K}^\times \arrow[r, "(-)^d"] \arrow[d, equal] & \overline{K}^\times \arrow[r] \arrow[d, "(-)^{n/d}"] & 1 \\
1 \arrow[r] & \mathbb{Z}/n \arrow[r] & \overline{K}^\times \arrow[r, "(-)^n"] & \overline{K}^\times \arrow[r] & 1
\end{tikzcd}$$

d'où un diagramme commutatif

$$\begin{tikzcd}
K^\times \arrow[r] \arrow[d, "(-)^{n/d}"] & \mathrm{H}^1(K, \mathbb{Z}/m) \arrow[d, "(\iota_n^m)_*"] \\
K^\times \arrow[r] & \mathrm{H}^1(K, \mathbb{Z}/n)
\end{tikzcd} \tag{5-3}$$

dont les flèches horizontales sont des morphismes de la théorie de Kummer.

Proposition 5.2 (« Lemme arithmétique » pour les groupes abéliens finis). *Soient k un corps de nombres, A un groupe abélien fini muni de l'action triviale de Γ_k, et $(a_i)_{i \in I}$ une famille finie d'éléments de* $\mathrm{H}^1(k, A)$. *Soit* $(\lambda_i)_{i \in I} \in \mathrm{H}^2(k, A \otimes \hat{A})^{|I|}$ *remplissant la condition suivante : pour tout $v \in \Omega_k$, il existe $c_v \in$* $\mathrm{H}^1(k_v, \hat{A})$ *tel que $(a_i)_v \cup c_v = (\lambda_i)_v$ pour tout $i \in I$. Alors pour tout sous-ensemble fini $S \subseteq \Omega_k$, il existe $b \in$* $\mathrm{H}^1(k, \hat{A})$ *tel que :*

1. $a_i \cup b = \lambda_i$ pour tout $i \in I$.

2. *$b_v = c_v$ pour tout $v \in S$.*

Démonstration. Écrivons $A = \prod_{p\in J} \mathbb{Z}/n_p$ (alors $\hat{A} = \prod_{q\in J} \mu_{n_q}$), et $d_{p,q} = \mathrm{PGCD}(n_p, n_q)$ pour tous $p, q \in J$. De plus, pour tous $i \in I$ et $v \in \Omega_k$, écrivons

$$\begin{aligned} a_i &= (a_i^p)_{p\in J} \in \mathrm{H}^1(k, A) = \prod_{p\in J} \mathrm{H}^1(k, \mathbb{Z}/n_p), \\ c_v &= (c_v^q)_{q\in J} \in \mathrm{H}^1(k_v, \hat{A}) = \prod_{q\in J} \mathrm{H}^1(k_v, \mu_{n_q}), \\ \lambda_i &= (\lambda_i^{p,q})_{p,q\in J} \in \mathrm{H}^2(k, A \otimes \hat{A}) = \prod_{p,q\in J} (\mathrm{Br}\, k)[d_{p,q}]. \end{aligned}$$

La condition $(a_i)_v \cup c_v = (\lambda_i)_v$ se réécrit sous la forme

$$((\iota^{n_p}_{n_q})_* a_i^p)_v \cup c_v^q = (a_i^p)_v \cup c_v^q = (\lambda_i^{p,q})_v \quad \forall p, q \in J \tag{5-4}$$

par biadditivité des cup-produits et au vu de (5-2), où $\iota^{n_p}_{n_q} : \mathbb{Z}/n_p \to \mathbb{Z}/n_q$ est défini comme la composée (5-1). Fixons $q \in J$ et appliquons la proposition 5.1 à la famille $((\iota^{n_p}_{n_q})_* a_i^p)_{i\in I, p\in J}$ pour trouver un $b^q \in \mathrm{H}^1(k, \mu_{n_q})$ tel que :

1. $a_i^p \cup b^q = \lambda_i^{p,q}$ pour tous $i \in I$ et $p \in J$.
2. $b_v^q = c_v^q$ pour tout $v \in S$.

Posons finalement $b = (b^q)_{q\in J} \in \mathrm{H}^1(k, \hat{A})$. Alors $a_i \cup b = \lambda_i$ (par biadditivité des cup-produits), et $b_v = c_v$ pour tout $v \in S$, ce qui achève la démonstration. □

Afin d'appliquer la proposition 5.2, il convient de prouver l'énoncé suivant.

Lemme 5.3. *Soient (K, v) un corps p-adique et n un entier tels que K contienne μ_n. Soit d un diviseur de n et soit $\tilde{a} \in K^\times$ tel que $v(\tilde{a})$ soit premier à d. Soit a son image dans $\mathrm{H}^1(k, \mu_n)$ par la théorie de Kummer. Alors pour tout $r \in (1/d)\mathbb{Z}/\mathbb{Z}$, il existe $b \in \mathrm{H}^1(K, \mathbb{Z}/n)$ tel que $\mathrm{inv}_K(a \cup b) = r$.*

Démonstration. Posons $A := \{\mathrm{inv}_K(a \cup b) : b \in \mathrm{H}^1(K, \mathbb{Z}/n)\} \subseteq \mathbb{Q}/\mathbb{Z}$ et montrons que A contient $1/d$.

Commençons par le cas où $d = n$. Il suffit de montrer que pour tout nombre premier ℓ divisant n, A contient $1/\ell^{v_\ell(n)}$. En effet, comme ℓ ne divise pas $v(\tilde{a})$, on a $(\tilde{a})^{n/\ell} \notin K^{\times n}$ et donc $(n/\ell)a \neq 0$. Par dualité locale de Tate, il existe $b \in \mathrm{H}^1(k, \mathbb{Z}/n)$ tel que $\mathrm{inv}_K((n/\ell)a \cup b) \neq 0$ dans $\mathbb{Q}/\mathbb{Z}$. Écrivons $\mathrm{inv}_K(a \cup b) = t/n$ avec $t \in \mathbb{Z}$, alors $\mathrm{inv}_K((n/\ell)a \cup b) = (n/\ell)\,\mathrm{inv}_K(a \cup b) = t/\ell$ est non nul dans $\mathbb{Q}/\mathbb{Z}$, d'où ℓ ne divise pas t. Or A contient $\mathrm{inv}_K(a \cup (n/\ell^{v_\ell(n)})b) = (n/\ell^{v_\ell(n)})\,\mathrm{inv}_K(a \cup b) = t/\ell^{v_\ell(n)}$, donc il contient $1/\ell^{v_\ell(n)}$. Ainsi, A contient $1/n$ comme voulu.

Revenons au cas général. On a un diagramme commutatif de Γ_K-modules

$$\begin{tikzcd} 1 \arrow[r] & \mu_n \arrow[r] \arrow[d, "(-)^{n/d}"] & \overline{K}^\times \arrow[r, "(-)^n"] \arrow[d, "(-)^{n/d}"] & \overline{K}^\times \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & \mu_d \arrow[r] & \overline{K}^\times \arrow[r, "(-)^d"] & \overline{K}^\times \arrow[r] & 1 \end{tikzcd}$$

dont les deux lignes sont exactes. D'où un diagramme commutatif

$$\begin{tikzcd}
K^\times \arrow[r] \arrow[d, equal] & \mathrm{H}^1(K, \mu_n) \arrow[d] \\
K^\times \arrow[r] & \mathrm{H}^1(K, \mu_d)
\end{tikzcd}$$

D'où l'image a' de $a \in \mathrm{H}^1(K, \mu_n)$ par le morphisme induit par $\mu_n \xrightarrow{(-)^{n/d}} \mu_d$ coïncide avec l'image de $\tilde{a}$ dans $\mathrm{H}^1(K, \mu_d)$ par la théorie de Kummer. Comme $v(\tilde{a})$ est premier à d, par le résultat dans le cas précédent, il existe $b' \in \mathrm{H}^1(K, \mathbb{Z}/d)$ tel que $\mathrm{inv}_K(a' \cup b') = 1/d$. On a un diagramme commutatif

$$\begin{tikzcd}
\mu_n \times \mathbb{Z}/n \arrow[rr] \arrow[d, shift right=3, "(-)^{n/d}"'] & & \overline{K}^\times \\
\mu_d \times \mathbb{Z}/d \arrow[u, hook, shift right=3] \arrow[urr] & &
\end{tikzcd}$$

Notant $b \in \mathrm{H}^1(K, \mathbb{Z}/n)$ l'image de b' par le morphisme induit par $\mathbb{Z}/d \hookrightarrow \mathbb{Z}/n$, on a $a \cup b = a' \cup b'$, d'où A contient $\mathrm{inv}_K(a \cup b) = \mathrm{inv}_K(a' \cup b') = 1/d$. Le lemme est finalement démontré. □

5B. ***Construction du morphisme $\phi : M \otimes M \to Z$.*** Comme on a vu dans le paragraphe 3B, on peut construire une extension

$$0 \to Z \to F \to M \oplus M \to 0$$

à partir d'un morphisme $\phi : M \otimes M \to Z$. Nous allons maintenant choisir M, Z et ϕ. Les notations suivantes seront fixées jusqu'à la fin du texte.

- A est un groupe abélien fini et k est un corps de nombres contenant $\mu_{\exp(A)}$. On munit A de l'action triviale de Γ_k et l'on fixe un générateur de $\mu_{\exp(A)}$ (ce qui définit un isomorphisme $A = \hat{A}$). L/k est une extension finie galoisienne et $\mathfrak{g} = \mathrm{Gal}(L/k)$ (dans la construction originelle de [Borovoi et Kunyavskii 1997], $A = \mathbb{Z}/p^2$ et $\mathfrak{g} = \mathbb{Z}/p \times \mathbb{Z}/p$, où p est un nombre premier).

- Pour toute place v de k, une place w_v de L divisant v est choisie et $\mathfrak{g}_v \subseteq \mathfrak{g}$ est le groupe de décomposition de $w_v|v$. On fixe également un système de représentants $\mathscr{E}_v$ des classes à gauche de $\mathfrak{g}$ suivant $\mathfrak{g}_v$ et l'on pose $e_v = |\mathscr{E}_v| = [\mathfrak{g} : \mathfrak{g}_v]$. Alors pour toute place w de L divisant v, il existe un unique $s \in \mathscr{E}_v$ tel que $w = sw_v$. De plus, si $\sigma \in \Gamma_k$ est un relevé de s, alors $\Gamma_{L_w} = \sigma \Gamma_{L_{w_v}} \sigma^{-1}$. De plus, pour tout Γ_k-module B sur lequel Γ_L agit trivialement et tout $r \geqslant 1$, on dispose d'un isomorphisme

$$\mathrm{Z}^r(L_{w_v}, B) \to \mathrm{Z}^r(L_w, B),$$

qui à chaque r-cocycle $c : \Gamma^r_{L_{w_v}} \to B$ associe le r-cocycle

$$\Gamma^r_{L_w} \to B, \quad (\tau_1, \ldots, \tau_r) \mapsto c(\sigma^{-1}\tau_1\sigma, \ldots, \sigma^{-1}\tau_r\sigma).$$

Cet isomorphisme-là induit un isomorphisme $\mathrm{H}^r(L_{w_v}, B) \to \mathrm{H}^r(L_w, B)$, qui est compatible avec les flèches de restriction de $\mathrm{H}^r(k_v, B)$. On va noter l'image de chaque classe $\gamma \in \mathrm{H}^r(L_{w_v}, B)$ par ${}^s\gamma \in \mathrm{H}^r(L_w, B)$. Si $\gamma \in \mathrm{H}^r(L, B)$, alors ${}^s(\gamma_{w_v}) = ({}^s\gamma)_w \in \mathrm{H}^r(L_w, B)$.

- $M = \mathrm{Ind}_{\Gamma_k}^{\Gamma_L} A$ et $j : A \otimes A \hookrightarrow M \otimes M$ est l'inclusion canonique, cf. lemme 2.5.
- Z est le conoyau de j et $\phi : M \otimes M \to Z$ est la projection. $\Phi : (M \oplus M) \times (M \oplus M) \to Z$ est l'application biadditive définie par (3-1), c'est-à-dire que

$$\Phi((x, y), (x', y')) = \phi(x \otimes y') \quad \forall x, y, x', y' \in M.$$

Soit F le produit croisé $Z \times_\Phi (M \oplus M)$. On verra que $Z = Z(F) = [F, F]$ (proposition 5.4). On munit F d'une action de Γ_k compatible avec celles sur Z et sur $M \otimes M$.

Proposition 5.4. *Avec les notations ci-dessus, on a les résultats suivants* :

1. $Z = Z(F) = [F, F]$.
2. *Soit X un espace homogène de* SL_m *à stabilisateur géométrique F. Alors* $Б(X) = Б_\omega(X) = 0$ *et* $\mathrm{Br}_{\mathrm{nr}}\, X = \mathrm{Br}_{\mathrm{nr},1}\, X$. *Si de plus l'action extérieure de Γ_k sur F est induite par l'action coordonnée par coordonnée, alors* $\mathrm{Br}_{\mathrm{nr}}\, X = \mathrm{Br}_0\, X$.

Démonstration. On rappelle que $M = \{\mathfrak{g} \to A\}$ (le Γ_k-module des applications $\mathfrak{g} \to A$) et que $M \otimes M = \{\mathfrak{g} \times \mathfrak{g} \to A \otimes A\}$.

1. Par le lemme 3.5, $Z = [F, F]$ puisque ϕ est surjectif. Montrons que ϕ est non dégénéré.

Notons d'abord que si $a \in A$ est tel que $a \otimes b = 0$ pour tout $b \in A$, alors $a = 0$. En effet, en choisissant un isomorphisme $A \simeq \mathrm{Hom}(A, \mathbb{Z}/\exp(A))$, on obtient un accouplement parfait $A \otimes A \to \mathbb{Z}/\exp(A)$.

Supposons maintenant que $x : \mathfrak{g} \to A$ est tel que $\phi(x \otimes y) = 0$ pour tout $y : \mathfrak{g} \to A$. Pour tout $a \in A$, soit $y_a : \mathfrak{g} \to A$ défini par $y_a(1) = a$ et $y_a(g) = 0$ pour tout $g \neq 1$. Alors $\phi(x \otimes y_a) = 0$, donc il existe $m_a \in A \otimes A$ tel que $x \otimes y_a = j(m_a)$, c'est-à-dire que

$$x(g) \otimes y_a(h) = m_a \quad \forall g, h \in \mathfrak{g},$$

d'où $x(g) \otimes a = m_a = x(g) \otimes 0 = 0$ pour tous $g \in \mathfrak{g}$ et $a \in A$, donc $x(g) = 0$, ainsi $x = 0$. De même, si $y \in M$ est tel que $\phi(x \otimes y) = 0$ pour tout $x \in M$, on vérifie sans peine que $y = 0$. Ainsi, ϕ est bien non dégénéré et donc $Z = Z(F)$ au vu du lemme 3.6.

2. Calculons $\mathrm{Br}_{\mathrm{nr}}\, \overline{X}$. Au vu de la proposition 4.9, ce groupe est $\mathrm{Hom}((\mathrm{Ker}\,\phi)/H, \mathbb{Q}/\mathbb{Z})$, où H est le sous-groupe $\langle x \otimes y : x, y \in M, \phi(x \otimes y) = 0\rangle$ de $M \otimes M$. Tout élément de $\mathrm{Ker}\,\phi$ est de la forme $j(m)$ pour un $m \in A \otimes A$. Écrivons $m = \sum_{i \in I} a_i \otimes b_i$, où I est fini et $a_i, b_i \in A$. On définit $x_i, y_i : \mathfrak{g} \to A$ par

$$x_i(g) = a_i, \quad y_i(g) = b_i$$

pour tous $g \in \mathfrak{g}$ et $i \in I$. Alors $j(a_i \otimes b_i) = x_i \otimes y_i$, d'où $\phi(x_i \otimes y_i) = 0$. On en déduit que

$$j(m) = \sum_{i \in I} j(a_i \otimes b_i) = \sum_i x_i \otimes y_i \in H,$$

d'où $\operatorname{Ker}\phi = H$, donc $\mathrm{Br}_{\mathrm{nr}}\,\overline{X} = 0$. Il s'ensuit que $\mathrm{Br}_{\mathrm{nr},1}\, X = \mathrm{Br}_{\mathrm{nr}}\, X$ et $\mathrm{Br}_{\mathrm{nr},a}\, X = (\mathrm{Br}_{\mathrm{nr}}\, X)/(\mathrm{Br}_0\, X)$.

Calculons $\text{Б}(X)$ et $\text{Б}_\omega(X)$. Par le lemme de Shapiro, $\text{Ш}^1_\omega(k, \hat{M}) = \text{Ш}^1_\omega(L, \hat{A}) = \text{Ш}^1_\omega(L, A)$. Or $\text{Ш}^1_\omega(L, A) = 0$ par une application du théorème de Chebotarev (cf. [Harari 2017, corollaire 18.4]), donc $\text{Ш}^1_\omega(k, \hat{M}) = 0$. Par la proposition 4.1, on a $\text{Б}_\omega(X) = 0$ et a fortiori $\text{Б}(X) = 0$.

Finalement, si l'action extérieure de Γ_k sur F est induite par l'action coordonnée par coordonnée, alors $\mathrm{Br}_{\mathrm{nr},a}\, X = \text{Б}_\omega(X) = 0$ par la proposition 4.6, d'où $\mathrm{Br}_{\mathrm{nr}}\, X = \mathrm{Br}_{\mathrm{nr},1}\, X = \mathrm{Br}_0\, X$. □

Pour les principaux théorèmes, on considère seulement l'action coordonnée par coordonnée de Γ_k sur F. On suppose ceci pour le reste du texte.

5C. ***Principe de Hasse.*** Le théorème suivant sera le cœur des preuves de nos principaux résultats. Son deuxième point sera utile pour l'étude de l'approximation faible. Les lecteurs souhaitant s'habituer à l'idée de sa preuve sont conseillés de se restreindre au cas où $A = \mathbb{Z}/n$.

Théorème 5.5. *Soient A un groupe abélien fini, k un corps de nombres contenant $\mu_{\exp(A)}$, L/k une extension finie galoisienne, $M = \operatorname{Ind}_{\Gamma_k}^{\Gamma_L} A$, $j : A \otimes A \hookrightarrow M \otimes M$ l'inclusion canonique, Z le conoyau de j et $\phi : M \otimes M \to Z$ la projection. De ϕ on définit une application biadditive $\Phi : (M \oplus M) \times (M \oplus M) \to Z$ par* (3-1) *et l'on pose $F = Z \times_\Phi (M \oplus M)$, muni de l'action coordonnée par coordonnée de Γ_k. Soit $u \in \mathrm{H}^2(k, M \otimes M)$. Alors, étant donné* :

— *un sous-ensemble fini $S \subseteq \Omega_k$ tel que $u_v = 0$ pour tout $v \notin S$* ;

— *pour tout $v \in S$, des éléments $x'_v, y'_v \in \mathrm{H}^1(k_v, M)$ et $\lambda'_v \in \mathrm{H}^2(k_v, A \otimes A)$ tels que $x'_v \cup y'_v = u_v + j_*\lambda'_v$ dans $\mathrm{H}^2(k_v, M \otimes M)$* ;

il existe $x, y \in \mathrm{H}^1(k, M)$ et $\lambda \in \mathrm{H}^2(k, A \otimes A)$ tels que les conditions suivantes soient satisfaites :

1. *$x \cup y = u + j_*\lambda$ dans $\mathrm{H}^2(k, M \otimes M)$.*

2. *$x_v = x'_v$, $y_v = y'_v$ et $\lambda_v = \lambda'_v$ pour tout $v \in S$.*

Démonstration. Gardons les notations au début du paragraphe 5B. Par le lemme 2.3, on dispose d'un isomorphisme $\mathrm{sh}' : \mathrm{H}^2(k, M \otimes M) \to \mathrm{H}^2(L, A \otimes A)^{|\mathfrak{g}|}$; écrivons

$$\mathrm{sh}'(u) = (\gamma_g)_{g \in \mathfrak{g}} \in \mathrm{H}^2(L, A \otimes A)^{|\mathfrak{g}|}.$$

Par le lemme 2.10, on a

$$\forall v \notin S,\ \forall h \in \mathfrak{g}_v,\ \forall s, t \in \mathscr{E}_v,\ ({}^{t^{-1}}\gamma_{sht^{-1}})_{w_v} = 0 \quad \text{dans } \mathrm{H}^2(L_{w_v}, A \otimes A),$$

ou $(\gamma_{sht^{-1}})_{tw_v} = 0$ dans $\mathrm{H}^2(L_{tw_v}, A \otimes A)$. Pour tous $g \in \mathfrak{g}$ et $w | v$, on peut écrire $w = tw_v$ pour un $t \in \mathscr{E}_v$, puis $gt = sh$ pour un $s \in \mathscr{E}_v$ et un $h \in \mathfrak{g}_v$. On a ainsi

$$\forall v \notin S,\ \forall g \in \mathfrak{g},\ \forall w | v,\ (\gamma_g)_w = 0 \quad \text{dans } \mathrm{H}^2(L_w, A \otimes A). \tag{5-5}$$

On procède en plusieurs étapes.

Étape 1. *Approchons les* λ'_v. Écrivons $A = \prod_{p\in J} \mathbb{Z}/n_p = \prod_{p\in J} \mu_{n_p}$, et $d_{p,q} = \mathrm{PGCD}(n_p, n_q)$ pour tous $p, q \in J$. Par le théorème de Chebotarev, il existe $|J|^2$ places (deux à deux distinctes) $v_{p,q} \notin S$ de k $(p, q \in J)$ qui sont finies et totalement décomposées dans L (donc $\mathscr{E}_{v_{p,q}} = \mathfrak{g}$). Pour tout $v \in S$, écrivons

$$\lambda'_v = ({\lambda'_v}^{p,q})_{p,q\in J} \in \mathrm{H}^2(k_v, A \otimes A) = \prod_{p,q\in J} (\mathrm{Br}\, k_v)[d_{p,q}].$$

Pour tous $p, q \in J$, par la loi de réciprocité globale, il existe $\lambda^{p,q} \in (\mathrm{Br}\, k)[d_{p,q}]$ tel que :

1. $\lambda^{p,q}_v = {\lambda'_v}^{p,q}$ pour tout $v \in S$.
2. $\mathrm{inv}_{v_{p,q}}(\lambda^{p,q}_{v_{p,q}}) = -\sum_{v\in S} \mathrm{inv}_v({\lambda'_v}^{p,q})$.
3. $\lambda^{p,q}_v = 0$ pour tout $v \notin S \cup \{v_{p,q}\}$.

Posons $\lambda = (\lambda^{p,q})_{p,q\in J} \in \prod_{p,q\in J} (\mathrm{Br}\, k)[d_{p,q}] = \mathrm{H}^2(k, A \otimes A)$. Alors $\lambda_v = \lambda'_v$ pour tout $v \in S$ et $\lambda_v = 0$ pour tout $v \notin S \cup \{v_{p,q} : p, q \in J\}$. En particulier, on a

$$\forall v \in S,\ x'_v \cup y'_v = u_v + j_*\lambda_v \quad \text{dans } \mathrm{H}^2(k_v, M \otimes M). \tag{5-6}$$

Étape 2. *Approchons les* x'_v. Pour tout $v \in S$, on dispose (par le lemme 2.6) d'un isomorphisme

$$\mathrm{sh}_v : \mathrm{H}^1(k_v, M) \xrightarrow{\simeq} \mathrm{H}^1(L_{w_v}, A)^{e_v}.$$

Écrivons $\mathrm{sh}_v(x'_v) = (a'_{v,s})_{s\in\mathscr{E}_v} \in \mathrm{H}^1(L_{w_v}, A)^{e_v}$ et $\mathrm{sh}_v(y'_v) = (b'_{v,s})_{s\in\mathscr{E}_v} \in \mathrm{H}^1(L_{w_v}, A)^{e_v}$.

Pour tous $p, q \in J$, on choisit une uniformisante $\varpi_{p,q} \in k^\times$ de $k_{v_{p,q}}$. Pour tout $p \in J$, le théorème des restes chinois donne un élément $\tilde{a}^p \in L^\times$ tel que :

1. $\tilde{a}^p_w = \varpi_{p,q} \pmod{L_w^{\times n_p}}$ pour toute place w de L divisant une place $v_{p,q}$, où $q \in J$.
2. $\tilde{a}^p_w \in L_w^{\times n_p}$ pour toute place w de L divisant une place $v_{p',q}$, où $p' \in J \setminus \{p\}$ et $q \in J$.

On note $a'^p \in \mathrm{H}^1(L, \mu_{n_p}) = \mathrm{H}^1(L, \mathbb{Z}/n_p)$ l'image de $\tilde{a}^p$ par la théorie de Kummer. Comme $Ш^1_\omega(L, A) = 0$ par le théorème de Chebotarev, le Γ_L-module A vérifie l'approximation faible au sens du lemme 1.1 (cf. [Harari 2017, exercice 17.5 et corollaire 18.4]), donc il existe un $a \in \mathrm{H}^1(L, A)$ tel que :

1. $a_{sw_v} = {}^s a'_{v,s} \in \mathrm{H}^1(L_{sw_v}, A)$ pour tous $v \in S$ et $s \in \mathscr{E}_v$.
2. $a_w = ({a'}^p_w)_{p\in J} \in \prod_{p\in J} \mathrm{H}^1(L_w, \mathbb{Z}/n_p) = \mathrm{H}^1(L_w, A)$ pour toute place w de L divisant une place $v_{p,q}$, où $p, q \in J$.

Soit $x = \mathrm{sh}^{-1}(a) \in \mathrm{H}^1(k, M)$. Pour tous $v \in S$ et $s \in \mathscr{E}_v$, on a $a_{sw_v} = {}^s a'_{v,s} \in \mathrm{H}^1(L_{sw_v}, A)$, d'où $({}^{s^{-1}}a)_{w_v} = a'_{s,v} \in \mathrm{H}^1(L_{w_v}, A)$. Par le lemme 2.9, on a $x_v = x'_v$ pour tout $v \in S$. Ainsi (5-6) devient

$$\forall v \in S,\ x_v \cup y'_v = u_v + j_*\lambda_v \quad \text{dans } \mathrm{H}^2(k_v, M \otimes M).$$

Au vu des lemmes 2.7, 2.8, 2.9 et 2.10, on a

$$\forall v \in S,\ \forall h \in \mathfrak{g}_v,\ \forall s, t \in \mathscr{E}_v,\ {}^{h^{-1}s^{-1}}a_{w_v} \cup b'_{v,t} = ({}^{t^{-1}}\gamma_{sht^{-1}})_{w_v} + \mathrm{res}(\lambda)_{w_v} \quad \text{dans } \mathrm{H}^2(L_{w_v}, A \otimes A),$$

ou ${}^{th^{-1}s^{-1}}a_{tw_v} \cup {}^{t}b'_{v,t} = (\gamma_{sht^{-1}})_{tw_v} + \mathrm{res}(\lambda)_{tw_v}$ dans $\mathrm{H}^2(L_{tw_v}, A \otimes A)$. Pour tous $g \in \mathfrak{g}$ et $t \in \mathscr{E}_v$, on peut écrire $gt = sh$ pour un $s \in \mathscr{E}_v$ et un $h \in \mathfrak{g}_v$. On a ainsi

$$\forall v \in S,\ \forall g \in \mathfrak{g},\ \forall t \in \mathscr{E}_v,\ {}^{g^{-1}}a_{tw_v} \cup {}^{t}b'_{v,t} = (\gamma_g)_{tw_v} + \mathrm{res}(\lambda)_{tw_v} \quad \text{dans } \mathrm{H}^2(L_{tw_v}, A \otimes A). \tag{5-7}$$

Étape 3. *Vérifions l'hypothèse du lemme arithmétique.* On va appliquer la proposition 5.2 :

— au corps de nombres L ;

— à la famille $({}^{g^{-1}}a)_{g\in\mathfrak{g}} \in \mathrm{H}^1(L, A)$;

— à la famille $(\gamma_g + \mathrm{res}(\lambda))_{g\in\mathfrak{g}} \in \mathrm{H}^2(L, A \otimes A)^{|\mathfrak{g}|}$;

— et à l'ensemble $\{w \in \Omega_L : \exists v \in S \cup \{v_{p,q} : p, q \in J\},\ w|v\}$.

Soit w une place de L et montrons qu'il existe $c_w \in \mathrm{H}^1(L_w, A)$ tel que

$$\forall g \in \mathfrak{g},\ {}^{g^{-1}}a_w \cup c_w = (\gamma_g)_w + \mathrm{res}(\lambda)_w \quad \text{dans } \mathrm{H}^2(L_w, A \otimes A).$$

Notons v la place de k au-dessous de w. On distingue trois cas.

— Si $v \in S$: au vu de (5-7), il suffit de prendre $c_w = {}^{t}b'_{v,t}$, où $t \in \mathscr{E}_v$ est tel que $w = tw_v$.

— Si $v = v_{p',q'}$, où $p', q' \in J$: rappelons que v est totalement décomposée dans L et que $\varpi := \varpi_{p',q'} \in k^\times$ est une uniformisante de k_v. D'une part, $\tilde{a}_w^{p'} = \varpi \pmod{L_w^{\times n_{p'}}}$, donc l'image $a_w^{p'} \in \mathrm{H}^1(L_w, \mu_{n_{p'}})$ de $\tilde{a}_w^{p'}$ (par la théorie de Kummer) est $\mathfrak{g}$-équivariante. Or $\tilde{a}_w^{p} \in L_w^{\times n_p}$ pour tout $p \in J \setminus \{p'\}$, donc l'image de $\tilde{a}_w^{p}$ dans $\mathrm{H}^1(L_w, \mu_{n_p})$ (par la théorie de Kummer) est $a_w^p = 0$. En particulier, $a_w = (a_w^p)_{p\in J} \in \mathrm{H}^1(L_w, A)$ est $\mathfrak{g}$-équivariant. D'autre part, $(\gamma_g)_w = 0$ pour tout $g \in \mathfrak{g}$ puisque $u_v = 0$. Ainsi, il faut chercher $c_w = (c_w^q)_{q\in J} \in \prod_{q\in J} \mathrm{H}^1(L_w, \mu_{n_q})$ tel que

$$a_w \cup c_w = \mathrm{res}(\lambda)_w \quad \text{dans } \mathrm{H}^2(L_w, A \otimes A),$$

c'est-à-dire

$$\forall p, q \in J,\ a_w^p \cup c_w^q = \mathrm{res}(\lambda^{p,q})_w \quad \text{dans } (\mathrm{Br}\, L_w)[d_{p,q}]. \tag{5-8}$$

On choisit $c_w^q = 0$ pour tout $q \in J \setminus \{q'\}$. Pour le $c_w^{q'}$, on note $\alpha \in \mathrm{H}^1(L_w, \mu_{n_{q'}}) = \mathrm{H}^1(L_w, \mathbb{Z}/n_{q'})$ l'image de $\tilde{a}_w^{p'}$ par la théorie de Kummer, et l'on choisit $r \in (\mathrm{Br}\, L_w)[n_{q'}]$ tel que $(n_{q'}/d_{p',q'})r = \mathrm{res}(\lambda^{p',q'})_w$. Comme $w(\tilde{a}^{p'}) = v(\tilde{a}^{p'}) = 1$, le lemme 5.3 assure qu'il existe $c_w^{q'} \in \mathrm{H}^1(L_w, \mathbb{Z}/n_{q'}) = \mathrm{H}^1(L_w, \mu_{n_{q'}})$ tel que $\alpha \cup c_w^{q'} = r$, d'où $(n_{q'}/d_{p',q'})\alpha \cup c_w^{q'} = \mathrm{res}(\lambda^{p',q'})_w$. Au vu de (5-3), on a $(\iota_{n_{q'}}^{n_{p'}})_* a_w^{p'} = (n'_q/d_{p',q'})\alpha \in \mathrm{H}^1(L_w, \mathbb{Z}/n_{q'})$, d'où $a_w^{p'} \cup c_w^{q'} = \mathrm{res}(\lambda^{p',q'})_w$ en vertu de (5-2).

On prend finalement $c_w = (c_w^q)_{q\in J}$. On a déjà vu que cet élément vérifie (5-8) pour $(p, q) = (p', q')$. Or, pour tout $(p, q) \in (J \times J) \setminus \{(p', q')\}$, on a soit $a_w^p = 0$ (si $p \neq p'$) ou $c_w^q = 0$ (si $q \neq q'$), et de plus $\lambda_v^{p,q} = 0$ par notre choix de $\lambda^{p,q}$, d'où $\mathrm{res}(\lambda^{p,q})_w = 0 = a_w^p \cup c_w^q$, ce qui établit (5-8) pour tous $p, q \in J$.

— Si $v \notin S \cup \{v_{p,q} : p, q \in J\}$. Dans ce cas, on a $u_v = 0$ et $\lambda_v = 0$, d'où $(\gamma_g)_w = \mathrm{res}(\lambda)_w = 0$ pour tous $g \in \mathfrak{g}$, donc il suffit de prendre $c_w = 0$.

L'hypothèse de la proposition 5.2 est alors vérifiée.

Étape 4. *Utilisons le lemme arithmétique pour approcher les y'_v.* La proposition 5.2 nous permet de fabriquer un élément $b \in \mathrm{H}^1(L, A)$ satisfaisant les conditions suivantes.

1. ${}^{g^{-1}}a \cup b = \gamma_g + \mathrm{res}(\lambda)$ dans $\mathrm{H}^2(L, A \otimes A)$ pour tout $g \in \mathfrak{g}$.
2. $b_{tw_v} = {}^t b'_{v,t}$ dans $\mathrm{H}^1(L_{tw_v}, A)$ pour tous $v \in S$ et $t \in \mathscr{E}_v$.

On note $y = \mathrm{sh}^{-1}(b) \in \mathrm{H}^1(k, M)$. Regardons les deux conditions ci-dessus.

1. Pour la première condition, par les lemmes 2.4 et 2.5, on a $x \cup y = u + j_*\lambda$ dans $\mathrm{H}^2(k, M \otimes M)$.
2. Soit $v \in S$. Pour tout $t \in \mathscr{E}_v$, la deuxième condition implique que ${}^{t^{-1}}b_{w_v} = b'_{t,v}$ dans $\mathrm{H}^1(L_{w_v}, A)$. En vertu du lemme 2.9, on a $y_v = y'_v$. Rappelons qu'on a déjà $x_v = x'_v$ et $\lambda_v = \lambda'_v$ pour tout $v \in S$.

Le théorème est finalement démontré. □

Nous sommes maintenant en mesure d'établir le théorème A.

Théorème 5.6. *Soient A un groupe abélien fini, k un corps de nombres contenant $\mu_{\exp(A)}$, L/k une extension finie galoisienne, $M = \mathrm{Ind}_{\Gamma_k}^{\Gamma_L} A$, $j : A \otimes A \hookrightarrow M \otimes M$ l'inclusion canonique, Z le conoyau de j et $\phi : M \otimes M \to Z$ la projection. De ϕ on définit une application biadditive $\Phi : (M \oplus M) \times (M \oplus M) \to Z$ par* (3-1) *et l'on pose $F = Z \times_\Phi (M \oplus M)$. On munit F de l'action coordonnée par coordonnée de Γ_k. Si X est un espace homogène de* SL_m *de lien de Springer* lien(F) *tel que $X(k_v) \neq \varnothing$ pour toute place v de k, alors $X(k) \neq \varnothing$.*

Démonstration. Notons $\Delta : \mathrm{H}^2(k, M \oplus M) \to \mathrm{H}^2(k, Z)$ l'application connectante induite par l'extension centrale $0 \to Z \to F \to M \oplus M \to 0$. Rappelons que $Z = Z(F) = [F, F]$ par la proposition 5.4. Soit $\eta_0 \in \mathrm{H}^2(k, F)$ la classe neutre privilégiée. Alors il existe une unique classe $\beta \in \mathrm{H}^2(k, Z)$ telle que la classe de Springer de X vaut $\eta_X = \beta \cdot \eta_0$ (cf. paragraphe 3A). Soit v une place de Ω_k. Si $X(k_v) \neq \varnothing$, par la proposition 3.3 et le lemme 3.8, il existera $(x'_v, y'_v) \in \mathrm{H}^1(k_v, M \oplus M)$ tel que $\beta_v = \Delta(x'_v, y'_v) = \phi_*(x'_v \cup y'_v)$ dans $\mathrm{H}^2(k_v, Z)$, donc l'image de β_v dans $\mathrm{H}^3(k_v, A \otimes A)$ sera nulle. Ainsi, lorsque $X(k_v) \neq \varnothing$ pour tout v, l'image de β dans $\mathrm{H}^3(k, A \otimes A)$ sera nulle partout localement. Or $Ш^3(k, A \otimes A) = 0$ (c'est une conséquence d'une version simple de la dualité de Poitou–Tate, cf. [Harari 2017, théorème 17.13]), donc β s'enverra sur $0 \in \mathrm{H}^3(k, A \otimes A)$, d'où il existera $u \in \mathrm{H}^2(k, M \otimes M)$ tel que $\beta = \phi_*(u)$.

Soit $S \subseteq \Omega_k$ l'ensemble des places v telles que $u_v \neq 0$. Pour tout $v \in S$, comme $\phi_*(x'_v \cup y'_v) = \beta_v = \phi_*(u_v)$ dans $\mathrm{H}^2(k_v, Z)$, il existe $\lambda'_v \in \mathrm{H}^2(k_v, A \otimes A)$ tel que $x'_v \cup y'_v = u_v + j_*\lambda'_v$ dans $\mathrm{H}^2(k_v, M \otimes M)$. Par le théorème 5.5, on peut trouver $x, y \in \mathrm{H}^1(k, M)$ et $\lambda \in \mathrm{H}^2(k, A \otimes A)$ tels que $x \cup y = u + j_*\lambda$ dans $\mathrm{H}^2(k, M \otimes M)$. En particulier, $\beta = \phi_*(u) = \phi_*(x \cup y) = \Delta(x, y)$ par le lemme 3.8. Au vu de la proposition 3.3, on peut conclure que $X(k) \neq \varnothing$. □

5D. ***Approximation faible.*** Gardons les notations au début du paragraphe 5B. On a une suite exacte

$$0 \to A \otimes A \xrightarrow{j} M \otimes M \xrightarrow{\phi} Z \to 0 \tag{5-9}$$

de Γ_k-modules. En dualisant, on obtient une suite exacte

$$0 \to \hat{Z} \xrightarrow{\hat{\phi}} \widehat{M \otimes M} \xrightarrow{\hat{j}} \widehat{A \otimes A} \to 0. \tag{5-10}$$

Notons que Γ_k agit trivialement sur $A \otimes A$ et sur $\widehat{A \otimes A}$.

Lemme 5.7. *Le sous-groupe* $Ш^1_\omega(k, \hat{Z}) \subseteq \mathrm{H}^1(k, \hat{Z})$ *est inclus dans l'image du morphisme connectant* $\hat{\delta} : \widehat{A \otimes A} \to \mathrm{H}^1(k, \hat{Z})$ *induit par* (5-10).

Démonstration. Comme (5-10) est déployé par L, on peut identifier $\mathrm{H}^1(\mathfrak{g}, \hat{Z})$ à un sous-groupe de $\mathrm{H}^1(k, \hat{Z})$ (par la suite exacte d'inflation-restriction). Une application du théorème de Chebotarev donne $Ш^1_\omega(L, \hat{Z}) = 0$ (voir [Harari 2017, corollaire 18.4]), donc on a $Ш^1_\omega(k, \hat{Z}) = Ш^1_\omega(\mathfrak{g}, \hat{Z}) \subseteq \mathrm{H}^1(\mathfrak{g}, \hat{Z})$. Maintenant, $M \otimes M$ est un $\mathfrak{g}$-module induit par le lemme 2.3, donc il en va de même pour $\widehat{M \otimes M}$. Par le lemme de Shapiro, $\mathrm{H}^1(\mathfrak{g}, \widehat{M \otimes M}) = 0$ et donc le morphisme connectant $\widehat{A \otimes A} \to \mathrm{H}^1(\mathfrak{g}, \hat{Z})$ est surjectif. D'où le lemme. □

On démontre maintenant le théorème B.

Théorème 5.8. *Soient A un groupe abélien fini, k un corps de nombres contenant $\mu_{\exp(A)}$, L/k une extension finie galoisienne, $M = \mathrm{Ind}_{\Gamma_k}^{\Gamma_L} A$, $j : A \otimes A \hookrightarrow M \otimes M$ l'inclusion canonique, Z le conoyau de j et $\phi : M \otimes M \to Z$ la projection. De ϕ on définit une application biadditive $\Phi : (M \oplus M) \times (M \oplus M) \to Z$ par* (3-1) *et l'on pose $F = Z \times_\Phi (M \oplus M)$. On munit F de l'action coordonnée par coordonnée de Γ_k. Si X est un espace homogène de* SL_m *de lien de Springer* $\mathrm{lien}(F)$ *tel que $X(k) \neq \varnothing$, alors X vérifie l'approximation faible.*

Démonstration. Par la proposition 3.3, $X \simeq {}_{\mathfrak{a}}F \setminus \mathrm{SL}_m$ pour un certain 1-cocycle $\mathfrak{a} = (\mathfrak{x}, \mathfrak{y}) : \Gamma_k \to M \oplus M$. Par le lemme 1.1, on s'est ramené à la question d'approximation faible pour ${}_{\mathfrak{a}}F$, i.e., il faut démontrer que pour tout sous-ensemble fini $S \subseteq \Omega_k$, la restriction

$$\mathrm{H}^1(k, {}_{\mathfrak{a}}F) \to \prod_{v \in S} \mathrm{H}^1(k_v, {}_{\mathfrak{a}}F)$$

est surjective. Soit alors $f'_v = (z'_v, a'_v) : \Gamma_{k_v} \to {}_{\mathfrak{a}}F$ une famille de 1-cocycles, $v \in S$, où $a'_v = (x'_v, y'_v)$. Pour tout $v \in S$, par le lemme 3.8, a'_v est un cocycle et de plus

$$\mathrm{d}z'_v + \phi_*(\mathfrak{x}_v \cup y'_v + x'_v \cup \mathfrak{y}_v + x'_v \cup y'_v + \mathrm{d}(x'_v \otimes \mathfrak{y}_v)) = 0 \quad \text{dans } \mathrm{Z}^2(k_v, Z).$$

Écrivons $z'_v = \phi_* \varepsilon'_v$ pour une 1-cochaîne $\varepsilon'_v : \Gamma_{k_v} \to M \otimes M$. Il existe alors un 2-cocycle $\lambda'_v : \Gamma_{k_v} \times \Gamma_{k_v} \to A \otimes A$ tel que

$$\mathrm{d}\varepsilon'_v + \mathfrak{x}_v \cup y'_v + x'_v \cup \mathfrak{y}_v + x'_v \cup y'_v + \mathrm{d}(x'_v \otimes \mathfrak{y}_v) = j_* \lambda'_v \quad \text{dans } \mathrm{Z}^2(k_v, M \otimes M). \tag{5-11}$$

Considérons l'élément $u = [\mathfrak{x} \cup \mathfrak{y}] \in \mathrm{H}^2(k, M \otimes M)$. Quitte à agrandir S, on peut supposer que $u_v = 0$ pour tout $v \notin S$. De (5-11), on a

$$\forall v \in S,\ [(x'_v + \mathfrak{x}_v) \cup (y'_v + \mathfrak{y}_v)] = [\mathfrak{x}_v \cup \mathfrak{y}_v] + j_*[\lambda'_v] \quad \text{dans } \mathrm{H}^2(k_v, M \otimes M).$$

Par le théorème 5.5, il existe des 1-cocycles $\tilde{x}, \tilde{y} : \Gamma_k \to M$ et un 2-cocycle $\lambda : \Gamma_k \times \Gamma_k \to A \otimes A$ tels que les conditions suivantes soient remplies :

1. $[\tilde{x} \cup \tilde{y}] = [\mathfrak{x} \cup \mathfrak{y}] + j_*[\lambda]$ dans $\mathrm{H}^2(k, M \otimes M)$.
2. Pour tout $v \in S$, $[\tilde{x}_v] = [x'_v + \mathfrak{x}_v]$, $[\tilde{y}_v] = [y'_v + \mathfrak{y}_v]$ et $[\lambda_v] = [\lambda'_v]$.

Soient $x = \tilde{x} - \mathfrak{x}$, $y = \tilde{y} - \mathfrak{y}$ et $a = (x, y)$. Alors $[x_v] = [x'_v]$ et $[y_v] = [y'_v]$ pour tout $v \in S$. De $[\tilde{x} \cup \tilde{y}] = [\mathfrak{x} \cup \mathfrak{y}] + j_*[\lambda]$, on voit qu'il existe une 1-cochaîne $\varepsilon : \Gamma_k \to M \otimes M$ telle que

$$\mathrm{d}\varepsilon + \mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y}) = j_*\lambda. \tag{5-12}$$

Posons $z := \phi_*\varepsilon$, alors (5-12) implique que $\mathrm{d}z + \phi_*(\mathfrak{x} \cup y + x \cup \mathfrak{y} + x \cup y + \mathrm{d}(x \otimes \mathfrak{y})) = 0$ et donc $(z, a) : \Gamma_k \to F$ est un cocycle par le lemme 3.8.

Soit $v \in S$. Puisque $[x'_v] = [x_v]$ et $[y'_v] = [y_v]$ dans $\mathrm{H}^1(k, M)$, on peut écrire $x'_v = x_v + \mathrm{d}\xi_v$ et $y'_v = y_v + \mathrm{d}\eta_v$, où $\xi_v, \eta_v \in M$. On considère le 1-cocycle

$$c_v := z'_v - z_v + \phi_*(-(x_v + \mathfrak{x}_v) \cup \eta_v + \xi_v \cup (y'_v + \mathfrak{y}_v) + \mathrm{d}\xi_v \otimes \mathfrak{y}_v) : \Gamma_{k_v} \to Z$$

comme dans l'énoncé du lemme 3.9. Au vu de (5-11) et (5-12), le troisième point de ce lemme-là donne $\delta([c_v]) = [\lambda'_v - \lambda_v] = 0$, où $\delta : \mathrm{H}^1(k_v, Z) \to \mathrm{H}^2(k_v, A \otimes A)$ désigne le morphisme connectant induit par (5-9). Or, en vertu du lemme 5.7 tout élément de $\text{Ш}^1_S(k, \hat{Z})$ appartient à l'image du morphisme connectant $\hat{\delta} : \widehat{A \otimes A} \to \mathrm{H}^1(k, \hat{Z})$ induit par (5-10). Puisque les cup-produits sont compatibles avec les morphismes connectants, on voit que la famille $([c_v])_{v \in S}$ est orthogonale à $\text{Ш}^1_S(k, \hat{Z})$ par rapport à l'accouplement

$$\prod_{v \in S} \mathrm{H}^1(k_v, Z) \times \mathrm{H}^1(k, \hat{Z}) \to \mathbb{Q}/\mathbb{Z},$$

obtenu en rassemblant les dualités locales de Tate. Par [Harari 2017, exercice 17.5], il existe un 1-cocycle $\tilde{z} : \Gamma_k \to Z$ tel que $[\tilde{z}_v] = [c_v]$ dans $\mathrm{H}^1(k_v, Z)$ pour tout $v \in S$. On pose finalement

$$f := (\tilde{z}, 0)(z, a) = (z + \tilde{z}, a) : \Gamma_k \to {}_{\mathfrak{a}}F,$$

qui est un 1-cocycle puisque (z, a) et $(\tilde{z}, 0)$ le sont (notons que Z est central dans ${}_{\mathfrak{a}}F$). Soit $v \in S$, il reste à montrer que $[f_v] = [f'_v]$ dans $\mathrm{H}^1(k_v, {}_{\mathfrak{a}}F)$. En effet, la 1-cochaîne

$$z'_v - (z_v + \tilde{z}_v) + \phi_*(-(x_v + \mathfrak{x}_v) \cup \eta_v + \xi_v \cup (y'_v + \mathfrak{y}_v) + \mathrm{d}\xi_v \otimes \mathfrak{y}_v) = c_v - \tilde{z}_v : \Gamma_{k_v} \to Z$$

est un cobord, donc f_v est cohomologue à f'_v par le lemme 3.9. On a donc trouvé une classe $[f] \in \mathrm{H}^1(k, {}_{\mathfrak{a}}F)$ qui se restreint à $([f'_v])_{v \in S} \in \prod_{v \in S} \mathrm{H}^1(k_v, {}_{\mathfrak{a}}F)$. Ainsi ${}_{\mathfrak{a}}F$ vérifie bien l'approximation faible, ce qui achève la démonstration du théorème. □

Remerciements

Ce travail est financé par un « Contrat doctoral spécifique normalien » de l'École normale supérieure de Paris. L'auteur est reconnaissant à David Harari pour ses commentaires précieux ainsi que pour son soutien. Il remercie Alexeï Skorobogatov, Jean-Louis Colliot-Thélène et Mikhaïl Borovoi pour les discussions pertinentes, ainsi que les rapporteurs pour avoir lu attentivement le texte et pour leurs remarques.

Bibliographie

[Bogomolov 1987] F. A. Bogomolov, "The Brauer group of quotient spaces by linear group actions", *Izv. Akad. Nauk SSSR Ser. Mat.* **51**:3 (1987), 485–516. En russe ; traduit en anglais à *Math. USSR Izv.* **30**:3 (1988), 455–485. Zbl

[Borovoi 1993] M. V. Borovoi, “Abelianization of the second nonabelian Galois cohomology”, *Duke Math. J.* **72**:1 (1993), 217–239. MR Zbl

[Borovoi 1996] M. Borovoi, “The Brauer–Manin obstructions for homogeneous spaces with connected or abelian stabilizer”, *J. Reine Angew. Math.* **473** (1996), 181–194. MR Zbl

[Borovoi et Kunyavskii 1997] M. Borovoi et B. Kunyavskii, “On the Hasse principle for homogeneous spaces with finite stabilizers”, *Ann. Fac. Sci. Toulouse Math.* (6) **6**:3 (1997), 481–497. Correction à la référence suivante. MR Zbl

[Borovoi et Kunyavskii 2001] M. Borovoi et B. Kunyavskii, “Erratum: On the Hasse principle for homogeneous spaces with finite stabilizers”, *Ann. Fac. Sci. Toulouse Math.* (6) **10**:4 (2001), 779. MR

[Colliot-Thélène et Skorobogatov 2021] J.-L. Colliot-Thélène et A. N. Skorobogatov, *The Brauer–Grothendieck group*, Ergebnisse der Math. (3) **71**, Springer, 2021. MR Zbl

[Demarche 2010] C. Demarche, “Groupe de Brauer non ramifié d’espaces homogènes à stabilisateurs finis”, *Math. Ann.* **346**:4 (2010), 949–968. MR Zbl

[Demarche et Lucchini Arteche 2019] C. Demarche et G. Lucchini Arteche, “Le principe de Hasse pour les espaces homogènes: réduction au cas des stabilisateurs finis”, *Compos. Math.* **155**:8 (2019), 1568–1593. MR Zbl

[Flicker et al. 1998] Y. Z. Flicker, C. Scheiderer et R. Sujatha, “Grothendieck’s theorem on non-abelian H^2 and local-global principles”, *J. Amer. Math. Soc.* **11**:3 (1998), 731–750. MR Zbl

[Harari 2007] D. Harari, “Quelques propriétés d’approximation reliées à la cohomologie galoisienne d’un groupe algébrique fini”, *Bull. Soc. Math. France* **135**:4 (2007), 549–564. MR Zbl

[Harari 2017] D. Harari, *Cohomologie galoisienne et théorie du corps de classes*, EDP Sciences, Les Ulis, 2017. MR Zbl

[Harari et Skorobogatov 2002] D. Harari et A. N. Skorobogatov, “Non-abelian cohomology and rational points”, *Compositio Math.* **130**:3 (2002), 241–273. MR Zbl

[Harpaz et Wittenberg 2020] Y. Harpaz et O. Wittenberg, “Zéro-cycles sur les espaces homogènes et problème de Galois inverse”, *J. Amer. Math. Soc.* **33**:3 (2020), 775–805. MR Zbl

[Manin 1971] Y. I. Manin, “Le groupe de Brauer–Grothendieck en géométrie diophantienne”, pp. 401–411 dans *Actes du Congrès International des Mathématiciens* (Nice, 1970), tome 1, édité par M. Berger et al., Gauthier-Villars, Paris, 1971. MR Zbl

[Moravec 2012] P. Moravec, “Unramified Brauer groups of finite and infinite groups”, *Amer. J. Math.* **134**:6 (2012), 1679–1704. MR Zbl

[Naidu 2007] D. Naidu, “Categorical Morita equivalence for group-theoretical categories”, *Comm. Algebra* **35**:11 (2007), 3544–3565. MR Zbl

[Serre 1962] J.-P. Serre, *Corps locaux*, Publ. Inst. Math. Univ. Nancago **8**, Hermann, Paris, 1962. MR Zbl

[Serre 1970] J.-P. Serre, *Cours d’arithmétique*, Collection SUP: Le Mathématicien **2**, Presses Universitaires de France, Paris, 1970. MR Zbl

[Serre 1994] J.-P. Serre, *Cohomologie galoisienne*, 5^{e} éd., Lecture Notes in Mathematics **5**, Springer, 1994. MR Zbl

[Skorobogatov 2001] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics **144**, Cambridge University Press, 2001. MR Zbl

Communicated by Bjorn Poonen
Received 2022-07-15 Revised 2022-12-22 Accepted 2023-02-13

manh-linh.nguyen@universite-paris-saclay.fr
Laboratoire de mathématiques d’Orsay, Université Paris-Saclay, Orsay, France

ALGEBRA AND NUMBER THEORY 18:2 (2024)
https://doi.org/10.2140/ant.2024.18.389

Partial sums of typical multiplicative functions over short moving intervals

Mayank Pandey, Victor Y. Wang and Max Wenqiang Xu

We prove that the k-th positive integer moment of partial sums of Steinhaus random multiplicative functions over the interval $(x, x+H]$ matches the corresponding Gaussian moment, as long as $H \ll x/(\log x)^{2k^2+2+o(1)}$ and H tends to infinity with x. We show that properly normalized partial sums of typical multiplicative functions arising from realizations of random multiplicative functions have Gaussian limiting distribution in short moving intervals $(x, x+H]$ with $H \ll X/(\log X)^{W(X)}$ tending to infinity with X, where x is uniformly chosen from $\{1, 2, \dots, X\}$, and $W(X)$ tends to infinity with X arbitrarily slowly. This makes some initial progress on a recent question of Harper.

1. Introduction

We are interested in the partial sums behavior of a family of completely multiplicative functions f supported on moving short intervals. Formally, for positive integers X, let $[X] := \{1, 2, \dots, X\}$ and

$$\mathcal{F}_X := \{f : [X] \to \{|z| = 1\} : f \text{ is completely multiplicative}\}.$$

For $f \in \mathcal{F}_X$, the function values $f(n)$ for all $n \leqslant X$ are uniquely determined by $(f(p))_{p \leqslant X}$. The Steinhaus random multiplicative function is defined by selecting $f(p)$ uniformly at random from the complex unit circle and defining $f(n)$ completely multiplicatively. One may view $\mathcal{F}_X$ as the family of all Steinhaus random multiplicative functions.

Let H be another positive integer. We are interested in for a typical $f \in \mathcal{F}_{X+H}$, whether the random partial sums

$$A_H(f, x) := \frac{1}{\sqrt{H}} \sum_{x < n \leqslant x+H} f(n), \tag{1-1}$$

where x is uniformly chosen from $[X]$, behave like a complex standard Gaussian. In this note, we provide a positive answer (Theorem 1.2) when $H \ll_A X/\log^A X$ holds for all $A > 0$. As we explain in Section 4, the answer is negative for $H \gg X \exp(-(\log\log X)^{1/2-\varepsilon})$, but the question remains open between these two thresholds.

MSC2020: primary 11K65; secondary 11D45, 11D57, 11D79, 11N37.

Keywords: random multiplicative function, short moving intervals, multiplicative Diophantine equations, paucity, Gaussian behavior, correlations of divisor functions.

We formalize the question by explaining how to measure the elements in $\mathcal{F}_X$. Via complete multiplicativity of $f \in \mathcal{F}_X$, define on $\mathcal{F}_X$ the product measure

$$\nu_X := \prod_{p \leqslant X} \mu_p,$$

where for any given prime p, we let μ_p denote the uniform distribution on the set $\{f(p)\} = \{|z| = 1\}$. For example, $\nu_X(\mathcal{F}_X) = 1$.

Question 1.1 [Harper 2022, open question (iv)]. What is the distribution of the normalized random sum defined in (1-1) (for most f) as x is uniformly chosen from $[X]$?

1A. ***Main results.*** In this note, we make some progress on Question 1.1. We use the notation $\xrightarrow{d}$ to denote convergence in distribution.

Theorem 1.2. *Let integer X be large and $W(X)$ tend to infinity arbitrarily slowly as X tends to infinity. Let $H := H(X) \ll X(\log X)^{-W(X)}$ and $H \to +\infty$ as $X \to +\infty$. Then, for almost all $f \in \mathcal{F}_{X+H}$, as $X \to +\infty$,*

$$\frac{1}{\sqrt{H}} \sum_{x<n\leqslant x+H} f(n) \xrightarrow{d} \mathcal{CN}(0, 1), \tag{1-2}$$

where x is chosen uniformly from $[X]$.

Here "almost all" means the total measure of such f is $1 - o_{X\to+\infty}(1)$ under ν_{X+H}.[1] Also, $\mathcal{CN}(0, 1)$ denotes the standard complex normal distribution; a standard complex normal random variable Z (with mean 0 and variance 1) can be written as $Z = X + iY$, where X and Y are independent real normal random variables with mean 0 and variance $\frac{1}{2}$. Recall that a real normal random variable W with mean 0 and variance σ^2 satisfies

$$\mathbb{P}(W \leqslant t) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{t} e^{-x^2/(2\sigma^2)}\, dx.$$

To prove Theorem 1.2, we establish moment statistics in several situations. We first show that the integer moments of random multiplicative functions f supported on suitable short intervals match the corresponding Gaussian moments. We write $\mathbb{E}_f$ to mean "average over $f \in \mathcal{F}_X$ with respect to ν_X" (where $\mathcal{F}_X$ is always clear from context).

Theorem 1.3. *Let $x, H, k \geqslant 1$ be integers. Let $f \in \mathcal{F}_{x+H}$. Let $E(k) = 2k^2 + 2$. Then*

$$\mathbb{E}_f \left| \frac{1}{\sqrt{H}} \sum_{x<n\leqslant x+H} f(n) \right|^{2k} = k! + O_k\left(H^{-1} + \frac{H^{1/2}}{\max(x, H)^{1/2}} + \frac{H \cdot (\log x + \log H)^{E(k)}}{\max(x, H)} \right),$$

with an implied constant depending only on k.

[1] More precisely, there exist nonempty measurable sets $\mathcal{G}_{X,H} \subseteq \mathcal{F}_{X+H}$ of measure $1 - o_{X\to+\infty}(1)$ (under ν_{X+H}) such that for every sequence of functions $f_X \in \mathcal{G}_{X,H}$ ($X \geqslant 1$), the random variable on the left-hand side of (1-2) (with $f = f_X$) converges in distribution to $\mathcal{CN}(0, 1)$ as $X \to +\infty$.

Notice that $k!$ is the $2k$-th moment of the standard complex Gaussian distribution. Given an integer $k \geqslant 1$, let $E'(k)$ be the smallest real number $r \geqslant 0$ such that for every $\varepsilon > 0$, we have $\mathbb{E}_f|A_H(f,x)|^{2k} \to k!$ whenever

$$x \to +\infty \quad \text{and} \quad (\log x)^{\varepsilon} \leqslant H \leqslant x/(\log x)^{r+\varepsilon}.$$

Theorem 1.3 shows that $E'(k) \leqslant E(k)$.[2] The paper [Chatterjee and Soundararajan 2012] studies the case $k = 2$, showing in particular that $E'(2) \leqslant 1$. In the case that f is supported on $\{1, 2 \ldots, x\}$, the $2k$-th moments for general k were studied in [Batyrev and Tschinkel 1998; de la Bretèche 2001a; 2001b; Granville and Soundararajan 2001; Heap and Lindqvist 2016; Harper 2019; Harper et al. 2015] and it is known that the moments there do not match Gaussian moments: for instance, by [Harper 2019, Theorem 1.1], there exists some constant $c > 0$ such that for all positive integers $k \leqslant c(\log x/\log\log x)$ (assuming x is large),

$$\mathbb{E}_f\left|\frac{1}{\sqrt{x}}\sum_{n\leqslant x} f(n)\right|^{2k} = e^{-k^2\log(k\log(2k))+O(k^2)}(\log x)^{(k-1)^2}. \tag{1-3}$$

While (1-3) is quite uniform over k, it is unclear how uniform in k one could make our Theorem 1.3. (See Remark 2.3 for some discussion of the k-aspect in our work.)

Remark 1.4. The powers of $\log x$ above are significant. For instance, Theorem 1.3 in the range $H \gg x$ follows directly from (1-3), since $(k-1)^2 \leqslant E(k)$. One may also wonder how far our bound $E'(k) \leqslant E(k)$ is from the truth. Based on a circle method heuristic for (1-4) along the lines of [Hooley 1986, Conjecture 2], with a Hardy–Littlewood contribution on the order of $(H^{2k}/Hx^{k-1})(\log x)^{(k-1)^2}$, and an additional contribution of roughly $k!H^k$ from trivial solutions, it is plausible that one could improve the right-hand side in Theorem 1.3 to $k! + O_k((H^{k-1}/x^{k-1})(\log x)^{(k-1)^2})$ for $H \in [x^{1-\delta}, x]$. If true, this would suggest that $E'(k) \leqslant k-1$ and we believe this might be the true order. For a discussion of how one might improve on Theorem 1.3, see the beginning of Section 4.

By orthogonality, Theorem 1.3 is a statement about the Diophantine point count

$$\#\{(n_1, n_2, \ldots, n_{2k}) \in (x, x+H]^{2k} : n_1 n_2 \cdots n_k = n_{k+1} n_{k+2} \cdots n_{2k}\}. \tag{1-4}$$

The circle method, or modern versions thereof such as [Duke et al. 1993; Heath-Brown 1996], might lead to an asymptotic for (1-4) uniformly over $H \in [x^{1-\delta}, x]$ for $k = 2$, unconditionally (compare [Heath-Brown 1996, Theorem 6]), or for $k = 3$, conditionally on standard number-theoretic hypotheses (compare [Wang 2021]). Alternatively, "multiplicative" harmonic analysis along the lines of [de la Bretèche 2001b; Harper et al. 2015; Heap and Lindqvist 2016] may in fact lead to an unconditional asymptotic over $H \in [x^{1-\delta}, x]$ for all k, with many main terms involving different powers of $\log x$, $\log H$. Nonetheless, for all k, we obtain an unconditional asymptotic for (1-4) uniformly over $H \ll x/(\log x)^{Ck^2}$, by replacing

[2] After writing the paper, the authors learned that for $H \leqslant x/\exp(C_k \log x/\log\log x)$, the Diophantine statement underlying Theorem 1.3 has essentially appeared before in the literature; see [Bourgain et al. 2014, proof of Theorem 34]. However, we handle a more delicate range of the form $H \leqslant x/(\log x)^{Ck^2}$.

the complicated "off-diagonal" contribution to (1-4) with a *larger but simpler* quantity; see Section 2 for details.

Remark 1.5. An analog of (1-4) for polynomial values $P(n_i)$ is studied in [Klurman et al. 2023; Wang and Xu 2022], and a similar flavor counting question to (1-4) is studied in [Fu et al. 2021] using the decoupling method.

After Theorem 1.3, our next step towards Theorem 1.2 is to establish concentration estimates for the moments of the random sums (1-1). We write $\mathbb{E}_x$ to denote "expectation over x uniformly chosen from $[X]$" (where X is always clear from context).

Theorem 1.6. *Let $X, k \geqslant 1$ be integers with X large. Suppose that $H := H(X) \to +\infty$ as $X \to +\infty$. There exists a large absolute constant $A > 0$ such that the following holds as long as $H \ll X(\log X)^{-C_k}$ with $C_k = Ak^{Ak^{Ak}}$. Let $f \in \mathcal{F}_{X+H}$; then*

$$\mathbb{E}_f\biggl(\mathbb{E}_x\biggl|\frac{1}{\sqrt{H}}\sum_{x<n\leqslant x+H} f(n)\biggr|^{2k} - k!\biggr)^2 = o_{X\to+\infty}(1). \tag{1-5}$$

Furthermore, for any fixed positive integer $\ell < k$, we have

$$\mathbb{E}_f\biggl|\mathbb{E}_x\biggl(\frac{1}{\sqrt{H}}\sum_{x<n\leqslant x+H} f(n)\biggr)^k\biggl(\frac{1}{\sqrt{H}}\sum_{x<n\leqslant x+H} \overline{f(n)}\biggr)^\ell\biggr|^2 = o_{X\to+\infty}(1). \tag{1-6}$$

We prove Theorem 1.3 in Section 2, and then we prove Theorem 1.6 in Section 3.

Proof of Theorem 1.2, assuming Theorem 1.6. We use the notation $A_H(f, x)$ from (1-1). By Markov's inequality, Theorem 1.6 implies that there exists a set of the form

$$\begin{aligned}\mathcal{G}_{X,H} := \bigl\{f \in \mathcal{F}_{X+H} : \mathbb{E}_x|A_H(f,x)|^{2k} - k! = o_{X\to+\infty}(1) \text{ for all } k \leqslant V(X),\\ \mathbb{E}_x[A_H(f,x)^k\overline{A_H(f,x)^\ell}] = o_{X\to+\infty}(1) \text{ for all distinct } k, \ell \leqslant V(X)\bigr\}\end{aligned}$$

for some $V(X) \to +\infty$ (making a choice of $V(X)$ based on $W(X)$) such that

$$\nu_{X+H}(\mathcal{G}_{X,H}) = 1 - o_{X\to+\infty}(1).$$

Since the distribution $\mathcal{CN}(0, 1)$ is uniquely determined by its moments (see e.g., [Billingsley 2012, Theorem 30.1 and Example 30.1]), Theorem 1.2 follows from the method of moments [Gut 2005, Chapter 5, Theorem 8.6] (applied to sequences of random variables $A_H(f, x)$ indexed by $f \in \mathcal{G}_{X,H}$ as $X \to +\infty$). □

We believe results similar to our theorems above should also hold in the (extended) Rademacher case, though we do not pursue that case in this paper.

1B. ***Notation.*** For any two functions $f, g : \mathbb{R} \to \mathbb{R}$, we write $f \ll g$, $g \gg f$, $g = \Omega(f)$ or $f = O(g)$ if there exists a positive constant C such that $|f| \leqslant Cg$, and we write $f \asymp g$ or $f = \Theta(g)$ if $f \ll g$ and $g \gg f$. We write O_k to indicate that the implicit constant depends on k. We write $o_{X\to+\infty}(g)$ to denote a quantity f such that f/g tends to zero as X tends to infinity.

2. Moments of random multiplicative functions in short intervals

In this section, we prove Theorem 1.3. For integers $k, n \geqslant 1$, let $\tau_k(n)$ denote the number of positive integer solutions $(d_1, \dots, d_k)$ to the equation $d_1 \cdots d_k = n$. It is known that (see [Norton 1992, Theorem 1.29 and Corollary 1.36])

$$\tau_k(n) \ll n^{O(\log k/\log\log n)} \quad \text{as } n \to +\infty, \text{ provided } k = o_{n\to+\infty}(\log n). \tag{2-1}$$

As we mentioned before, when $H \geqslant x$, Theorem 1.3 is implied by (1-3). From now on, we focus on the case $H \leqslant x$. We split the proof into two cases: small H and large H. For small H, we illustrate the general strategy and carelessly use divisor bounds; for large H, we take advantage of bounds of Shiu [1980] and Henriot [2012] on mean values and correlations of multiplicative functions over short intervals, together with a decomposition idea.

2A. ***Case 1:*** $\boldsymbol{H \leqslant x^{1-\varepsilon k^{-1}}}$**.** Here we take ε to be a small absolute constant, e.g., $\varepsilon = \frac{1}{100}$.

We begin with the following proposition.

Proposition 2.1. *Let $k, y, H \geqslant 1$ be integers. Suppose y is large and $k \leqslant \log\log y$. Then $N_k(H; y)$, the number of integer tuples $(h_1, h_2, \dots, h_k) \in [-H, H]^k$ with $y \mid h_1h_2\cdots h_k$ and $h_1h_2\cdots h_k \neq 0$, is at most $(2H)^k \cdot O(H^{O(k\log k/\log\log y)}/y)$.*

Proof. The case $k = 1$ is trivial; one has $N_1(H; y) \leqslant 2H/y$. Suppose $k \geqslant 2$. Whenever $y \mid h_1h_2\cdots h_k \neq 0$, there exists a factorization $y = u_1u_2\cdots u_k$ where u_i are positive integers such that $u_i \mid h_i \neq 0$ for all $1 \leqslant i \leqslant k$. (Explicitly, one can take $u_1 = \gcd(h_1, y)$ and $u_i = \gcd(h_i, y/\gcd(y, h_1h_2\cdots h_{i-1}))$.) It follows that $N_k(H; y) = 0$ if $y > H^k$, and

$$N_k(H; y) \leqslant \sum_{u_1u_2\cdots u_k = y} N_1(H; u_1)N_1(H; u_2)\cdots N_1(H; u_k) \leqslant \tau_k(y)\cdot(2H)^k/y \tag{2-2}$$

if $y \leqslant H^k$. By the divisor bound (2-1), Proposition 2.1 follows. □

Corollary 2.2. *Let $k, H, x \geqslant 1$ be integers. Suppose x is large and $k \leqslant \log\log x$. Then $S_k(x, H)$, the set of integer tuples $(h_1, h_2, \dots, h_k, y) \in [-H, H]^k \times (x, x+H]$ with $y \mid h_1h_2\cdots h_k$ and $h_1h_2\cdots h_k \neq 0$, has size at most $(2H)^k \cdot O(H^{1+O(k\log k/\log\log x)}/x)$.*

Proof. $\#S_k(x, H) = \sum_{x<y\leqslant x+H} N_k(H; y)$. But here $N_k(H; y) \ll (2H)^k \cdot H^{O(k\log k/\log\log x)}/x$. □

The $2k$-th moment in Theorem 1.3 is H^{-k} times the point count (1-4) for the Diophantine equation

$$n_1n_2\cdots n_k = n_{k+1}n_{k+2}\cdots n_{2k}. \tag{2-3}$$

There are $k!H^k(1+O(k^2/H)) = k!H^k + O_k(H^{k-1})$ trivial solutions. (We call a solution to (2-3) *trivial* if the tuple $(n_{k+1}, \dots n_{2k})$ equals a permutation of $(n_1, \dots n_k)$.) The number of trivial solutions is clearly $\geqslant k!H(H-1)\cdots(H-k+1)$, and $\leqslant k!H^k$.) It remains to bound $N_k(x, H)$, the number of nontrivial solutions $(n_1, \dots, n_{2k}) \in (x, x+H]^{2k}$ to (2-3).

We will show that $N_k(x, H) \ll H^k \cdot (H/x)^{1/2}$. To this end, let $N_k'(x, H)$ denote the number of nontrivial solutions in $(x, x+H]^{2k}$ with the further constraint that

$$n_{2k} \notin \{n_1, n_2, \dots, n_k\}. \tag{2-4}$$

Then for any $k \geqslant 2$, we have

$$N_k(x, H) \leqslant N_k'(x, H) + k \cdot (H+1) \cdot N_{k-1}(x, H), \tag{2-5}$$

since for each $(n_1, \dots, n_{2k}) \in (x, x+H]^{2k}$, either (2-4) holds or there exists $i \in [k]$ satisfying $n_i = n_{2k} \in (x, x+H]$.

A key observation is that for nontrivial solutions to (2-3) with constraint (2-4),[3]

$$n_{2k} \mid (n_1 - n_{2k})(n_2 - n_{2k}) \cdots (n_k - n_{2k}),$$

and if we write $h_i := n_i - n_{2k}$ then $h_i \in [-H, H]$ are nonzero. Given $h_1, h_2, \dots, h_k, y$, let

$$C_{h_1,\dots,h_k,y} := \prod_{1 \leqslant i \leqslant k} (h_i + y).$$

Then $N_k'(x, H)$ is (upon changing variables from $n_1, \dots, n_k$ to $h_1, \dots, h_k$) at most

$$\sum_{\substack{(h_1,\dots,h_k,n_{2k}) \in S_k(x,H) \\ h_i + n_{2k} > 0}} \#\left\{(n_{k+1}, \dots, n_{2k-1}) \in (x, x+H]^{k-1} : \left(\prod_{i=1}^{k-1} n_{k+i}\right) \,\middle|\, C_{h_1,\dots,h_k,n_{2k}}\right\}. \tag{2-6}$$

If x is large and k is fixed (or $k \leqslant \log\log x$, say), then by the divisor bound (2-1), the quantity (2-6) is at most

$$\ll (H+x)^{O(k \log k / \log\log x)} \cdot \#S_k(x, H) \ll O(H)^k \cdot O(H \cdot x^{-1+O(k \log k/\log\log x)}),$$

where in the last step we used Corollary 2.2.

By (2-5), it follows that x is large and k is fixed (or $k \leqslant \log\log x$, say), then

$$N_k(x, H) \leqslant k \cdot \max_{1 \leqslant j \leqslant k} (O(kH)^{k-j} \cdot N_j'(x, H)) \ll k \cdot O(kH)^k \cdot O(H \cdot x^{-1+O(k \log k/\log\log x)}). \tag{2-7}$$

(Note that $N_1(x, H) = 0$.) So in particular, $N_k(x, H) \ll H^k \cdot (H/x)^{1/2}$ for fixed k (or for x large and $k \leqslant (\log\log x)^{1/2-\delta}$, say), since $H \leqslant x^{1-\varepsilon k^{-1}}$. This suffices for Theorem 1.3.

[3] After writing the paper, the authors learned that this observation has appeared before in the literature (see [Bourgain et al. 2014, proof of Lemma 22]); however, we take the idea further, both in Section 2 and in Section 3.

Remark 2.3. The argument above in fact gives, in Case 1, a version of Theorem 1.3 with an implied constant of $O(k!k^2)$, uniformly over $k \leqslant (\log\log x)^{1/2-\delta}$, say. However, in Case 2 below, our proof relies on a larger body of knowledge for which the k-dependence does not seem easy to work out; this is why we essentially keep k fixed in Theorem 1.3.

2B. *Case 2:* $x^{1-2\varepsilon k^{-1}} \leqslant H \leqslant x$.

Again, one can assume $\varepsilon = \frac{1}{100}$. In this case, we employ the following tool due to Henriot [2012, Theorem 3]. For the multiplicative functions f in (2-8) (and in similar places below), we let $f(m) := 0$ if $m \leqslant 0$.

Definition 2.4. Given a real $A_1 \geqslant 1$ and a function $A_2 = A_2(\epsilon) \geqslant 1$ (defined for reals $\epsilon > 0$), let $\mathcal{M}(A_1, A_2)$ denote the set of nonnegative multiplicative functions $f(n)$ such that $f(p^\ell) \leqslant A_1^\ell$ (for all primes p and integers $\ell \geqslant 1$) and $f(n) \leqslant A_2 n^\epsilon$ (for all $n \geqslant 1$).

Lemma 2.5. *Let $f_1, f_2 \in \mathcal{M}(A_1, A_2)$ and $\beta \in (0, 1)$. Let $a, q \in \mathbb{Z}$ with $|a|, q \geqslant 1$ and* $\gcd(a, q) = 1$. *If $x, y \geqslant 2$ are reals with $x^\beta \leqslant y \leqslant x$ and $x \geqslant \max(q, |a|)^\beta$, then*

$$\sum_{x \leqslant n \leqslant x+y} f_1(n) f_2(qn+a) \ll_{\beta, A_1, A_2} \Delta_D \cdot y \cdot \sum_{n_1 n_2 \leqslant x} \frac{f_1(n_1) f_2(n_2)}{n_1 n_2}, \tag{2-8}$$

where $\Delta_D \leqslant \prod_{p \mid a^2} (1 + (2A_1 + A_1^2) p^{-1})$. Furthermore,

$$\Delta_D \leqslant \left(\frac{|a|}{\phi(|a|)} \right)^{2A_1 + A_1^2} \quad (\textit{where } \phi \textit{ denotes Euler's totient function}). \tag{2-9}$$

Proof. Everything but (2-9) follows from [Henriot 2012, Theorem 3] and the unraveling of definitions done in [Matomäki et al. 2019, proof of Lemma 2.3(ii)]; in the notation of [Henriot 2012, Theorem 3], we take

$$(k, Q_1(n), Q_2(n), \alpha, \delta, A, B, F(n_1, n_2)) = \big(2, n, qn+a, \tfrac{9}{10}\beta, \tfrac{9}{10}\beta, A_1, A_2(\epsilon)^2, f_1(n_1) f_2(n_2)\big),$$

where $\epsilon = \alpha/(100(2+\delta^{-1}))$.[4] The inequality (2-9) then follows from the fact that $1 + rp^{-1} \leqslant (1+p^{-1})^r \leqslant (1-p^{-1})^{-r}$ for every prime p and real $r \geqslant 1$. □

Also useful to us will be the following immediate consequence of Shiu [1980, Theorem 1].

Lemma 2.6. *Let $f \in \mathcal{M}(A_1, A_2)$ and $\beta \in (0, 1)$. If $x, y \geqslant 2$ are reals with $x^\beta \leqslant y \leqslant x$, then*

$$\sum_{x \leqslant n \leqslant x+y} f(n) \ll_{\beta, A_1, A_2} \frac{y}{\log x} \exp\biggl(\sum_{p \leqslant x} \frac{f(p)}{p} \biggr).$$

We will apply the above results to $f = \tau_k$ over intervals of the form $[x, x+y]$ with $y \gg x^{1/2k}$, say. Here $\tau_k \in \mathcal{M}(k, O_{k,\epsilon}(1))$, by (2-1) and the fact that $\tau_k(p) = k$ and

$$\tau_k(mn) \leqslant \tau_k(m) \tau_k(n) \quad \text{for arbitrary integers } m, n \geqslant 1. \tag{2-10}$$

[4] In fact, one could extract a more complicated version of (2-8) from [Henriot 2012, Theorem 3], which in some cases (e.g., if $f_1 = f_2 = \tau_k$) would improve the right-hand side of (2-8) by roughly a factor of $\log x$.

Also, recall, for integers $k \geqslant 1$ and reals $x \geqslant 2$, the standard bound

$$\sum_{n \leqslant x} \tau_k(n) \ll_k \frac{x}{\log x} \exp\biggl(\sum_{p \leqslant x} \frac{k}{p}\biggr) \ll_k x(\log x)^{k-1} \tag{2-11}$$

(see e.g., [Matomäki et al. 2019, Section 2.2]) and the consequence

$$\sum_{n_1 n_2 \leqslant x} \tau_k(n_1)\tau_k(n_2) = \sum_{n \leqslant x} \tau_{2k}(n) \ll_k x(\log x)^{2k-1}. \tag{2-12}$$

(See [Norton 1992] for a version of (2-11) with an explicit dependence on k. For Lemmas 2.5 and 2.6, we are not aware of any explicit dependence on β, A_1, A_2 in the literature.)

Lemma 2.7. *Let $V, U, q \geqslant 1$ be integers with $q \leqslant U^{k-2}$, where $k \geqslant 2$. Let $\rho \in \{-1, 1\}$. Then*

$$\sum_{\substack{u \in [U,2U) \\ 1 \leqslant v \leqslant V}} \tau_k(u)\tau_k(\rho v + uq) \ll_k VU(1 + \log VU)^{3k}.$$

Proof. First suppose $V \geqslant U$. If $u \in [U, 2U)$, then $I := \{\rho v + uq : 1 \leqslant v \leqslant V\}$ is an interval of length $V \geqslant \max(V, U)$ contained in $[-V, V + 2U^{k-1}]$, so by Lemma 2.6 and (2-11), we obtain the bound

$$\sum_{1 \leqslant v \leqslant V} \tau_k(\rho v + uq) \ll_k V(1 + \log V)^{k-1}.$$

(We consider the cases $0 \in I$ and $0 \notin I$ separately. The former case follows directly from (2-11); the latter case requires Lemma 2.6.) Then sum over u using (2-11). Since $(1 + \log V)^{k-1}(1 + \log U)^{k-1} \leqslant (1 + \log VU)^{2k-2}$, Lemma 2.7 follows.

Now suppose $V \leqslant U$. By casework on $d := \gcd(v, q) \leqslant q$, we have

$$\sum_{\substack{u \in [U,2U) \\ 1 \leqslant v \leqslant V}} \tau_k(u)\tau_k(\rho v + uq) \leqslant \sum_{d \mid q} \tau_k(d) \sum_{\substack{u \in [U,2U) \\ 1 \leqslant a \leqslant V/d \\ \gcd(a, q/d) = 1}} \tau_k(u)\tau_k(\rho a + uq/d).$$

Since $d \mid q$ and $1 \leqslant a \leqslant V/d$, we have $U \geqslant \max(a, q^{1/k})$. Now for any fixed $1 \leqslant a \leqslant V/d$,

$$\sum_{u \in [U,2U)} \tau_k(u)\tau_k(\rho a + uq/d) \ll_k \left(\frac{a}{\phi(a)}\right)^{2k+k^2} \cdot U \cdot (1 + \log U)^{2k}$$

by Lemma 2.5 and (2-12), provided $\gcd(a, q/d) = 1$. Upon summing over $1 \leqslant a \leqslant V/d$ using [Montgomery and Vaughan 2007, page 61, (2.32)], it follows that

$$\sum_{\substack{u \in [U,2U) \\ 1 \leqslant v \leqslant V}} \tau_k(u)\tau_k(\rho v + uq) \ll_k \sum_{d \mid q} \tau_k(d) \cdot \tfrac{V}{d} \cdot U \cdot (1 + \log U)^{2k}.$$

Since $\sum_{d \leqslant q} (\tau_k(d)/d) \ll_k (1 + \log q)^k$ (by (2-11)) and $q \leqslant U^{k-2}$, Lemma 2.7 follows. □

Lemma 2.8. *Let* $V_1, U_2, \dots, U_k \geqslant 1$ *be integers, where* $k \geqslant 2$. *Let* $\varepsilon_1 \in \{-1, 1\}$. *Then*

$$\sum_{\substack{v_1,u_2,\dots,u_k\geqslant 1\\ u_i\in[U_i,2U_i)\\ v_1\leqslant V_1}} \tau_k(u_2)\cdots\tau_k(u_k)\tau_k(\varepsilon_1 v_1 + u_2\cdots u_k) \ll_k L_k(V_1U_2\cdots U_k),$$

where $L_k(r) := r\cdot(1+\log r)^{3k+(k-2)(k-1)} = r\cdot(1+\log r)^{k^2+2}$ *for* $r \geqslant 1$.

Proof. We may assume $U_2 \geqslant \cdots \geqslant U_k$. Let $q := u_3\cdots u_k \leqslant U_2^{k-2}$ and apply Lemma 2.7 (with $(V, U) = (V_1, U_2)$) to sum over u_2, v_1. Then sum over the $k-2$ variables $u_3, \dots, u_k$ using (2-11). □

With the lemmas above in hand, we now build on the strategy from Case 1 to attack Case 2. As before, we let $N_k'(x, H)$ denote the number of nontrivial solutions $(n_1, \dots, n_k, n_{k+1}, \dots, n_{2k}) \in (x, x+H]^{2k}$ to (2-3) with constraint (2-4). Again, for such solutions we write $h_i = n_i - n_{2k} \in [-H, H]\setminus\{0\}$, and there exist positive integers u_i $(1 \leqslant i \leqslant k)$ such that $u_i \mid h_i$ with $u_1u_2\cdots u_k = n_{2k} \in (x, x+H]$; so $u_i \leqslant H$, and there exist signs $\varepsilon_i \in \{-1, 1\}$ and positive integers $v_i \leqslant H/U_i$ with $h_i = \varepsilon_i u_i v_i$, whence

$$C_{h_1,\dots,h_k,n_{2k}} := \prod_{i=1}^{k}(h_i + n_{2k}) = \prod_{1\leqslant i\leqslant k}(\varepsilon_i u_i v_i + u_1u_2\cdots u_k).$$

As before, the quantity $N_k'(x, H)$ is at most (2-6). Upon splitting the range $[H]$ for each u_i into $\leqslant 1 + \log_2 H \ll 1 + \log x$ dyadic intervals, we conclude that

$$N_k'(x, H) \leqslant \sum_{\varepsilon_i, U_i} \sum_{\substack{u_i\in[U_i,2U_i)\\ v_i\leqslant H/U_i\\ x<n_{2k}\leqslant x+H\\ h_i+n_{2k}>0}} \tau_k(C_{h_1,\dots,h_k,n_{2k}}) \leqslant 2^k\cdot O(1+\log x)^k\cdot \mathcal{S}(x, H), \tag{2-13}$$

where we let $n_{2k} := u_1u_2\cdots u_k$ and $h_i := \varepsilon_i u_i v_i$ in the sum over u_i, v_i (for notational brevity), and where $\mathcal{S}(x, H)$ denotes the maximum of the quantity

$$S(\vec{\varepsilon}, \vec{U}) := \sum_{\substack{u_i\in[U_i,2U_i)\\ v_i\leqslant H/U_i\\ x<n_{2k}\leqslant x+H\\ h_i+n_{2k}>0}} \tau_k(C_{h_1,\dots,h_k,n_{2k}}) = \sum_{\substack{u_i\in[U_i,2U_i)\\ v_i\leqslant H/U_i\\ x<n_{2k}\leqslant x+H\\ h_i+n_{2k}>0}} \tau_k\biggl(\prod_{1\leqslant i\leqslant k}(\varepsilon_i u_i v_i + u_1u_2\cdots u_k)\biggr)$$

over all tuples $\vec{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k) \in \{-1, 1\}^k$ and $\vec{U} = (U_1, \dots, U_k)$ where each $U_i \in [H]\cap\{1, 2, 4, 8, \dots\}$ with $2^{-k}x < U_1\cdots U_k \leqslant x+H$. Now, for the rest of Section 2, fix a choice of $\varepsilon_1, \dots, \varepsilon_k, U_1, \dots, U_k$ with

$$\mathcal{S}(x, H) = S(\vec{\varepsilon}, \vec{U}).$$

By symmetry, we may assume that $U_1 \geqslant U_2 \geqslant \cdots \geqslant U_k$.

We now bound $S(\vec{\varepsilon}, \vec{U})$, assuming $k \geqslant 2$. (For $k = 1$, we can directly note that $N_1'(x, H) = 0$.) A key observation is that since $U_1U_2\cdots U_k \leqslant x+H \leqslant 2x$ and $U_1 \geqslant U_2 \geqslant \cdots \geqslant U_k \geqslant 1$, we have (since

$H \geqslant x^{1-2\varepsilon}$ and $k \geqslant 2$)

$$\frac{H}{U_k} \geqslant \frac{H}{U_{k-1}} \geqslant \cdots \geqslant \frac{H}{U_2} \geqslant \frac{H}{(U_1U_2)^{1/2}} \geqslant \frac{x^{1-2\varepsilon}}{(2x)^{1/2}} \gg x^{1/3}.$$

By the submultiplicativity property (2-10), we have that $S(\vec{\varepsilon}, \vec{U})$ is at most

$$\sum_{\substack{u_i \in [U_i, 2U_i) \\ x < u_1u_2\cdots u_k \leqslant x+H}} \sum_{v_i \leqslant H/u_i} \tau_k(u_1)\tau_k(u_2)\cdots\tau_k(u_k) \prod_{1 \leqslant i \leqslant k} \tau_k(\varepsilon_i v_i + u_1u_2\cdots u_{-i}\cdots u_k), \tag{2-14}$$

where u_{-i} means that the factor u_i is not included. But for each $i \geqslant 2$ and $u_i \in [U_i, 2U_i)$, Lemma 2.6 and (2-11) imply (since $u_1u_2\cdots u_{-i}\cdots u_k \leqslant u_1\cdots u_k \ll x$ and $H/u_i \gg x^{1/3}$)

$$\sum_{v_i \leqslant H/u_i} \tau_k(\varepsilon_i v_i + u_1u_2\cdots u_{-i}\cdots u_k) \ll_k (H/U_i)\cdot(1+\log x)^{k-1}; \tag{2-15}$$

compare the use of Lemma 2.6 and (2-11) in the proof of Lemma 2.7. By (2-15) (multiplied over $2 \leqslant i \leqslant k$) and Lemma 2.8 (with $V_1 = H/U_1$), we conclude that the quantity (2-14) (and thus $S(\vec{\varepsilon}, \vec{U})$) is at most

$$\ll_k \frac{H^{k-1}(1+\log x)^{(k-1)^2}}{U_2\cdots U_k} \cdot L_k((H/U_1)\cdot U_2\cdots U_k) \cdot \max_{\substack{u_2,\ldots,u_k \geqslant 1 \\ u_i \in [U_i, 2U_i)}} \sum_{\substack{u_1 \in [U_1, 2U_1) \\ x < u_1u_2\cdots u_k \leqslant x+H}} \tau_k(u_1).$$

For the innermost sum, first note that $(U_2\cdots U_k)^{1/(k-1)} \leqslant (U_1\cdots U_k)^{1/k} \leqslant (2x)^{1/k}$ which implies that

$$H/(u_2\cdots u_k) \gg_k H/(U_2\cdots U_k) \gg_k x^{1-2\varepsilon k^{-1}}/x^{(k-1)/k} \geqslant x^{1/2k}$$

(since $H \geqslant x^{1-2\varepsilon k^{-1}}$); then by Lemma 2.6 and (2-11), we have (for any given $u_2, \ldots, u_k$)

$$\sum_{\substack{u_1 \geqslant 1 \\ x < u_1u_2\cdots u_k \leqslant x+H}} \tau_k(u_1) \ll_k \frac{H}{U_2\cdots U_k}\cdot(1+\log x)^{k-1}.$$

It follows that $S(\vec{\varepsilon}, \vec{U})$ is at most

$$\ll_k \frac{H^{k-1}(1+\log x)^{(k-1)^2}}{U_2\cdots U_k} \cdot \frac{H}{U_1} \cdot U_2\cdots U_k(1+\log x)^{k^2+2} \cdot \frac{H}{U_2\cdots U_k} \cdot (1+\log x)^{k-1},$$

which simplifies to $O_k(1)\cdot H^k \cdot (H/x)\cdot(1+\log x)^{2k^2-k+2}$.

Plugging the above estimate into (2-13), we have (assuming $k \geqslant 2$)

$$N'_k(x, H) \ll_k O(1+\log x)^k \cdot \mathcal{S}(x, H) \ll_k H^k \cdot (H/x)\cdot(1+\log x)^{2k^2+2}, \tag{2-16}$$

in the given range of H. Then by using the first part of (2-7) (and noting that $N_1(x, H) = N'_1(x, H) = 0$) as before, we have (for arbitrary $k \geqslant 1$)

$$N_k(x, H) \leqslant k \cdot \max_{1 \leqslant j \leqslant k} (O(kH)^{k-j} \cdot N'_j(x, H)) \ll_k H^k \cdot (H/x)\cdot(1+\log x)^{2k^2+2},$$

which suffices for Theorem 1.3.

3. Proof of Theorem 1.6

In this section, we prove Theorem 1.6. Let rad_k be the multiplicative function

$$\mathrm{rad}_k(n) = \min_{n_1 \cdots n_k = n} [n_1, \dots, n_k],$$

where $[n_1, \dots, n_k]$ denotes the least common multiple of $n_1, \dots, n_k$. In particular, for prime powers p^ℓ we have

$$\mathrm{rad}_k(p^\ell) = p^{\lceil \ell/k \rceil}. \tag{3-1}$$

Recall that we use $\tau_k(n)$ to denote the k-folder divisor function as defined in (2-6). We begin with the following sequence of lemmas.

Lemma 3.1. *Let $k, y, X, H \geqslant 1$ be integers. Then $M_k(X, H; y) := \{(x, t_1, t_2, \dots, t_k) \in [X] \times [H]^k : y \mid (x+t_1)(x+t_2) \cdots (x+t_k)\}$ has size at most $H^k \tau_k(y) \cdot (1 + X/\mathrm{rad}_k(y))$.*

Proof. Suppose that $y \mid (x+t_1) \dots (x+t_k)$. Then there exist integers $y_1, \dots, y_k \geqslant 1$ with $y_1 \cdots y_k = y$ and $y_i \mid x + t_i$ $(1 \leqslant i \leqslant k)$.

For any given choice of $y_1, \dots, y_k, t_1, \dots, t_k$, the conditions $y_i \mid x + t_i$, when satisfiable, impose on x a congruence condition modulo $[y_1, \dots, y_k]$. It follows that for any given $t_1, \dots, t_k$, the number of values of $x \in [X]$ with $(x, t_1, \dots, t_k) \in M_k(X, H; y)$ is at most

$$\sum_{y_1 \cdots y_k = y} (1 + X/[y_1, \dots, y_k]) \leqslant \tau_k(y) \cdot (1 + X/\mathrm{rad}_k(y)).$$

Lemma 3.1 follows upon summing over $t_1, \dots, t_k \in [H]$. □

Remark 3.2. For a typical value of $y \leqslant X$, Lemma 3.1 saves a factor of roughly y over the trivial bound $H^k X$, even if $H \leqslant X^{1-\delta}$, say. Lemma 3.1 is close to optimal on average over $y \leqslant X$, as one can prove by considering prime values of y, for instance. In some regimes, one can do better by other arguments: one can first fix a choice of y_i (then select x and choose $t_i \equiv -x \mod y_i$) to get

$$|M_k(X, H; y)| \leqslant \sum_{y_1 \cdots y_k = y} X \prod_i (1 + H/y_i) \leqslant \tau_k(y) X \max_{y_1 \cdots y_k = y} \prod_i (1 + H/y_i),$$

which beats Lemma 3.1 when $H \geqslant y$ and $y/\mathrm{rad}_k(y)$ is large, but not in general.

Lemma 3.3. *Let $k, y, X, H \geqslant 1$ be integers. Then $B_k(X, H; y)$, which denotes the set of integer tuples $(x, t_1, \dots, t_k, h_1, \dots, h_k) \in [X] \times [H]^k \times [-H, H]^k$ with $y \mid (x+t_1)(x+t_2) \cdots (x+t_k) h_1 h_2 \cdots h_k$ and $h_1 h_2 \cdots h_k \neq 0$, has size at most $O(H)^{2k} \cdot \tau_2(y) \tau_k(y)^2 \cdot O(1 + X/\mathrm{rad}_k(y))$.*

Proof. We write $y = uv$ with $u \mid (x+t_1)(x+t_2) \cdots (x+t_k)$ and $v \mid h_1 h_2 \cdots h_k$ (where $u, v \geqslant 1$). The number of choices of (u, v) is $\leqslant \tau_2(y)$. Using the notation in Lemma 3.1 and Proposition 2.1, we then find that

$$|B_k(X, H; y)| \leqslant \sum_{uv = y} |M_k(X, H; u)| \cdot N_k(H; v) \leqslant \tau_2(y) \max_{uv = y} |M_k(X, H; u)| \cdot N_k(H; v).$$

Now for any fixed u, v, we apply Lemma 3.1 to bound $|M_k(X, H; u)|$ and (2-2) to bound $N_k(H; v)$, getting

$$|M_k(X, H; u)| \leqslant H^k \tau_k(u) \cdot (1 + X/\operatorname{rad}_k(u)) \quad \text{and} \quad N_k(H; v) \leqslant (2H)^k \tau_k(v)/v,$$

respectively. This leads to the total bound

$$|B_k(X, H; y)| \ll \tau_2(y) H^{2k} \tau_k(y)^2 \cdot \left(1 + \frac{X}{v \operatorname{rad}_k(u)}\right).$$

For any $uv = y$, we have

$$v \operatorname{rad}_k(u) \geqslant \operatorname{rad}_k(y),$$

by the multiplicativity of rad_k, the formula (3-1), and the inequality $p^{\ell_2} p^{\lceil \ell_1/k \rceil} \geqslant p^{\lceil (\ell_1+\ell_2)/k \rceil}$ (valid for all primes p and integers $\ell_1, \ell_2 \geqslant 0$). Thus we complete the proof. □

If we allowed $h_1 h_2 \cdots h_k = 0$, we would have $X \cdot O(H)^{2k-1}$ tuples in $B_k(X, H; y)$. Lemma 3.3 gives a relative saving of roughly y/H on average over $y \ll X$; this follows from (the proof of) Lemma 3.5 below, whose proof requires the following lemma.

Lemma 3.4. *Let $K, k \geqslant 2$ be integers. For integers $i \geqslant 1$, let*

$$c_i := \sum_{(i-1)k < j \leqslant ik} \binom{j + K - 1}{K - 1}.$$

Then $c_i \leqslant K^K (ik)^K$. Furthermore, for all primes p and reals $s > 1$, we have

$$\sum_{j \geqslant 1} \tau_K(p^j) \frac{p^j}{\operatorname{rad}_k(p^j)} p^{-js} \leqslant 1 + \frac{c_1}{p^s} + \frac{c_2}{p^{2s}} + \cdots .$$

Proof. The first part is clear, since $c_i \leqslant \sum_{0 \leqslant j \leqslant ik} \binom{j+K-1}{K-1} = \binom{ik+K}{K} \leqslant (K + ik)^K \leqslant K^K (ik)^K$ (since $K, k \geqslant 2$). The second part follows from the inequality

$$\sum_{(i-1)k < j \leqslant ik} \frac{\tau_K(p^j) p^j}{\operatorname{rad}_k(p^j) p^{js}} = \sum_{(i-1)k < j \leqslant ik} \frac{\binom{j+K-1}{K-1}}{p^{\lceil j/k \rceil} p^{j(s-1)}} \leqslant \sum_{(i-1)k < j \leqslant ik} \frac{\binom{j+K-1}{K-1}}{p^i p^{i(s-1)}} = \frac{c_i}{p^{is}},$$

which holds because we have $\lceil j/k \rceil = i$ and $j \geqslant i$ whenever $(i-1)k < j \leqslant ik$. □

It turns out that to prove the key Lemma 3.7 (below) for Theorem 1.6, we need a bound of the form (3-2).

Lemma 3.5. *Let $k, X, H \geqslant 1$ be integers with X large and $H \leqslant X$. There exists a positive integer $\mathcal{C}_k = O(k^{O(k^{O(k)})})$ (depending only on k) such that the following holds:*

$$\mathbb{E}_{x \in [X]} \sum_{y \in (x, x+H]} \tau_{2k}(y)^{2k} \cdot \tau_2(y) \tau_k(y)^2 \cdot (1 + X/\operatorname{rad}_k(y)) \ll_k H (\log X)^{\mathcal{C}_k}. \tag{3-2}$$

Proof. The case $k = 1$ is clear by (2-11) (since $\mathrm{rad}_1(y) = y$), so suppose $k \geqslant 2$ for the remainder of this proof. Let $K := (2k)^{2k} \cdot 2k^2 \leqslant k^{4k+3}$. Then $\tau_{2k}(y)^{2k}\tau_2(y)\tau_k(y)^2 \leqslant \tau_K(y)$, since for all integers $j_1, j_2 \geqslant 1$ we have $\tau_{j_1}(y)\tau_{j_2}(y) \leqslant \tau_{j_1 j_2}(y)$ by [Benatar et al. 2022, (3.2)]. By Rankin's trick, the left-hand side of (3-2) is therefore at most H times

$$\sum_{y \leqslant x+H} \tau_K(y) \cdot (X^{-1} + \mathrm{rad}_k(y)^{-1}) \ll_K (\log X)^{K-1} + \sum_{n \geqslant 1} \tau_K(n) \frac{n}{\mathrm{rad}_k(n)} n^{-1-1/\log X}.$$

By Lemma 3.4 and the multiplicativity of τ_K and rad_k, we find that for $s > 1$, we have

$$\sum_{n \geqslant 1} \tau_K(n) \frac{n}{\mathrm{rad}_k(n)} n^{-s} \leqslant \prod_{p \geqslant 2} \left(1 + \frac{c_1}{p^s} + \frac{c_2}{p^{2s}} + \cdots \right), \tag{3-3}$$

where $c_i \leqslant K^K (ik)^K \leqslant K^{2K}(2K)^K 2^{i/2}$ (since $k \leqslant K$ and $i^K/2^{i/2} \leqslant (2K/\log 2)^K/e^K$, and $e \log 2 \geqslant 1$). But then

$$\frac{c_2}{p^2} + \frac{c_3}{p^3} + \cdots \ll \frac{K^{4K}}{p^2}.$$

Therefore, the right-hand side of (3-3) is at most

$$\prod_{p \geqslant 2} \left(1 + \frac{1}{p^s}\right)^{c_1} \prod_{p \geqslant 2} \left(1 + \frac{1}{p^2}\right)^{O(K^{4K})}.$$

After plugging in $s = 1 + 1/\log X$ and the bound $c_1 \leqslant K^{2K}$, Lemma 3.5 follows. □

We also need a simple but finicky combinatorial estimate.

Lemma 3.6. *Let $k, x, H \geqslant 1$ be integers. Let $\mathcal{A}_{1,2}(x, H)$ be the number of tuples $(a_1, \dots, a_{2k}) \in (x, x+H]^{2k}$ satisfying both*

(1) $\{a_1, \dots, a_k\} = \{a_{k+1}, \dots, a_{2k}\}$ (*in the usual sense, without multiplicities*), *and*

(2) $a_1 \cdots a_k = a_{k+1} \cdots a_{2k}$.

Let $\mathcal{A}_1(x, H)$ be the number of tuples $(a_1, \dots, a_{2k}) \in (x, x+H]^{2k}$ satisfying (1) (*but not necessarily* (2)). *Then $\mathcal{A}_{1,2}(x, H) \geqslant k!H^k - O_k(H^{k-1})$ and $\mathcal{A}_1(x, H) \leqslant k!H^k + O_k(H^{k-1})$.*

Proof. Call a tuple $(a_1, \dots, a_{2k}) \in (x, x+H]^{2k}$ good if it satisfies (1). Let $\mathcal{A}_1^\star$ be the number of good tuples where $a_1, \dots, a_k$ are pairwise distinct. Let $\mathcal{A}_1^\dagger$ be the number of remaining good tuples, namely good tuples where $\prod_{1 \leqslant i < j \leqslant k}(a_i - a_j) = 0$. Then $\mathcal{A}_1 \leqslant \mathcal{A}_1^\star + \mathcal{A}_1^\dagger$.

Clearly $\mathcal{A}_1^\star = k!H(H-1)\cdots(H-k+1)$ (since when the a_i are all different for $1 \leqslant i \leqslant k$, condition (1) implies that $(a_{k+1}, \dots, a_{2k})$ is a permutation of $(a_1, \dots, a_k)$; and conversely, when $(a_{k+1}, \dots, a_{2k})$ is a permutation of $(a_1, \dots, a_k)$, both (1) and (2) hold). Furthermore, $\mathcal{A}_{1,2} \geqslant \mathcal{A}_1^\star$.

On the other hand, $\mathcal{A}_1^\dagger \leqslant \binom{H}{k-1} \cdot (k-1)^{2k}$ (since if $\prod_{1 \leqslant i < j \leqslant k}(a_i - a_j) = 0$, then $\{a_1, \dots, a_k\}$ must lie in some $(k-1)$-element subset $S \subseteq (x, x+H]$, and then condition (1) implies that each of $a_1, \dots, a_{2k}$ is an element of S).

We now know $\mathcal{A}_1^\star = k!H^k + O_k(H^{k-1})$ and $\mathcal{A}_1^\dagger \ll_k H^{k-1}$. So $\mathcal{A}_{1,2} \geqslant \mathcal{A}_1^\star \geqslant k!H^k - O_k(H^{k-1})$, and $\mathcal{A}_1 \leqslant \mathcal{A}_1^\star + \mathcal{A}_1^\dagger \leqslant k!H^k + O_k(H^{k-1})$. □

Given integers $x_1, x_2, H \geqslant 1$, let $I_j = (x_j, x_j + H]$ for $j \in \{1, 2\}$. We are now ready to estimate the size of the set

$$\{(n_1, n_2, \dots, n_{2k}; m_1, m_2, \dots, m_{2k}) \in I_1^{2k} \times I_2^{2k} : n_1 \cdots n_k m_1 \cdots m_k = n_{k+1} \cdots n_{2k} m_{k+1} \cdots m_{2k}\}. \tag{3-4}$$

Lemma 3.7. *Fix an integer $k \geqslant 1$; let C_k be as in Lemma 3.5. Let X, H be large integers with $H := H(X) \to +\infty$ as $X \to +\infty$. Suppose $H \ll X(\log X)^{-2C_k}$. Then in expectation over $x_1, x_2 \in [X]$, the size of the set* (3-4) *is $k!^2 H^{2k} + o_{X\to+\infty}(H^{2k})$.*

Proof. We roughly follow the proof from Section 2 of Theorem 1.3; however, the present situation is more complicated in some aspects, which we address using some new symmetry tricks.

First, let $T_k^\star(I_1, I_2)$ be the subset of (3-4) satisfying the following conditions:

(1) If $u \in \{m_{k+1}, \dots, m_{2k}\}$, then $u \in \{m_1, \dots, m_k\}$.

(2) If $u \in \{m_1, \dots, m_k\}$, then $u \in \{m_{k+1}, \dots, m_{2k}\}$.

(3) If $u \in \{n_{k+1}, \dots, n_{2k}\}$, then $u \in \{n_1, \dots, n_k\}$.

(4) If $u \in \{n_1, \dots, n_k\}$, then $u \in \{n_{k+1}, \dots, n_{2k}\}$.

In the notation of Lemma 3.6, applied with $a = m$ and $a = n$ (separately), we have $\#T_k^\star(I_1, I_2) \geqslant \mathcal{A}_{1,2}(x_1, H)\mathcal{A}_{1,2}(x_2, H)$ and $\#T_k^\star(I_1, I_2) \leqslant \mathcal{A}_1(x_1, H)\mathcal{A}_1(x_2, H)$, so

$$\#T_k^\star(I_1, I_2) = (k!H^k + O_k(H^{k-1}))^2 = k!^2 H^{2k} + O_k(H^{2k-1}). \tag{3-5}$$

In general, given an element $\mathfrak{n} \in I_1^{2k} \times I_2^{2k}$ of (3-4), let $\mathcal{U}$ be the set of integers u that violate at least one of the conditions (1)–(4) above. Then $\mathfrak{n} \in T_k^\star(I_1, I_2)$ if and only if $\mathcal{U} = \varnothing$. This simple observation will help us estimate the size of (3-4).

Let $N_k^\star(I_1, I_2)$ be the subset of (3-4) satisfying the following conditions:

(1) $n_{2k} \notin \{n_1, \dots, n_k\}$. (This implies, but is not equivalent to, $n_{2k} \in \mathcal{U}$.)

(2) If $u \in \mathcal{U}$, then $\tau_{2k}(u) \leqslant \tau_{2k}(n_{2k})$.

Then (3-4) has size at least $\#T_k^\star(I_1, I_2)$ and we claim that (3-4) has size at most

$$\leqslant \#T_k^\star(I_1, I_2) + 2k \cdot \#N_k^\star(I_1, I_2) + 2k \cdot \#N_k^\star(I_2, I_1).$$

First note that for each element $\mathfrak{n}$ of (3-4) lying outside of $T_k^\star(I_1, I_2)$, there exist $v \in \mathcal{U}$ and $(a, b, c) \in \{m, n\} \times \{0, k\} \times [k]$, with $\tau_{2k}(v) = \max_{u\in\mathcal{U}} \tau_{2k}(u)$, such that $a_{b+c} = v$ and $a_{b+c} \notin \{a_{(k-b)+i} : i \in [k]\}$; the existence of v with $\tau_{2k}(v) = \max_{u\in\mathcal{U}} \tau_{2k}(u)$ follows from the fact that $\mathcal{U} \neq \varnothing$, and the existence of (a, b, c) then follows from the definition of $\mathcal{U}$. The claim then follows from the definitions of $N_k^\star(I_1, I_2)$ and $N_k^\star(I_2, I_1)$, upon summing over all possibilities for a, b, c.

It follows that in expectation over $x_1, x_2 \in [X]$, the size of (3-4) is

$$\mathbb{E}_{x_1,x_2}\#T_k^\star(I_1, I_2) + O(2k \cdot \mathbb{E}_{x_1,x_2}\#N_k^\star(I_1, I_2)). \tag{3-6}$$

The projection $I_1^{2k} \times I_2^{2k} \ni (n_1, \dots, n_{2k}; m_1, \dots, m_{2k}) \mapsto (n_1, \dots, n_k; m_1, \dots, m_k; n_{2k}) \in I_1^k \times I_2^k \times I_1$, i.e., "forgetting" $n_{k+1}, \dots, n_{2k-1}, m_{k+1}, \dots, m_{2k}$, defines a map π from $N_k^\star(I_1, I_2)$ to the set

$$D_k^\star(I_1, I_2) := \{(n_1, \dots, n_k; m_1, \dots, m_k; n_{2k}) \in I_1^k \times I_2^k \times I_1 : n_{2k} \mid n_1 \cdots n_k m_1 \cdots m_k, n_{2k} \notin \{n_1, \dots, n_k\}\}.$$

We now bound the fibers of π. Suppose $(n_1, \dots, n_{2k}; m_1, \dots, m_{2k}) \in N_k^\star(I_1, I_2)$. Let $S_1 := \{i \in \{k+1, \dots, 2k\} : n_i \notin \mathcal{U}\}$ and $S_2 := \{j \in \{k+1, \dots, 2k\} : m_j \notin \mathcal{U}\}$, and let

$$z := \prod_{i \in \{k+1,\dots,2k\} \setminus S_1} n_i \prod_{j \in \{k+1,\dots,2k\} \setminus S_2} m_j = \frac{n_1 \cdots n_k m_1 \cdots m_k}{\prod_{i \in S_1} n_i \prod_{j \in S_2} m_j}.$$

Then the following hold:

- $n_i \in \{n_1, \dots, n_k\}$ for all $i \in S_1$, and $m_j \in \{m_1, \dots, m_k\}$ for all $j \in S_2$.
- z depends only on $n_1, \dots, n_k, m_1, \dots, m_k, (n_i)_{i \in S_1}, (m_j)_{j \in S_2}$.
- $\tau_{2k-|S_1|-|S_2|}(z) \leqslant \tau_{2k}(z) \leqslant \tau_{2k}(n_{2k})^{2k-|S_1|-|S_2|}$. (The upper bound on $\tau_{2k}(z)$ arises as follows: since z is the product of $2k-|S_1|-|S_2|$ elements u_l of $\mathcal{U}$, we have an upper bound $\leqslant \prod_{1 \leqslant l \leqslant 2k-|S_1|-|S_2|} \tau_{2k}(u_l)$, which is $\leqslant \prod_{1 \leqslant l \leqslant 2k-|S_1|-|S_2|} \tau_{2k}(n_{2k})$.)

Therefore, the fiber of π over $(n_1, \dots, n_k; m_1, \dots, m_k; n_{2k}) \in D_k^\star(I_1, I_2)$ has size at most

$$\sum_{S_1, S_2 \subseteq \{k+1,\dots,2k\}} k^{|S_1|} \cdot k^{|S_2|} \cdot \tau_{2k}(n_{2k})^{2k-|S_1|-|S_2|} = \sum_{0 \leqslant l \leqslant 2k} \binom{2k}{l} k^l \tau_{2k}(n_{2k})^{2k-l}, \tag{3-7}$$

where each S_t $(1 \leqslant t \leqslant 2)$ runs through all possible subsets of $\{k+1, \dots, 2k\}$.

The right-hand side of (3-7) equals $(k + \tau_{2k}(n_{2k}))^{2k} \leqslant (k+1)^{2k} \tau_{2k}(n_{2k})^{2k}$, so upon summing over $(n_1, \dots, n_k; m_1, \dots, m_k; n_{2k}) \in D_k^\star(I_1, I_2)$, we conclude that

$$\#N_k^\star(I_1, I_2) \leqslant (k+1)^{2k} \sum_{(n_1,\dots,n_k; m_1,\dots,m_k; n_{2k}) \in D_k^\star(I_1, I_2)} \tau_{2k}(n_{2k})^{2k}. \tag{3-8}$$

We use (3-8) to bound $\mathbb{E}_{x_2}\#N_k^\star(I_1, I_2)$. Note that if $(n_1, \dots, n_k; m_1, \dots, m_k; n_{2k}) \in D_k^\star(I_1, I_2)$ and $y := n_{2k}$ (so that in particular, $m_i - x_2 \in [H]$ and $n_i - y \in [-H, H] \setminus \{0\}$ for all $i \in [k]$), then $y \in (x_1, x_1 + H]$ and

$$(x_2, m_1 - x_2, \dots, m_k - x_2, n_1 - y, \dots, n_k - y) \in B_k(X, H; y),$$

in the notation of Lemma 3.3. Therefore, summing (3-8) over $x_2 \in [X]$ gives the inequality

$$X \cdot \mathbb{E}_{x_2}\#N_k^\star(I_1, I_2) = \sum_{x_2 \in [X]} \#N_k^\star(I_1, I_2) \ll_k \sum_{y \in (x_1, x_1+H]} \tau_{2k}(y)^{2k} \cdot |B_k(X, H; y)|.$$

We next apply Lemma 3.3 to give an upper bound on $|B_k(X, H; y)|$, which leads to

$$X \cdot \mathbb{E}_{x_2} \# N_k^\star(I_1, I_2) \ll_k \sum_{y \in (x_1, x_1+H]} \tau_{2k}(y)^{2k} O(H)^{2k} \cdot \tau_2(y)\tau_k(y)^2 \cdot O(1 + X/\operatorname{rad}_k(y)).$$

Average over x_1 by using Lemma 3.5, to get

$$\mathbb{E}_{x_1,x_2} \# N_k^\star(I_1, I_2) \ll_k O(H)^{2k} \cdot H \cdot X^{-1} (\log X)^{C_k}. \tag{3-9}$$

This is $\ll_k H^{2k}(\log X)^{-C_k}$ in our range of H. By (3-5) and (3-9), quantity (3-6) is $k!^2 H^{2k} + O_k(H^{2k-1}) + O_k(H^{2k}(\log X)^{-C_k})$. Lemma 3.7 follows. □

Proof of Theorem 1.6. Assume A is large and $H \ll X(\log X)^{-C_k}$, where $C_k = Ak^{Ak^{Ak}}$. Let $C := 10$, so that the quantity $E(k) = 2k^2 + 2$ in Theorem 1.3 satisfies

$$E(k) \leqslant 4Ck^2, \quad E(k+\ell) \leqslant 5Ck^2 \quad \text{for all } 1 \leqslant \ell \leqslant k-1. \tag{3-10}$$

(This is just for uniform notational convenience.)

(a) We prove (1-5), a bound on the quantity

$$\mathbb{E}_f(\mathbb{E}_x |A_H(f, x)|^{2k} - k!)^2, \tag{3-11}$$

where $A_H(f, x)$ is defined as in (1-1). By expanding the square, we can rewrite (3-11) as

$$\mathbb{E}_f(\mathbb{E}_x |A_H(f, x)|^{2k})^2 - 2k! \mathbb{E}_f \mathbb{E}_x |A_H(f, x)|^{2k} + k!^2. \tag{3-12}$$

The subtracted term in (3-12) can be computed by switching the summation: it equals

$$-2k! \mathbb{E}_x \mathbb{E}_f |A_H(f, x)|^{2k}. \tag{3-13}$$

We estimate (3-13) by a combination of trivial bounds (based on the divisor bound (2-1)) and the moment estimate in Theorem 1.3. We split the sum $\mathbb{E}_x \mathbb{E}_f |A_H(f, x)|^{2k}$ into two ranges, and apply Theorem 1.3 and (3-10), to get that $X \cdot \mathbb{E}_x \mathbb{E}_f |A_H(f, x)|^{2k}$ equals

$$\begin{aligned} &\sum_{1 \leqslant x \leqslant H(\log X)^{5Ck^2}} \mathbb{E}_f |A_H(f, x)|^{2k} + \sum_{H(\log X)^{5Ck^2} \leqslant x \leqslant X} \mathbb{E}_f |A_H(f, x)|^{2k} \\ &\qquad = \sum_{1 \leqslant x \leqslant H(\log X)^{5Ck^2}} O((\log X)^{4Ck^2}) + \sum_{H(\log X)^{5Ck^2} \leqslant x \leqslant X} (k! + O((\log X)^{-Ck^2})). \end{aligned}$$

Upon summing over both ranges of x above, it follows that $\mathbb{E}_x \mathbb{E}_f |A_H(f, x)|^{2k} = k! + o_{X \to +\infty}(1)$ in the given range of H (provided A is large enough that $C_k \geqslant 10Ck^2$).

We next focus on the first term in (3-12). We expand out the expression and switch the expectations to get that the first term in (3-12) is

$$\mathbb{E}_{x_1} \mathbb{E}_{x_2} \mathbb{E}_f |A_H(f, x_1)|^{2k} |A_H(f, x_2)|^{2k}. \tag{3-14}$$

Now we use orthogonality and apply Lemma 3.7 to see that (3-14) is $k!^2 + o_{X\to+\infty}(1)$ in the given range of H (if A is sufficiently large). Combining the above together, (1-5) follows.

(b) We prove (1-6), a bound on the quantity (in the notation $A_H(f,x)$ from (1-1))

$$\mathbb{E}_f|\mathbb{E}_x[A_H(f,x)^k\overline{A_H(f,x)^\ell}]|^2 = X^{-2}\sum_{x_1,x_2\in[X]}\mathcal{B}_H(x_1,x_2), \tag{3-15}$$

where $1\leqslant \ell\leqslant k-1$ and $\mathcal{B}_H(x_1,x_2) := \mathbb{E}_f A_H(f,x_1)^k\overline{A_H(f,x_1)^\ell A_H(f,x_2)^k}A_H(f,x_2)^\ell$. This is the same as counting solutions to

$$n_1n_2\cdots n_k\cdot m_1m_2\cdots m_\ell = n_{k+1}n_{k+2}\cdots n_{k+\ell}\cdot m_{\ell+1}m_{\ell+2}\cdots m_{\ell+k}, \tag{3-16}$$

where $x_1\leqslant n_i\leqslant x_1+H$ and $x_2\leqslant m_i\leqslant x_2+H$ for all $1\leqslant i\leqslant k+\ell$. Suppose that $x_1\geqslant x_2$. The left-hand side in (3-16) is

$$n_1n_2\cdots n_k\cdot m_1m_2\cdots m_\ell \geqslant x_1^kx_2^\ell,$$

while the right-hand side in (3-16) is

$$n_{k+1}n_{k+2}\cdots n_{k+\ell}\cdot m_{\ell+1}m_{\ell+2}\cdots m_{\ell+k}\leqslant (x_1+H)^\ell(x_2+H)^k\leqslant x_1^\ell x_2^k\bigl(1+\tfrac{H}{x_2}\bigr)^{k+\ell}.$$

To make them equal, we must have

$$x_1/x_2\leqslant (x_1/x_2)^{k-\ell}\leqslant \bigl(1+\tfrac{H}{x_2}\bigr)^{2k},$$

which implies that (under the assumption $Hk = o(x_2)$)

$$x_2\leqslant x_1\leqslant x_2+O(kH).$$

From now on, we only need to consider two cases:

(1) $\min(x_1,x_2)\ll kH$.

(2) $|x_1-x_2| = O(kH)$.

We first deal with case (1): $\min(x_1,x_2)\ll kH$. By the Cauchy–Schwarz inequality,

$$|\mathcal{B}_H(x_1,x_2)|^2\ll_k (\mathbb{E}_f|A_H(f,x_1)|^{2(k+\ell)})\cdot(\mathbb{E}_f|A_H(f,x_2)|^{2(k+\ell)}).$$

Theorem 1.3 and (3-10) imply that $\mathcal{B}_H(x_1,x_2)\ll_k(\log X)^{5Ck^2}$. So the contribution to (3-15) over all pairs (x_1,x_2) with $\min\{x_1,x_2\}\leqslant H$ is at most $\ll 1/(\log X)^{C_k-10Ck^2}$, which is $o_{X\to+\infty}(1)$ by our choice of C_k.

We next deal with case (2): $|x_1-x_2| = O(kH)$. Assume $x_2<x_1$. Then all the variables m_i, n_j are in $[x_2, x_1+H]$, so by Theorem 1.3 and (3-10), the contribution in this case to (3-16) over x_1, x_2 is at most

$$\ll_k XH(\log X)^{10Ck^2}\cdot H^{k+\ell}(\log X)^{5Ck^2}\ll X^2(\log X)^{15Ck^2-C_k}\cdot H^{k+\ell} = X^2\cdot o_{X\to+\infty}(H^{k+\ell}),$$

by our choice of C_k. After dividing by $X^2H^{k+\ell}$, we see that the total contribution to (3-15) in this case is $o_{X\to+\infty}(1)$.

Combining the two cases above, we obtain the desired (1-6). □

4. Concluding remarks

Recall the exponent $E'(k)$ defined after Theorem 1.3. As we mentioned before, Theorem 1.3 implies $E'(k) \leqslant E(k) = 2k^2 + 2$, and the truth may be that $E'(k)$ grows linearly in k. The method used in [de la Bretèche 2001b; Harper et al. 2015; Heap and Lindqvist 2016] may help to extend Theorem 1.3, i.e., to improve on the bound $E'(k) \leqslant E(k)$. Alternatively, one might try to improve on Theorem 1.3 via Hooley's Δ-function technique [1979]; note that $(x, x+H] \subseteq (x, ex]$ if $H \leqslant x$.

The true threshold in the problem studied in Theorem 1.2 is more delicate. A closely related problem is to understand for what range of H, as $X \to +\infty$, the following holds:

$$\frac{1}{\sqrt{H}} \sum_{X < n \leqslant X+H} f(n) \xrightarrow{d} \mathcal{CN}(0, 1), \tag{4-1}$$

where f is a Steinhaus random multiplicative function over the short interval $(X, X+H]$. In contrast to the problem we studied in this paper, X is first fixed in (4-1) and the random multiplicative function f varies. For this question, it is known that [Soundararajan and Xu 2022] if $H \to +\infty$ and $H \ll X/(\log X)^{2\log 2 - 1 + \varepsilon}$, then such a central limit theorem holds. In the other direction, by using Harper's remarkable results and methods [2020] one may be able to show that

$$\mathbb{E}_f \left| \frac{1}{\sqrt{H}} \sum_{X < n \leqslant X+H} f(n) \right| = o_{X \to +\infty}(1), \quad \text{if } H \gg \frac{X}{\exp((\log\log X)^{1/2-\varepsilon})}; \tag{4-2}$$

see [Soundararajan and Xu 2022] for more discussions. Thus, in the above range of H, the $\sqrt{H}$-normalized partial sums do not have Gaussian limiting distribution. It would be interesting to know if another choice of normalization would lead to a Gaussian distribution. Now we return to the question we studied in Theorem 1.2. We established "typical Gaussian behavior" over a range of the form $H \ll X/(\log X)^{W(X)} = X/(\exp(W(X) \log\log X))$ (where $H \to +\infty$). It seems that to extend the range of H so that such a Gaussian behavior holds, significant new ideas would be needed. It would be interesting to understand the whole story for all ranges of H, for both the question studied in Theorem 1.2 and that in (4-1).

Acknowledgements

We thank Andrew Granville and the anonymous referee for many detailed comments that led us to significantly improve the results and presentation of our work. We thank and Adam Harper for helpful discussions and useful comments and corrections on earlier versions. We also thank Yuqiu Fu, Larry Guth, Kannan Soundararajan, Katharine Woo, and Liyang Yang for helpful discussions. Finally, we thank Peter Sarnak for introducing us (the authors) to each other during the "50 Years of Number Theory and Random Matrix Theory" Conference at IAS and making the collaboration possible.

References

[Batyrev and Tschinkel 1998] V. V. Batyrev and Y. Tschinkel, "Manin's conjecture for toric varieties", *J. Algebraic Geom.* **7**:1 (1998), 15–53. MR Zbl

[Benatar et al. 2022] J. Benatar, A. Nishry, and B. Rodgers, "Moments of polynomials with random multiplicative coefficients", *Mathematika* **68**:1 (2022), 191–216. MR Zbl

[Billingsley 2012] P. Billingsley, *Probability and measure*, 3rd ed., Wiley, Hoboken, NJ, 2012. MR Zbl

[Bourgain et al. 2014] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, "Multiplicative congruences with variables from short intervals", *J. Anal. Math.* **124** (2014), 117–147. MR Zbl

[de la Bretèche 2001a] R. de la Bretèche, "Compter des points d'une variété torique", *J. Number Theory* **87**:2 (2001), 315–331. MR Zbl

[de la Bretèche 2001b] R. de la Bretèche, "Estimation de sommes multiples de fonctions arithmétiques", *Compositio Math.* **128**:3 (2001), 261–298. MR Zbl

[Chatterjee and Soundararajan 2012] S. Chatterjee and K. Soundararajan, "Random multiplicative functions in short intervals", *Int. Math. Res. Not.* **2012**:3 (2012), 479–492. MR Zbl

[Duke et al. 1993] W. Duke, J. Friedlander, and H. Iwaniec, "Bounds for automorphic L-functions", *Invent. Math.* **112**:1 (1993), 1–8. MR Zbl

[Fu et al. 2021] Y. Fu, L. Guth, and D. Maldague, "Decoupling inequalities for short generalized Dirichlet sequences", preprint, 2021. arXiv 2104.00856

[Granville and Soundararajan 2001] A. Granville and K. Soundararajan, "Large character sums", *J. Amer. Math. Soc.* **14**:2 (2001), 365–397. MR Zbl

[Gut 2005] A. Gut, *Probability: a graduate course*, Springer, 2005. MR Zbl

[Harper 2019] A. J. Harper, "Moments of random multiplicative functions, II: High moments", *Algebra Number Theory* **13**:10 (2019), 2277–2321. MR Zbl

[Harper 2020] A. J. Harper, "Moments of random multiplicative functions, I: Low moments, better than squareroot cancellation, and critical multiplicative chaos", *Forum Math. Pi* **8** (2020), art. id. e1. MR Zbl

[Harper 2022] A. J. Harper, "A note on character sums over short moving intervals", preprint, 2022. arXiv 2203.09448

[Harper et al. 2015] A. J. Harper, A. Nikeghbali, and M. Radziwiłł, "A note on Helson's conjecture on moments of random multiplicative functions", pp. 145–169 in *Analytic number theory*, edited by C. Pomerance and M. T. Rassias, Springer, 2015. MR Zbl

[Heap and Lindqvist 2016] W. P. Heap and S. Lindqvist, "Moments of random multiplicative functions and truncated characteristic polynomials", *Q. J. Math.* **67**:4 (2016), 683–714. MR Zbl

[Heath-Brown 1996] D. R. Heath-Brown, "A new form of the circle method, and its application to quadratic forms", *J. Reine Angew. Math.* **481** (1996), 149–206. MR Zbl

[Henriot 2012] K. Henriot, "Nair–Tenenbaum bounds uniform with respect to the discriminant", *Math. Proc. Cambridge Philos. Soc.* **152**:3 (2012), 405–424. MR Zbl

[Hooley 1979] C. Hooley, "On a new technique and its applications to the theory of numbers", *Proc. London Math. Soc.* (3) **38**:1 (1979), 115–151. MR Zbl

[Hooley 1986] C. Hooley, "On some topics connected with Waring's problem", *J. Reine Angew. Math.* **369** (1986), 110–153. MR Zbl

[Klurman et al. 2023] O. Klurman, I. D. Shkredov, and M. W. Xu, "On the random Chowla conjecture", *Geom. Funct. Anal.* **33**:3 (2023), 749–777. MR Zbl

[Matomäki et al. 2019] K. Matomäki, M. Radziwiłł, and T. Tao, "Correlations of the von Mangoldt and higher divisor functions II: Divisor correlations in short ranges", *Math. Ann.* **374**:1-2 (2019), 793–840. MR Zbl

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Studies in Advanced Mathematics **97**, Cambridge University Press, 2007. MR Zbl

[Norton 1992] K. K. Norton, “Upper bounds for sums of powers of divisor functions”, *J. Number Theory* **40**:1 (1992), 60–85. MR Zbl

[Shiu 1980] P. Shiu, “A Brun–Titchmarsh theorem for multiplicative functions”, *J. Reine Angew. Math.* **313** (1980), 161–170. MR Zbl

[Soundararajan and Xu 2022] K. Soundararajan and M. W. Xu, “Central limit theorems for random multiplicative functions”, preprint, 2022. arXiv 2212.06098

[Wang 2021] V. Y. Wang, “Approaching cubic diophantine statistics via mean-value L-function conjectures of random matrix theory type”, preprint, 2021. arXiv 2108.03398v1

[Wang and Xu 2022] V. Y. Wang and M. W. Xu, “Paucity phenomena for polynomial products”, preprint, 2022. arXiv 2211.02908

Communicated by Andrew Granville
Received 2022-07-24 Revised 2023-03-08 Accepted 2023-05-13

mayankpandey9973@gmail.com *Princeton University, Princeton, NJ, United States*

vywang@alum.mit.edu *Courant Institute, New York University, New York, NY, United States*

maxxu@stanford.edu *Department of Mathematics, Stanford University, Stanford, CA, United States*

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.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

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@msp.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 18 No. 2 2024