Algebra & Number Theory

Volume 9
2015
No. 8

msp

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2015 is US $255/year for the electronic version, and $440/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers 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. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

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 9:8 (2015)
dx.doi.org/10.2140/ant.2015.9.1741

G-valued crystalline representations with minuscule p-adic Hodge type

Brandon Levin

We study G-valued semistable Galois deformation rings, where G is a reductive group. We develop a theory of Kisin modules with G-structure and use this to identify the connected components of crystalline deformation rings of minuscule p-adic Hodge type with the connected components of moduli of "finite flat models with G-structure". The main ingredients are a construction in integral p-adic Hodge theory using Liu's theory of $(\varphi, \hat{G})$-modules and the local models constructed by Pappas and Zhu.

1. Introduction

1.1. *Overview.* One of the principal challenges in the study of modularity lifting or, more generally, automorphy lifting via the techniques introduced in [Taylor and Wiles 1995] is understanding local deformation conditions at $\ell = p$. Kisin [2009] introduced a ground-breaking new technique for studying one such condition, flat deformations, which led to better modularity lifting theorems. Kisin [2008] extended those techniques to construct potentially semistable deformation rings with specified Hodge–Tate weights. In this paper, we study Galois deformations valued in a reductive group G and extend Kisin's techniques to this setting. In particular, we define and prove structural results about "flat" G-valued deformations.

Let G be a reductive group over a $\mathbb{Z}_p$-finite flat local domain Λ with connected fibers. Let $\mathbb{F}$ be the residue field of Λ and $F := \Lambda[1/p]$. Let $K/\mathbb{Q}_p$ be a finite extension with absolute Galois group Γ_K and fix a representation $\bar{\eta} : \Gamma_K \to G(\mathbb{F})$. The

MSC2010: primary 11S20; secondary 14L15, 14F30.

Keywords: Galois representation, p-adic Hodge theory, finite flat group scheme, local model.

(framed) G-valued deformation functor is represented by a complete local Noetherian Λ-algebra $R^{\square}_{G,\bar{\eta}}$. For any geometric cocharacter μ of $\mathrm{Res}_{(K\otimes_{\mathbb{Q}_p}F)/F}\,G_F$, there exists a quotient $R^{\mathrm{st},\mu}_{\bar{\eta}}$ (resp. $R^{\mathrm{cris},\mu}_{\bar{\eta}}$) of $R^{\square}_{G,\bar{\eta}}$ whose points over finite extensions F'/F are semistable (resp. crystalline) representations with p-adic Hodge type μ (see [Balaji 2012, Theorem 3.0.12]).

When $G = \mathrm{GL}_n$ and μ is minuscule, $R^{\mathrm{cris},\mu}_{\bar{\eta}}$ it appears the thesis changed is a quotient of a flat deformation ring. For modularity lifting, it is important to know the connected components of Spec $R^{\mathrm{cris},\mu}_{\bar{\eta}}[1/p]$. Intuitively, Kisin's [2009] technique is to resolve the flat deformation ring by "moduli of finite flat models" of deformations of $\bar{\eta}$. When $K/\mathbb{Q}_p$ is ramified, the resolution is not smooth, but its singularities are relatively mild, which allowed for the determination of the connected components in many instances when $G = \mathrm{GL}_2$ [Kisin 2009, Propositions 2.5.6 and 2.5.15]. Kisin's technique extends beyond the flat setting (for μ arbitrary), where one resolves deformation rings by moduli spaces of integral p-adic Hodge theory data called $\mathfrak{S}$-modules of finite height, also known as *Kisin modules*.

In this paper, we define a notion of Kisin module with G-structure or, as we call them, *G-Kisin modules* (Definition 2.2.7) and we construct a resolution

$$\Theta : X^{\mathrm{cris},\mu}_{\bar{\eta}} \to \mathrm{Spec}\, R^{\mathrm{cris},\mu}_{\bar{\eta}},$$

where Θ is a projective morphism and $\Theta[1/p]$ is an isomorphism (see Propositions 2.3.3 and 2.3.9). The same construction works for $R^{\mathrm{st},\mu}_{\bar{\eta}}$ as well. The goal then is to understand the singularities of $X^{\mathrm{cris},\mu}_{\bar{\eta}}$. The natural generalization of the flat condition for GL_n to an arbitrary group G is *minuscule* p-adic Hodge type μ. A cocharacter μ of a reductive group H is minuscule if its weights when acting on Lie H lie in $\{-1, 0, 1\}$ (see Definition 4.1.1 and discussion afterward). Our main theorem is a generalization of the main result of [Kisin 2009] on the geometry of $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ for G reductive and μ minuscule:

Theorem 4.4.1. *Assume $p \nmid \pi_1(G^{\mathrm{der}})$, where G^{der} is the derived subgroup of G. Let μ be a minuscule geometric cocharacter of $\mathrm{Res}_{(K\otimes_{\mathbb{Q}_p}F)/F}\,G_F$. Then $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ is normal and $X^{\mathrm{cris},\mu}_{\bar{\eta}} \otimes_{\Lambda_{[\mu]}} \mathbb{F}_{[\mu]}$ is reduced, where $\Lambda_{[\mu]}$ is the ring of integers of the reflex field of μ.*

When $G = \mathrm{GSp}_{2g}$, this is a result of Broshi [2008]; also, this is a stronger result than in [Levin 2013], where we placed a more restrictive hypothesis on μ (see Remark 1.1.1). The significance of Theorem 4.4.1 is that it allows one to identify the connected components of Spec $R^{\mathrm{cris},\mu}_{\bar{\eta}}[1/p]$ with the connected components of the fiber in $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ over the closed point of Spec $R^{\mathrm{cris},\mu}_{\bar{\eta}}$, a projective scheme over $\mathbb{F}_{[\mu]}$ (see Corollary 4.4.2). This identification led to the successful determination of the connected components of Spec $R^{\mathrm{cris},\mu}_{\bar{\eta}}[1/p]$ in the case when $G = \mathrm{GL}_2$ [Kisin 2009; Gee 2006; Imai 2010; 2012; Hellmann 2011]. Outside of GL_2, relatively little is known about the connected components of these deformations rings without restricting the ramification in K.

When $K/\mathbb{Q}_p$ is unramified, we have a stronger result:

Theorem 4.4.6. *Assume $K/\mathbb{Q}_p$ is unramified, $p > 3$, and $p \nmid \pi_1(G^{\mathrm{ad}})$. Then the universal crystalline deformation ring $R_{\bar{\eta}}^{\mathrm{cris},\mu}$ is formally smooth over $\Lambda_{[\mu]}$. In particular,* Spec $R_{\bar{\eta}}^{\mathrm{cris},\mu}[1/p]$ *is connected.*

Remark 1.1.1. In [Levin 2013], we made the assumption on the cocharacter μ that there exists a representation $\rho : G \to \mathrm{GL}(V)$ such that $\rho \circ \mu$ is minuscule. This extra hypothesis on μ excluded most adjoint groups like PGL_n as well as exceptional types like E_6 and E_7, both of which have minuscule cocharacters. One can weaken the assumptions in Theorem 4.4.6 if one assumes this stronger condition on μ.

Remark 1.1.2. The groups $\pi_1(G^{\mathrm{der}})$ and $\pi_1(G^{\mathrm{ad}})$ appearing in Theorems 4.4.1 and 4.4.6 are the fundamental groups in the sense of semisimple groups. Note that $\pi_1(G^{\mathrm{der}})$ is a subgroup of $\pi_1(G^{\mathrm{ad}})$. The assumption that $p \nmid \pi_1(G^{\mathrm{der}})$ insures that the local models we use have nice geometric properties. The stronger assumption in Theorem 4.4.6 that $p \nmid \pi_1(G^{\mathrm{ad}})$ is probably not necessary and is a byproduct of the argument, which involves reduction to the adjoint group.

There are two main ingredients in the proof of Theorem 4.4.1 and its applications, one coming from integral p-adic Hodge theory and the other from local models of Shimura varieties. In Kisin's original construction, a key input was an advance in integral p-adic Hodge theory, building on work of Breuil, which allows one to describe finite flat group schemes over $\mathcal{O}_K$ in terms of certain linear algebra objects called *Kisin modules* of height in [0, 1] [Kisin 2006; 2009]. More precisely, then, $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ is a moduli space of G-Kisin modules with "type" μ. Intuitively, one can imagine $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ as a moduli of finite flat models with additional structure.

The proof of Theorem 4.4.1 uses a recent advance of Liu [2010] in integral p-adic Hodge theory to overcome a difficulty in identifying the local structure of $X_{\bar{\eta}}^{\mathrm{cris},\mu}$. Heuristically, the difficulty arises because for a general group G one cannot work only in the setting of Kisin modules of height in [0, 1], where one has a nice equivalence of categories between that category and the category of finite flat group schemes. Beyond the height-in-[0, 1] situation, the Kisin module only remembers the Galois action of the subgroup $\Gamma_\infty \subset \Gamma_K$ which fixes the field $K(\pi^{1/p}, \pi^{1/p^2}, \dots)$ for some compatible system of p-power roots of a uniformizer π of K.

Liu [2010] introduced a more complicated linear algebra structure on a Kisin module, called a $(\varphi, \widehat{G})$-module, which captures the action of Γ_K, the full Galois group. We call them $(\varphi, \widehat{\Gamma})$-modules to avoid confusion with the group G. Let A be a finite local Λ-algebra which is either Artinian or flat. Our principal result

(Theorem 4.3.6) says roughly that, if $\rho : \Gamma_\infty \to G(A)$ has "type" μ, i.e., comes from a G-Kisin module $(\mathfrak{P}_A, \phi_A)$ over A of type μ with μ minuscule, then there exists a canonical extension $\tilde{\rho} : \Gamma_K \to G(A)$ and, furthermore, if A is flat over $\mathbb{Z}_p$ then $\tilde{\rho}[1/p]$ is crystalline. This is rough in the sense that what we actually prove is an isomorphism of certain deformation functors. As a consequence, we get that the local structure of $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ at a point $(\mathfrak{P}_{\mathbb{F}'}, \phi_{\mathbb{F}'}) \in X_{\bar{\eta}}^{\mathrm{cris},\mu}(\mathbb{F}')$ is smoothly equivalent to the deformation groupoid $D^{\mu}_{\mathfrak{P}_{\mathbb{F}'}}$ of $\mathfrak{P}_{\mathbb{F}'}$ with type μ.

To prove Theorem 4.4.1, one studies the geometry of $D^{\mu}_{\mathfrak{P}_{\mathbb{F}'}}$. Here, the key input comes from the theory of local models of Shimura varieties. A *local model* is a projective scheme X over the ring of integers of a p-adic field F such that X is supposed to étale-locally model the integral structure of a Shimura variety. Classically, local models were built out of moduli spaces of linear algebra structures. Rapoport and Zink [1996] formalized the theory of local models for Shimura varieties of PEL type. Subsequent refinements of these local models were studied mostly on a case by case basis by Faltings, Görtz, Haines, Pappas, and Rapoport, among others.

Pappas and Zhu [2013] define, for any triple (G, P, μ), where G is a reductive group over F (which splits over a tame extension), P is a parahoric subgroup, and μ is any cocharacter of G, a local model $M(\mu)$ over the ring of integers of the reflex field of μ. Their construction, unlike previous constructions, is purely group-theoretic, i.e., it does not rely on any particular representation of G. They build their local models inside degenerations of affine Grassmannians extending constructions of Beilinson, Drinfeld, Gaitsgory, and Zhu to mixed characteristic. The geometric fact we will use is that $M(\mu)$ is normal with special fiber reduced [Pappas and Zhu 2013, Theorem 0.1].

The significance of local models in this paper is that the singularities of $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ are smoothly equivalent to those of a local model $M(\mu)$ for the Weil-restricted group $\mathrm{Res}_{(K \otimes_{\mathbb{Q}_p} F)/F} G_F$. This equivalence comes from a diagram of formally smooth morphisms (3-3-9-2):

$$\begin{array}{ccc} & \widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} & \\ \swarrow & & \searrow \\ D^{\mu}_{\mathfrak{P}_{\mathbb{F}}} & & \overline{D}^{\mu}_{Q_{\mathbb{F}}}, \end{array} \qquad (1\text{-}1\text{-}2\text{-}1)$$

which generalizes constructions from [Kisin 2009, Proposition 2.2.11; Pappas and Rapoport 2009, §3]. The deformation functor $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$ is represented by the completed local ring at an $\mathbb{F}$-point of $M(\mu)$. Intuitively, the above modification corresponds to adding a trivialization to the G-Kisin module and then taking the "image of Frobenius". We construct the diagram (1-1-2-1) in Section 3 with no assumptions on the cocharacter μ (to be precise, $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ is deformations of type less than or equal to μ in general). It is intriguing to wonder whether $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ and diagram (1-1-2-1) have any relevance to studying higher-weight Galois deformation rings, i.e., when μ is not minuscule.

As a remark, we usually cannot apply [Pappas and Zhu 2013] directly, since the group $\mathrm{Res}_{(K\otimes_{\mathbb{Q}_p} F)/F}\, G$ will generally not split over a tame extension. In [Levin 2013], we develop a theory of local models following Pappas and Zhu's approach but adapted to these Weil-restricted groups (for maximal special parahoric level). These results are reviewed in Section 3.2 and are studied in more generality in [Levin 2014].

We now a give brief outline of the article. In Section 2, we define and develop the theory of G-Kisin modules and construct resolutions of semistable and crystalline G-valued deformation rings (Propositions 2.3.3 and 2.3.9). This closely follows the approach of [Kisin 2008]. The proof that "semistable implies finite height" (Proposition 2.3.13) requires an extra argument not present in the GL_n case (Lemma 2.3.6). In Section 3, we study the relationship between deformations of G-Kisin modules and local models. We construct the big diagram (Theorem 3.3.3) and then impose the μ-type condition to arrive at the diagram (3-3-9-2). We also give an initial description of the local structure of $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ in Corollary 3.3.15. Section 4.2 develops the theory of $(\varphi, \widehat{\Gamma})$-modules with G-structure and Section 4.3 is devoted to the proof of our key result (Theorem 4.3.6) in integral p-adic Hodge theory. In the last section, Section 4.4, we prove Theorems 4.4.1 and 4.4.6, which follow relatively formally from the results of Sections 3.3 and 4.3.

1.2. ***Notations and conventions.*** We take F to be our coefficient field, a finite extension of $\mathbb{Q}_p$. Let Λ be the ring of integers of F with residue field $\mathbb{F}$. Let G be a reductive group scheme over Λ with connected fibers and ${}^f\mathrm{Rep}_{\Lambda}(G)$ the category of representations of G on finite free Λ-modules. We will use V to denote a fixed faithful representation of G, i.e., $V \in {}^f\mathrm{Rep}_{\Lambda}(G)$ such that $G \to \mathrm{GL}(V)$ is a closed immersion. The derived subgroup of G will be denoted by G^{der} and its adjoint quotient by G^{ad}.

All G-bundles will be with respect to the fppf topology. If X is a Λ-scheme, then $\mathrm{GBun}(X)$ will denote the category of G-bundles on X. We will denote the trivial G-bundle by $\mathscr{E}^0$. For any G-bundle P on a Λ-scheme X and any $W \in {}^f\mathrm{Rep}_{\Lambda}(G)$, $P(W)$ will denote the pushout of P with respect to W (see the discussion before Theorem 2.1.1). Let $\overline{F}$ be an algebraic closure of F. For a linear algebraic F-group H, $X_*(H)$ will denote the group $\mathrm{Hom}(\mathbb{G}_{\mathrm{m}}, H_{\overline{F}})$ of geometric cocharacters. For $\mu \in X_*(H)$, $[\mu]$ will denote its conjugacy class. The reflex field $F_{[\mu]}$ of $[\mu]$ is the smallest subfield of $\overline{F}$ over which the conjugacy class $[\mu]$ is defined.

If Γ is a profinite group and B is a finite Λ-algebra, then ${}^f\mathrm{Rep}_B(\Gamma)$ will be the category of continuous representations of Γ on finite projective B-modules where B is given the p-adic topology. More generally, $\mathrm{GRep}_B(\Gamma)$ will denote the category of pairs (P, η) where P is a G-bundle over Spec B and $\eta : \Gamma \to \mathrm{Aut}_G(P)$ is a continuous homomorphism.

Let K be a p-adic field with ring of integers $\mathbb{O}_K$ and residue field k. Denote its absolute Galois group by Γ_K. We furthermore take $W := W(k)$ and $K_0 := W[1/p]$. We fix a uniformizer π of K and let $E(u)$ the minimal polynomial of π over K_0. Our convention will be to work with covariant p-adic Hodge theory functors, so we take the p-adic cyclotomic character to have Hodge–Tate weight -1.

For any local ring R, we let m_R denote the maximal ideal. We will denote the completion of B with respect to a specified topology by $\widehat{B}$.

2. Kisin modules with G-structure

In this section, we construct resolutions of Galois deformation rings by moduli spaces of Kisin modules (i.e., $\mathfrak{S}$-modules) with G-structure. For GL_n, this technique was introduced in [Kisin 2009] to study flat deformation rings. In [Kisin 2008], the same technique is used to construct potentially semistable deformation rings for GL_n. Here we develop a theory of G-Kisin modules (Definition 2.2.7). In particular, in Section 2.4, we show the existence of a universal G-Kisin module over these deformation rings (Theorem 2.4.2) and relate the filtration defined by a G-Kisin module to p-adic Hodge type. One can construct G-valued semistable and crystalline deformation rings with fixed p-adic Hodge type without G-Kisin modules [Balaji 2012]. However, the existence of a resolution by a moduli space of Kisin modules allows for finer analysis of the deformation rings; see Section 4.

2.1. ***Background on G-bundles.*** All bundles will be for the fppf topology. For any G-bundle P on a Λ-scheme X and any $W \in {}^f\mathrm{Rep}_\Lambda(G)$, define

$$P(W) := P \times^G W = (P \times W)/\sim$$

to be the pushout of P with respect to W. This is a vector bundle on X. This defines a functor from ${}^f\mathrm{Rep}_\Lambda(G)$ to the category Vec_X of vector bundles on X.

Theorem 2.1.1. *Let G be a flat affine group scheme of finite type over* Spec Λ *with connected fibers. Let X be a Λ-scheme. The functor $P \mapsto \{P(W)\}$ from the category of G-bundles on X to the category of fiber functors* (*i.e., faithful exact tensor functors*) *from ${}^f\mathrm{Rep}_\Lambda(G)$ to* Vec_X *is an equivalence of categories.*

Proof. When the base is a field, this is a well-known result [Deligne and Milne 1982, Theorem 3.2] in Tannakian theory. When the base is a Dedekind domain, see [Broshi 2013, Theorem 4.8] or [Levin 2013, Theorem 2.5.2]. □

We will also need the following gluing lemma for G-bundles:

Lemma 2.1.2. *Let B be any Λ-algebra. Let $f \in B$ be a non-zero-divisor and G be a flat affine group scheme of finite type over Λ. The category of triples $(P_f, \widehat{P}, \alpha)$, where $P_f \in \mathrm{GBun}(\mathrm{Spec}\, B_f)$, $\widehat{P} \in \mathrm{GBun}(\mathrm{Spec}\, \widehat{B})$, and α is an isomorphism between P_f and $\widehat{P}$ over $\mathrm{Spec}\, \widehat{B}_f$, is equivalent to the category of G-bundles on B.*

Proof. This is a generalization of the Beauville–Laszlo formal gluing lemma for vector bundles. See [Pappas and Zhu 2013, Lemma 5.1] or [Levin 2013, Theorem 3.1.8]. □

Let $i : H \subset G$ be a flat closed Λ-subgroup. We are interested in the "fibers" of the pushout map

$$i_* : \mathrm{HBun} \to \mathrm{GBun}$$

carrying an H-bundle Y to the G-bundle $Y \times^H G$. Let Q be a G-bundle on a Λ-scheme S. For any S-scheme X, define $\mathrm{Fib}_Q(X)$ to be the category of pairs (P, α), where $P \in \mathrm{HBun}(X)$ and $\alpha : i_*(P) \cong Q_X$ is an isomorphism in $\mathrm{GBun}(X)$. A morphism $(P, \alpha) \to (P', \alpha')$ is a map $f : P \to P'$ of H-bundles such that $\alpha' \circ i_*(f) \circ \alpha^{-1}$ is the identity.

Proposition 2.1.3. *The category $\mathrm{Fib}_Q(X)$ has no nontrivial automorphisms for any S-scheme X. Furthermore, the underlying functor $|\mathrm{Fib}_Q|$ is represented by the pushout $Q \times^G (G/H)$. In particular, if G/H is affine (resp. quasiaffine) over S then $|\mathrm{Fib}_Q|$ is affine (resp. quasiaffine) over X.*

Proof. See [Serre 1958, Proposition 9] or [Levin 2013, Lemma 2.2.3]. □

Proposition 2.1.4. *Let G be a smooth affine group scheme of finite type over* $\mathrm{Spec}\, \Lambda$ *with connected fibers.*

(1) *Let R any Λ-algebra and I a nilpotent ideal of R. For any G-bundle P on* $\mathrm{Spec}\, R$, *P is trivial if and only if $P \otimes_R R/I$ is trivial.*

(2) *Let R be any complete local Λ-algebra with finite residue field. Any G-bundle on* $\mathrm{Spec}\, R$ *is trivial.*

Proof. For (1), because G is smooth, P is also smooth. Thus, $P(R) \to P(R/I)$ is surjective. A G-bundle is trivial if and only if it admits a section.

Part (2) reduces to the case of $R = \mathbb{F}$ using part (1). Lang's theorem says that $H^1_{\text{ét}}(\mathbb{F}, G)$ is trivial for any smooth connected algebraic group over $\mathbb{F}$ (see [Springer 1998, Theorem 4.4.17]) □

2.2. *Definitions and first properties.* Let K be a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. Set $W := W(k)$ and $K_0 := W[1/p]$. Recall Breuil and Kisin's ring $\mathfrak{S} := W[\![u]\!]$ and let $E(u) \in W[u]$ be the Eisenstein polynomial associated to a choice of uniformizer π of K that generates K over K_0. Fix a compatible system $\{\pi^{1/p}, \pi^{1/p^2}, \ldots\}$ of p-power roots of π and let $K_\infty = K(\pi^{1/p}, \pi^{1/p^2}, \ldots)$. Set $\Gamma_\infty := \mathrm{Gal}(\overline{K}/K_\infty)$.

Let $\mathcal{O}_{\mathcal{E}}$ denote the p-adic completion of $\mathfrak{S}[1/u]$. We equip both $\mathcal{O}_{\mathcal{E}}$ and $\mathfrak{S}$ with a Frobenius endomorphism φ defined by taking the ordinary Frobenius lift on W and $u \mapsto u^p$. For any $\mathbb{Z}_p$-algebra B, let $\mathcal{O}_{\mathcal{E},B} := \mathcal{O}_{\mathcal{E}} \otimes_{\mathbb{Z}_p} B$ and $\mathfrak{S}_B := \mathfrak{S} \otimes_{\mathbb{Z}_p} B$. We equip both of these rings with Frobenii having trivial action on B. Note that all tensor products are over $\mathbb{Z}_p$ even though the group G may only be defined over the Λ.

Definition 2.2.1. Let B be any Λ-algebra. For any G-bundle on $\operatorname{Spec} \mathcal{O}_{\mathcal{E},B}$, we let $\varphi^*(P) := P \otimes_{\mathcal{O}_{\mathcal{E},B},\varphi} \mathcal{O}_{\mathcal{E},B}$ be the pullback under Frobenius. An $(\mathcal{O}_{\mathcal{E},B}, \varphi)$*-module with G-structure* is a pair (P, ϕ_P), where P is a G-bundle on $\operatorname{Spec} \mathcal{O}_{\mathcal{E},B}$ and $\phi_P : \varphi^*(P) \cong P$ is an isomorphism. Let $\mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathcal{E},B}}$ be the category of such pairs.

Remark 2.2.2. When $G = \mathrm{GL}_d$, $\mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathcal{E},B}}$ is equivalent to the category of rank-d étale $(\mathcal{O}_{\mathcal{E},B}, \varphi)$-modules via the usual equivalence between GL_d-bundles and rank-d vector bundles.

When B is $\mathbb{Z}_p$-finite and Artinian, the functor T_B defined by

$$T_B(M, \phi) = (M \otimes_{\mathcal{O}_{\mathcal{E}}} \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{un}}}})^{\phi=1}$$

induces an equivalence of categories between étale $(\mathcal{O}_{\mathcal{E},B}, \varphi)$-modules (which are $\mathcal{O}_{\mathcal{E},B}$-projective) and the category of representations of Γ_∞ on finite projective B-modules (see [Kisin 2009, Lemma 1.2.7]). A quasi-inverse is given by

$$\underline{M}_B(V) := (V \otimes_{\mathbb{Z}_p} \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{un}}}})^{\Gamma_\infty}.$$

This equivalence extends to algebras which are finite flat over $\mathbb{Z}_p$.

Definition 2.2.3. For any profinite group Γ and Λ-algebra B, define $\mathrm{GRep}_B(\Gamma)$ to be the category of pairs (P, η) where P is a G-bundle over $\operatorname{Spec} B$ and, with B given the p-adic topology, $\eta : \Gamma \to \mathrm{Aut}_G(P)$ is a continuous homomorphism.

In the G-setting, $\mathrm{GRep}_B(\Gamma)$ will play the role of representation of Γ on finite projective B-modules. We have the following generalization of T_B:

Proposition 2.2.4. *Let B be any Λ-algebra which is $\mathbb{Z}_p$-finite and either Artinian or $\mathbb{Z}_p$-flat. There exists an equivalence of categories*

$$T_{G,B} : \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathcal{E},B}} \to \mathrm{GRep}_B(\Gamma_\infty)$$

with a quasi-inverse $\underline{M}_{G,B}$. Furthermore, for any finite map $B \to B'$ and any $(P, \phi_P) \in \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathcal{E},B}}$, there is a natural isomorphism

$$T_{G,B'}(P \otimes_B B') \cong T_{G,B}(P) \otimes_B B'.$$

Proof. Using Theorem 2.1.1, we can give Tannakian interpretations of $\mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathcal{E},B}}$ and $\mathrm{GRep}_B(\Gamma_\infty)$. The former is equivalent to the category

$$[{}^f\operatorname{Rep}_\Lambda(G), \mathrm{Mod}^{\varphi,\text{ét}}_{\mathcal{O}_{\mathcal{E},B}}]^{\otimes}$$

of faithful exact tensor functors. The latter is equivalent to the category of faithful exact tensor functors from ${}^f\operatorname{Rep}_\Lambda(G)$ to ${}^f\operatorname{Rep}_B(\Gamma_\infty)$. We define $T_{G,B}(P,\phi_P)$ to be the functor which assigns to any $W \in {}^f\operatorname{Rep}_\Lambda(G)$ the Γ_∞-representation $T_B(P(W),\phi_{P(W)})$. This is an object of $\operatorname{GRep}_B(\Gamma_\infty)$ because T_B is a tensor exact functor (see [Broshi 2008, Lemma 3.4.1.6] or [Levin 2013, Theorem 4.1.3]). Similarly, one can define $\underline{M}_{G,B}$ which is quasi-inverse to $T_{G,B}$. Compatibility with extending the coefficients follows from [Kisin 2009, Lemma 1.2.7(3)]. □

Definition 2.2.5. Let B be any $\mathbb{Z}_p$-algebra. A *Kisin module with bounded height* over B is a finitely generated projective $\mathfrak{S}_B$-module $\mathfrak{M}_B$ together with an isomorphism $\phi_{\mathfrak{M}_B} : \varphi^*(\mathfrak{M}_B)[1/E(u)] \cong \mathfrak{M}_B[1/E(u)]$. We say that $(\mathfrak{M}_B, \phi_{\mathfrak{M}_B})$ has *height in* $[a,b]$ if

$$E(u)^a\mathfrak{M}_B \supset \phi_{\mathfrak{M}_B}(\varphi^*(\mathfrak{M}_B)) \supset E(u)^b\mathfrak{M}_B$$

as submodules of $\mathfrak{M}_B[1/E(u)]$.

Let $\operatorname{Mod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B}$ (resp. $\operatorname{Mod}^{\varphi,[a,b]}_{\mathfrak{S}_B}$) be the category of Kisin modules with bounded height (resp. height in $[a,b]$) with morphisms being $\mathfrak{S}_B$-module maps respecting Frobenii. Then $\operatorname{Mod}^{\varphi,[0,h]}_{\mathfrak{S}_B}$ is the usual category of Kisin modules with height at most h, as in [Brinon and Conrad 2009; Kisin 2006; 2009].

Example 2.2.6. Let $\mathfrak{S}(1)$ be the Kisin module whose underlying module is $\mathfrak{S}$ and whose Frobenius is given by $c_0^{-1}E(u)\varphi_{\mathfrak{S}}$ where $E(0) = c_0 p$. For any $\mathbb{Z}_p$-algebra, we define $\mathfrak{S}_B(1)$ by base change from $\mathbb{Z}_p$ and define $\mathcal{O}_{\mathcal{E},B}(1) := \mathfrak{S}_B(1) \otimes_{\mathfrak{S}_B} \mathcal{O}_{\mathcal{E},B}$, an étale $(\mathcal{O}_{\mathcal{E},B},\varphi)$-module.

In order to reduce to the effective case (height in $[0,h]$), it is often useful to "twist" by tensoring with $\mathfrak{S}_B(1)$. For any $\mathfrak{M}_B \in \operatorname{Mod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B}$ and any $n \in \mathbb{Z}$, define $\mathfrak{M}_B(n)$ by n-fold tensor product with $\mathfrak{S}_B(1)$ (negative n being tensoring with the dual). It is not hard to see that if $\mathfrak{M}_B \in \operatorname{Mod}^{\varphi,[a,b]}_{\mathfrak{S}_B}$ then $\mathfrak{M}_B(n) \in \operatorname{Mod}^{\varphi,[a+n,b+n]}_{\mathfrak{S}_B}$.

Definition 2.2.7. Let B be any Λ-algebra. A *G-Kisin module* over B is a pair $(\mathfrak{P}_B, \phi_{\mathfrak{P}_B})$, where $\mathfrak{P}_B$ is a G-bundle on $\mathfrak{S}_B$ and

$$\phi_{\mathfrak{P}_B} : \varphi^*(\mathfrak{P}_B)[1/E(u)] \cong \mathfrak{P}_B[1/E(u)]$$

is an isomorphism of G-bundles. Denote the category of such objects by $\operatorname{GMod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B}$.

Remark 2.2.8. Unlike the Kisin module for GL_n, G-bundles do not have endomorphisms. Additionally, there is no reasonable notion of effective G-Kisin module. The Frobenius on a G-Kisin module is only ever defined after inverting $E(u)$. Later, we use auxiliary representations of G to impose height conditions.

The category $\operatorname{Mod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B}$ is a tensor exact category, where a sequence of Kisin modules

$$0 \to \mathfrak{M}'_B \to \mathfrak{M}_B \to \mathfrak{M}''_B \to 0$$

is *exact* if the underlying sequence of $\mathfrak{S}_B$-modules is exact. For any representation $W \in {}^f\mathrm{Rep}_\Lambda(G)$, the pushout $(\mathfrak{P}_B(W), \phi_{\mathfrak{P}_B}(W))$ is a Kisin module with bounded height. Using Theorem 2.1.1, one can interpret $\mathrm{GMod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B}$ as the category of faithful exact tensor functors from ${}^f\mathrm{Rep}_\Lambda(G)$ to $\mathrm{Mod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B}$.

Since $E(u)$ is invertible in $\mathcal{O}_{\mathscr{E}}$, there is a natural map $\mathfrak{S}_B[1/E(u)] \to \mathcal{O}_{\mathscr{E},B}$ for any $\mathbb{Z}_p$-algebra B. This induces a functor

$$\Upsilon_G : \mathrm{GMod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B} \to \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathscr{E},B}}$$

for any Λ-algebra B.

Definition 2.2.9. Let B be any Λ-algebra and let $P_B \in \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathscr{E},B}}$. A *$G$-Kisin lattice of P_B* is a pair $(\mathfrak{P}_B, \alpha)$ where $\mathfrak{P}_B \in \mathrm{GMod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B}$ and $\alpha : \Upsilon_G(\mathfrak{P}_B) \cong P_B$ is an isomorphism.

From the Tannakian perspective, a G-Kisin lattice of P is equivalent to Kisin lattices $\mathfrak{M}_W$ in $P(W)$ for each $W \in {}^f\mathrm{Rep}_\Lambda(G)$ functorial in W and compatible with tensor products. Furthermore, we have the following, which says that the bounded height condition can be checked on a single faithful representation.

Proposition 2.2.10. *Let $P_B \in \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathscr{E},B}}$. A G-Kisin lattice of P_B is equivalent to an extension $\mathfrak{P}_B$ of the bundle P_B to* $\mathrm{Spec}\,\mathfrak{S}_B$ *such that, for a single faithful representation $V \in {}^f\mathrm{Rep}_\Lambda(G)$,*

$$\mathfrak{P}_B(V) \subset P_B(V)$$

is a Kisin lattice of bounded height.

Proof. The only claim which does not follow from unwinding definitions is that, if we have an extension $\mathfrak{P}_B$ such that $\mathfrak{P}_B(V) \subset P_B(V)$ is a Kisin lattice for a single faithful representation V, then $\mathfrak{P}_B(W) \subset P_B(W)$ is a Kisin lattice for all representations W of G.

By [Levin 2013, Theorem C.1.7], any $W \in {}^f\mathrm{Rep}_\Lambda(G)$ can be written as a subquotient of direct sums of tensor products of V and the dual of V. It suffices then to prove that bounded height is stable under duals, tensor products, quotients, and saturated subrepresentations.

Duals and tensor products are easy to check. For subquotients, let

$$0 \to M_B \to N_B \to L_B \to 0$$

be an exact sequence of étale $(\mathcal{O}_{\mathscr{E},B}, \varphi)$-modules. Suppose that the sequence is induced by an exact sequence

$$0 \to \mathfrak{M}_B \to \mathfrak{N}_B \to \mathfrak{L}_B \to 0$$

of projective $\mathfrak{S}_B$-lattices. Assume $\mathfrak{N}_B$ has bounded height with respect to ϕ_{N_B}. By twisting, we can assume $\mathfrak{N}_B$ has height in $[0, h]$.

Since $\mathfrak{M}_B = M_B \cap \mathfrak{N}_B$, $\mathfrak{M}_B$ is ϕ_{M_B}-stable. Similarly, $\mathfrak{L}_B$ is ϕ_{L_B}-stable. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \varphi^*(\mathfrak{M}_B) & \longrightarrow & \varphi^*(\mathfrak{N}_B) & \longrightarrow & \varphi^*(\mathfrak{L}_B) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_{M_B}} & & \downarrow{\scriptstyle \phi_{N_B}} & & \downarrow{\scriptstyle \phi_{L_B}} & & \\ 0 & \longrightarrow & \mathfrak{M}_B & \longrightarrow & \mathfrak{N}_B & \longrightarrow & \mathfrak{L}_B & \longrightarrow & 0. \end{array}$$

All the linearizations are injective because they are isomorphisms at the level of $\mathcal{O}_{\mathscr{E},B}$-modules. By the snake lemma, the sequence of cokernels is exact. If $E(u)^h$ kills $\mathrm{Coker}(\phi_{N_B})$, then it kills $\mathrm{Coker}(\phi_{M_B})$ and $\mathrm{Coker}(\phi_{P_B})$ as well. Thus, $\mathfrak{M}_B$ and $\mathfrak{P}_B$ both have height in $[0, h]$ whenever $\mathfrak{N}_B$ does. □

Definition 2.2.11. For any B as in Proposition 2.2.4, define

$$T_{G,\mathfrak{S}_B} : \mathrm{GMod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B} \to \mathrm{GRep}_B(\Gamma_\infty)$$

to be the composition $T_{G,\mathfrak{S}_B} := T_{G,B} \circ \Upsilon_G$.

We end this section with an important full faithfulness result:

Proposition 2.2.12. *Assume B is finite flat over Λ. Then the natural extension map*

$$\Upsilon_G : \mathrm{GMod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_B} \to \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathscr{E},B}}$$

is fully faithful.

Proof. This follows from the full faithfulness of Υ_{GL_n} for all $n \geq 1$ by considering a faithful representation of G. When $B = \mathbb{Z}_p$, this is [Brinon and Conrad 2009, Proposition 11.2.7]. One can reduce to this case by forgetting coefficients, since any finitely generated projective $\mathfrak{S}_B$-module is finite free over $\mathfrak{S}$. □

2.3. ***Resolutions of G-valued deformations rings.*** Fix a faithful representation V of G over Λ and integers a, b with $a \leq b$. We will use V and a, b to impose finiteness conditions on our moduli space.

Definition 2.3.1. Let B be any Λ-algebra. We say that a G-Kisin lattice $\mathfrak{P}_B$ in $(P_B, \phi_{P_B}) \in \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathscr{E},B}}$ has *height in* $[a, b]$ if $\mathfrak{P}_B(V)$ in $P_B(V)$ has height in $[a, b]$.

For any finite local Artinian Λ-algebra A and any $(P_A, \phi_{P_A}) \in \mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathscr{E},A}}$, consider the moduli problem over $\mathrm{Spec}\, A$, for any A-algebra B,

$$X^{[a,b]}_{P_A}(B) := \{G\text{-Kisin lattices in } P_A \otimes_{\mathcal{O}_{\mathscr{E},A}} \mathcal{O}_{\mathscr{E},B} \text{ with height in } [a,b]\}/\cong.$$

Theorem 2.3.2. *Assume that P_A is a trivial bundle over* $\mathrm{Spec}\, \mathcal{O}_{\mathscr{E},A}$. *The functor $X^{[a,b]}_{P_A}$ is represented by a closed finite-type subscheme of the affine Grassmannian* $\mathrm{Gr}_{G'}$ *over* $\mathrm{Spec}\, A$, *where G' is the Weil restriction* $\mathrm{Res}_{(W \otimes_{\mathbb{Z}_p} \Lambda)/\Lambda} G$.

Proof. By Proposition 2.2.10, $X_{P_A}^{[a,b]}(B)$ is the set of bundles over $\mathfrak{S}_B$ extending $P_B := P_A \otimes_{\mathcal{O}_{\mathcal{E},A}} \mathcal{O}_{\mathcal{E},B}$ with height in $[a,b]$ with respect to V. We want to identify this set with a subset of $\mathrm{Gr}_{G'}(B)$.

Consider the diagram

$$\begin{array}{ccc} \mathfrak{S} \otimes_{\mathbb{Z}_p} B & \longrightarrow & (W \otimes_{\mathbb{Z}_p} B)[\![u]\!] \\ \downarrow & & \downarrow \\ \mathcal{O}_{\mathcal{E},B} & \longrightarrow & (W \otimes_{\mathbb{Z}_p} B)((u)), \end{array}$$

where the vertical arrows are localization at u and the top horizontal arrow is u-adic completion. The Beauville–Laszlo gluing lemma, Lemma 2.1.2, says that the set of extensions of P_B to $\mathfrak{S}_B$ is in bijection with the set of extensions of $\widehat{P}_B$ to $W_B[\![u]\!]$, where $\widehat{P}_B$ is the u-adic completion. This second set is in bijection with the B-points of the Weil restriction $\mathrm{Res}_{(W \otimes_{\mathbb{Z}_p} \Lambda)/\Lambda} \mathrm{Gr}_G$, which is isomorphic to $\mathrm{Gr}_{G'}$ by [Richarz 2015, Lemma 1.16] or [Levin 2013, Proposition 3.4.2].

Set $M_A := P_A(V)$. By [Kisin 2008, Proposition 1.3], the functor $X_{M_A}^{[a,b]}$ of Kisin lattices in M_A with height in $[a,b]$ is represented by a closed subscheme of $\mathrm{Gr}_{\mathrm{Res}_{(W \otimes_{\mathbb{Z}_p} \Lambda)/\Lambda} \mathrm{GL}(V)}$. Evaluation at V induces a map of functors

$$X_{P_A}^{[a,b]} \to X_{M_A}^{[a,b]}. \tag{2-3-2-1}$$

By Proposition 2.2.10, the subset $X_{P_A}^{[a,b]}(B) \subset \mathrm{Gr}_{G'}(B)$ is exactly the preimage of $X_{M_A}^{[a,b]}(B)$. □

We now extend the construction beyond the Artinian setting by passing to the limit. Let R be a complete local Noetherian Λ-algebra with residue field $\mathbb{F}$. Let $\eta : \Gamma_\infty \to G(R)$ be a continuous representation.

Proposition 2.3.3. *For any $n \geq 1$, let $\eta_n : \Gamma_\infty \to G(R/m_R^n)$ denote the reduction modulo m_R^n. From $\{\eta_n\}$, we construct a system $\underline{M}_{G,R/m_R^n}(\eta_n) =: (P_{\eta_n}, \phi_n)$ in $\mathrm{GMod}^{\varphi}_{\mathcal{O}_{\mathcal{E},R/m_R^n}}$. Assume that P_{η_1} is a trivial G-bundle. There exists a projective R-scheme*

$$\Theta : X_\eta^{[a,b]} \to \operatorname{Spec} R$$

whose reduction modulo m_R^n is $X_{P_{\eta_n}}^{[a,b]}$ for any $n \geq 1$.

Proof. By Proposition 2.2.4, there are natural isomorphisms

$$P_{\eta_{n+1}} \otimes_{\mathcal{O}_{\mathcal{E},R/m_R^{n+1}}} \mathcal{O}_{\mathcal{E},R/m_R^n} \cong P_{\eta_n}$$

for all $n \geq 1$. Since P_{η_1} is a trivial G-bundle, all P_{η_n} are trivial, by Proposition 2.1.4(1), so we can apply Theorem 2.3.2. Consider then the system

$$\{X_{P_{\eta_n}}^{[a,b]}\}$$

of schemes over $\{R/m_R^n\}$. Since G' is reductive, the affine Grassmannian $\mathrm{Gr}_{G'}$ is ind-projective [Levin 2013, Theorem 3.3.11]. In particular, any ample line bundle on $\mathrm{Gr}_{G'}$ will restrict to a compatible system of ample line bundles on $\{X_{P_{\eta_n}}^{[a,b]}\}$. By formal GAGA [EGA III_1 1961, Théorème (5.4.5)], there exists a projective R-scheme $X_\eta^{[a,b]}$ whose reductions modulo m_R^n are $X_{P_{\eta_n}}^{[a,b]}$. □

Remark 2.3.4. Unlike for GL_n, there are nontrivial G-bundles over $\operatorname{Spec} \mathbb{F}((u))$, which is why we need the assumption in Proposition 2.3.3. If P_{η_1} admits any G-Kisin lattice $\mathfrak{P}_{\eta_1}$, then by Proposition 2.1.4(2) the G-bundle $\mathfrak{P}_{\eta_1}$ is trivial, since $\mathfrak{S}_{\mathbb{F}}$ is a semilocal ring with finite residue fields. Thus, the assumption in Proposition 2.3.3 is natural if you are interested in studying Γ_∞-representations of finite height. By Steinberg's theorem, one can always make P_{η_1} trivial by passing to a finite extension $\mathbb{F}'$ of $\mathbb{F}$.

We record for reference the following compatibility with base change:

Proposition 2.3.5. *Let $f : R \to S$ be a local map of complete local Noetherian Λ-algebras with finite residue fields of characteristic p. Let η_S be the induced map $\Gamma_\infty \to G(S)$. Then there is a natural map $f' : X_{\eta_S}^{[a,b]} \to X_\eta^{[a,b]}$ which makes the following diagram Cartesian*:

$$\begin{array}{ccc} X_{\eta_S}^{[a,b]} & \xrightarrow{f'} & X_\eta^{[a,b]} \\ \downarrow & & \downarrow \\ \operatorname{Spec} S & \xrightarrow{f} & \operatorname{Spec} R. \end{array}$$

In particular, *if $R \to S$ is surjective then f' is a closed immersion.*

We will now study the projective F-morphism

$$\Theta[1/p] : X_\eta^{[a,b]}[1/p] \to \operatorname{Spec} R[1/p].$$

We show it is a *closed immersion* (this is essentially a consequence of Proposition 2.2.12) and that the closed points of the image are G-valued representations with height in $[a, b]$ in a suitable sense; see Proposition 2.3.9. Next, we show that, if η is the restriction of $\eta' : \Gamma_K \to G(R)$, then the image of $\Theta[1/p]$ contains all semistable representations with $\eta'(V)$ having Hodge–Tate weights in $[a, b]$. These are generalizations of results from [Kisin 2008].

The following lemma will be useful at several key points:

Lemma 2.3.6 (extension lemma). *Let G be a smooth affine group scheme over Λ. Let C be a finite flat Λ-algebra and let U be the open complement of the finite set of closed points of* $\operatorname{Spec} \mathfrak{S}_C$.

(1) *There is an equivalence of categories between G-bundles Q on U and the category of triples* $(\mathfrak{P}^*, P, \gamma)$ *where* $\mathfrak{P}^*$ *is a G-bundle on* $\operatorname{Spec} \mathfrak{S}_C[1/p]$, *$P$ is a G-bundle on* $\operatorname{Spec} \mathbb{O}_{\mathscr{E},C}$, *and γ is an isomorphism of their restrictions to* $\operatorname{Spec} \mathbb{O}_{\mathscr{E},C}[1/p]$.

(2) *Assume G is a reductive group scheme with connected fibers. Let V be a faithful representation of G over Λ. If Q is a G-bundle on U such that the locally free coherent sheaf $Q(V)$ on U extends to a projective $\mathfrak{S}_C$-module $\mathfrak{M}_C$, then there exists a unique* (*up to unique isomorphism*) *G-bundle $\widetilde{Q}$ over* $\operatorname{Spec} \mathfrak{S}_C$ *such that $\widetilde{Q}|_U \cong Q$ and $\widetilde{Q}(V) = \mathfrak{M}_C$.*

Proof. Note that we can write U as the union of $\operatorname{Spec} \mathfrak{S}_C[1/u]$ and $\operatorname{Spec} \mathfrak{S}_C[1/p]$. Recall also that $\mathbb{O}_{\mathscr{E},C}$ is the p-adic completion of $\mathfrak{S}_C[1/u]$. Since p is a non-zero-divisor in $\mathfrak{S}_C[1/u]$, we can apply the gluing lemma, Lemma 2.1.2, to P and $\mathfrak{P}^*[1/u]$ to construct a G-bundle Q' on $\operatorname{Spec} \mathfrak{S}_C[1/u]$ which, by construction, is isomorphic to $\mathfrak{P}^*$ along $\operatorname{Spec} \mathfrak{S}_C[1/u, 1/p]$. The G-bundles $\mathfrak{P}^*$ and Q' glue to give a bundle Q over U. Each step in the construction is a categorical equivalence.

For part (2), consider the functor $|\mathrm{Fib}_{\mathfrak{M}_C}|$, which by Proposition 2.1.3 and [Levin 2013, Theorem C.2.5] is represented by an affine scheme Y. $\mathfrak{M}_C$ defines a U-point of $\mathrm{Fib}_{\mathfrak{M}_C}$. Since $\Gamma(U, \mathbb{O}_U) = \mathfrak{S}_C$, we deduce that

$$\operatorname{Hom}_{\mathfrak{S}_C}(\operatorname{Spec} \mathfrak{S}_C, \mathrm{Fib}_{\mathfrak{M}_C}) = \operatorname{Hom}_{\mathfrak{S}_C}(U, \mathrm{Fib}_{\mathfrak{M}_C}).$$

A $\mathfrak{S}_C$-point of $\mathrm{Fib}_{\mathfrak{M}_C}$ is exactly a bundle $\widetilde{Q}$ extending Q and mapping to $\mathfrak{M}_C$.

A similar argument, using that the Isom-scheme between G-bundles is representable by an affine scheme, shows that if an extension exists it is unique up to unique isomorphism (without any reductivity hypotheses). □

Let B be any finite local F-algebra with residue field F'. Define B^0 to be the subring of elements which map to $\mathbb{O}_{F'}$ modulo the maximal ideal of B. Let Int_B denote the set of finitely generated $\mathbb{O}_{F'}$-subalgebras C of B^0 such that $C[1/p] = B$.

Definition 2.3.7. A continuous homomorphism $\eta : \Gamma_\infty \to G(B)$ has *bounded height* if there exists a $C \in \mathrm{Int}_B$ and $g \in G(B)$ such that

(1) $\eta'_C := g\eta g^{-1}$ factors through $G(C)$;

(2) $\underline{M}_{G,C}(\eta'_C) \in \mathrm{GMod}^{\varphi}_{\mathbb{O}_{\mathscr{E},C}}$ admits a G-Kisin lattice of bounded height.

We define *height in* $[a, b]$ with respect to the chosen faithful representation V by replacing bounded height in (2) with height in $[a, b]$.

Lemma 2.3.8. *Let B be a finite local $\mathbb{Q}_p$-algebra and choose $C \in \mathrm{Int}_B$ and $M_C \in \mathrm{Mod}^{\varphi,ét}_{\mathbb{O}_{\mathscr{E},C}}$. If M_C, considered as an $\mathbb{O}_{\mathscr{E}}$-module, has bounded height* (*resp. height in* $[a, b]$), *then there exists some $C' \supset C$ in Int_B, such that $M_C \otimes_C C'$ has bounded height* (*resp. height in* $[a, b]$).

Proof. This is the main content in the proof of part (2) of Proposition 1.6.4 in [Kisin 2008]. If F' is the residue field of B, then one first constructs a Kisin lattice $\mathfrak{M}_{\mathcal{O}_{F'}}$ in $M_C \otimes_C \mathcal{O}_{F'}$. The Kisin lattice in $M_C \otimes_C C'$ is constructed by lifting $\mathfrak{M}_{\mathcal{O}_{F'}}$ (the extension to C' is required to insure that the lift is ϕ-stable). □

Proposition 2.3.9. *The morphism Θ becomes a closed immersion after inverting p. Furthermore, if* $\operatorname{Spec} R_\eta^{[a,b]} \subset \operatorname{Spec} R$ *is the scheme-theoretic image of Θ, then, for any finite F-algebra B, a Λ-algebra map $x : R \to B$ factors through $R_\eta^{[a,b]}$ if and only if $\eta \otimes_{R,x} B$ has height in $[a, b]$.*

Proof. The map Θ is injective on C-points for any finite flat Λ-algebra C, by Proposition 2.2.12. The proof of the first assertion is then the same as in [Kisin 2008, Proposition 1.6.4].

For the second assertion, say $x : R \to B$ factors through $R_\eta^{[a,b]}$. Because $\Theta[1/p]$ is a closed immersion, $x : R \to B$ comes from a B-point y of $X_\eta^{[a,b]}$. Any such x is induced by $x_C : R \to C$ for some $C \in \operatorname{Int}_B$. By properness of Θ, there exists $y_C \in X_\eta^{[a,b]}(C)$ such that $\Theta(y_C) = x_C$. This implies that $\eta \otimes_{R,x_C} C$ has height in $[a, b]$ as a G-valued representation and hence $\eta \otimes_{R,x} B$ also has height in $[a, b]$ (see Definition 2.3.7).

Now, let $x : R \to B$ be a homomorphism such that $\eta_B := \eta \otimes_{R,x} B$ has height in $[a, b]$ as a G-valued representation. Any homomorphism $R \to B$ factors through some $C \in \operatorname{Int}_B$, so that η_B has image in $G(C)$; call this map η_C. We claim that there exists some $C' \supset C$ in Int_B such that $\eta_{C'} = \eta_C \otimes_C C'$ has height in $[a, b]$ and hence x is in the image of $X_\eta^{[a,b]}(B)$. Essentially, we have to show that if one Galois stable "lattice" in η_B has finite height then all "lattices" do. For GL_n, this is Lemma 2.1.15 in [Kisin 2006]. We invoke the GL_n result below.

Since η_B has height in $[a, b]$, there exists $C' \in \operatorname{Int}_B$ and $g \in G(B)$ such that $\eta' = g\eta_B g^{-1}$ factors through $G(C')$ and has height in $[a, b]$. Enlarging C if necessary, we assume both η_C and η' are valued in $G(C)$. Let $P_\eta := \underline{M}_{G,C}(\eta)$ and $P_{\eta'} := \underline{M}_{G,C}(\eta')$. Then g induces an isomorphism

$$P_{\eta'}[1/p] \cong P_{\eta_C}[1/p].$$

Since $P_{\eta'}$ has a G-Kisin lattice with height in $[a, b]$, we get a bundle $\mathfrak{Q}_C$ over $\mathfrak{S}_C[1/p]$ extending $P_{\eta_C}[1/p]$. By Lemma 2.3.6(1), $P_{\eta'}$ and $\mathfrak{Q}_C$ glue to give a bundle Q_C over the complement of the closed points of $\operatorname{Spec} \mathfrak{S}_C$.

We would like to apply Lemma 2.3.6(2). $P_{\eta_C}(V)$ has height in $[a, b]$ as an $\mathcal{O}_{\mathscr{E}}$-module by [Kisin 2006, Lemma 2.1.15] since it corresponds to a lattice in $\eta_C(V)[1/p] \cong \eta'(V)[1/p]$. By Lemma 2.3.8, there exists $\widetilde{C} \supset C$ in Int_B such that $P_{\eta_C}(V) \otimes_C \widetilde{C}$ has height in $[a, b]$ as an $\mathcal{O}_{\mathscr{E},\widetilde{C}}$-module. Replace C by $\widetilde{C}$. Then, if $\mathfrak{M}_C$ is the unique Kisin lattice in $P_{\eta_C}(V)$, we have

$$\mathfrak{M}'_C[1/p] \cap P_{\eta_C}(V) = \mathfrak{M}_C,$$

where $\mathfrak{M}'_C$ is the unique Kisin lattice in $P_{\eta'}(V)$. This shows that $Q_C(V)$ extends across the closed points, so we can apply Lemma 2.3.6(2) to construct a G-Kisin lattice of P_{η_C}. □

Now, assume that η is the restriction to Γ_∞ of a continuous representation of Γ_K, which we continue to call η. Recall the definition of semistable for a G-valued representation:

Definition 2.3.10. If B is a finite F-algebra, a continuous representation $\eta_B : \Gamma_K \to G_F(B)$ is *semistable* (resp. *crystalline*) if, for all representations W in $\mathrm{Rep}_F(G_F)$, the induced representation $\eta_B(W)$ on $W \otimes_F B$ is semistable (resp. crystalline).

Note that because the semistable and crystalline conditions are stable under tensor products and subquotients, it suffices to check these conditions on a single faithful representation of G_F.

Remark 2.3.11. Since we are working with covariant functors, our convention will be that the cyclotomic character has Hodge–Tate weight -1. This is, unfortunately, opposite to the convention in [Kisin 2008].

The following theorem generalizes [Kisin 2008, Theorem 2.5.5]:

Theorem 2.3.12. *Let R be a complete local Noetherian Λ-algebra with finite residue field and $\eta : \Gamma_K \to G(R)$ a continuous representation. Given any a, b integers with $a < b$, there exists a quotient $R_\eta^{[a,b],\mathrm{st}}$ (resp. $R_\eta^{[a,b],\mathrm{cris}}$) of $R_\eta^{[a,b]}$ with the property that, if B is any finite F-algebra and $x : R \to B$ a map of Λ-algebras, then x factors through $R_\eta^{[a,b],\mathrm{st}}$ (resp. $R_\eta^{[a,b],\mathrm{cris}}$) if and only if $\eta_x : \Gamma_K \to G(B)$ is semistable (resp. crystalline) and $\eta_x(V)$ has Hodge–Tate weights in $[a,b]$.*

Since the semistable and crystalline properties can be checked on a single faithful representation, the quotients $R_{\eta(V)}^{[a,b],\mathrm{st}}$ and $R_{\eta(V)}^{[a,b],\mathrm{cris}}$ of R constructed by applying [Kisin 2008, Theorem 2.5.5] to $\eta(V)$ satisfy the universal property in Theorem 2.3.12 with respect to maps $x : R \to B$, where B is a finite F-algebra. What remains is to show that $R_\eta^{[a,b],\mathrm{st}} := R_{\eta(V)}^{[a,b],\mathrm{st}}$ is a quotient of $R_\eta^{[a,b]}$, i.e., that "semistable implies finite height".

Proposition 2.3.13. *Let R and η be as in* 2.3.12. *For any map $x : R \to B$ with B a finite local F-algebra, if the representation η_x is semistable and $\eta_x(V)$ has Hodge–Tate weights in $[a,b]$, then x factors through $R_\eta^{[a,b]}$.*

Proof. By Lemma 2.3.8, there exists $C \in \mathrm{Int}_B$ such that η_x factors through $\mathrm{GL}(V_C)$, hence $G(C)$, and that $M_C := P_{\eta_x}(V)$ admits a Kisin lattice $\mathfrak{M}_C$ with height in $[a,b]$. By Proposition 2.2.10, it suffices to extend the bundle P_{η_x} to $\mathrm{Spec}\, \mathfrak{S}_C$ such that $\mathfrak{P}_{\eta_x}(V) = \mathfrak{M}_C$.

We will apply Lemma 2.3.6. Consider a candidate fiber functor $\mathfrak{F}_{\eta_x}$ for $\mathfrak{P}_{\eta_x}$ which assigns to any $W \in {}^f\mathrm{Rep}_\Lambda(G)$ the unique Kisin lattice of bounded height in $\mathfrak{M}_W \subset P_{\eta_x}(W) = M_W$ (as an $\mathcal{O}_{\mathscr{E}}$-module, not as an $\mathcal{O}_{\mathscr{E},C'}$-module). Such a lattice exists since $\eta_x(W)$ is semistable. The difficulties are that $\mathfrak{M}_W$ may not be $\mathcal{O}_{\mathscr{E},C'}$-projective and that it is not obvious whether $\mathfrak{F}_{\eta_x}$ is exact. It can happen that a nonexact sequence of $\mathfrak{S}$-modules can map under $T_{\mathfrak{S}}$ to an exact sequence of Γ_∞-representations (see [Liu 2012, Example 2.5.6]).

Let $B = C[1/p]$. By [Kisin 2008, Corollary 1.6.3], $\mathfrak{M}_W[1/p]$ is finite projective over $\mathfrak{S}_C[1/p] = \mathfrak{S}_B$ for all W. We claim furthermore that $\mathfrak{F}_{\eta_x} \otimes_{\mathfrak{S}_C} \mathfrak{S}_B$ is exact. For any exact sequence $0 \to W'' \to W \to W' \to 0$ in ${}^f\mathrm{Rep}_\Lambda(G)$, we have a left-exact sequence

$$0 \to \mathfrak{M}_{W''}[1/p] \to \mathfrak{M}_W[1/p] \to \mathfrak{M}_{W'}[1/p].$$

Exactness on the right follows from [Levin 2013, Lemma 4.2.22] on the behavior of exactness for sequences of $\mathfrak{S}$-modules. Thus, $\mathfrak{F}_{\eta_x} \otimes_{\mathfrak{S}_C} \mathfrak{S}_B$ defines a bundle $\mathfrak{P}_B$ over $\mathfrak{S}_B$. Clearly, $\mathfrak{P}_B \otimes_{\mathfrak{S}_B} \mathcal{O}_{\mathscr{E},B} \cong P_{\eta_x} \otimes_{\mathcal{O}_{\mathscr{E},C}} \mathcal{O}_{\mathscr{E},B}$. By Lemma 2.3.6(1), we get a bundle Q over U such that $Q(W) = \mathfrak{M}_W|_U$. Since $\mathfrak{M}_V$ is a projective $\mathfrak{S}_C$-module by our choice of C, Q extends to a bundle $\widetilde{Q}$ over $\mathfrak{S}_C$ by Lemma 2.3.6(2). □

2.4. ***Universal G-Kisin module and filtrations.*** For this section, we make a small change in notation. Let R_0 be a complete local Noetherian Λ-algebra with finite residue field and let $R = R_0[1/p]$.

Define $\widehat{\mathfrak{S}}_{R_0}$ to be the m_{R_0}-adic completion of $\mathfrak{S} \otimes_{\mathbb{Z}_p} R_0$. The Frobenius on $\mathfrak{S} \otimes_{\mathbb{Z}_p} R_0$ extends to a Frobenius on $\widehat{\mathfrak{S}}_{R_0}$.

Definition 2.4.1. A $(\widehat{\mathfrak{S}}_{R_0}[1/p], \varphi)$-module of *bounded height* is a finitely generated projective $\widehat{\mathfrak{S}}_{R_0}[1/p]$-module $\mathfrak{M}_R$ together with an isomorphism

$$\phi_R : \varphi^*(\mathfrak{M}_R)[1/E(u)] \cong \mathfrak{M}_R[1/E(u)].$$

Let $\eta : \Gamma_\infty \to G(R_0)$ be continuous representation. If $\widehat{\mathcal{O}}_{\mathscr{E},R_0}$ is the m_{R_0}-adic completion of $\mathcal{O}_{\mathscr{E},R_0}$, then the inverse limit $\varprojlim \underline{M}_{G,R_0/m_{R_0}^n}(\eta_n)$ defines a pair (P_η, ϕ_η) over $\widehat{\mathcal{O}}_{\mathscr{E},R_0}$ [Levin 2013, Corollary 2.3.5]. Assume $R_0 = R_{0,\eta}^{[a,b]}$. For any finite F-algebra B and any homomorphism $x : R_0 \to B$, there is a unique G-Kisin lattice in $P_\eta \otimes_{\widehat{\mathcal{O}}_{\mathscr{E},R_0},x} \mathcal{O}_{\mathscr{E},B}$ by Proposition 2.2.12; call it $(\mathfrak{P}_x, \phi_x)$. In the following theorem, we construct a universal G-bundle over $\widehat{\mathfrak{S}}_{R_0}[1/p]$ with a Frobenius which specializes to $(\mathfrak{P}_x, \phi_x)$ at every x.

Theorem 2.4.2. *Assume that $R_0 = R_{0,\eta}^{[a,b]}$. Let B be a finite F-algebra. The pair $(P_\eta[1/p], \phi_\eta[1/p])$ extends to a G-bundle $\widetilde{\mathfrak{P}}_\eta$ over $\widehat{\mathfrak{S}}_{R_0}[1/p]$ together with a Frobenius*

$$\phi_{\widetilde{\mathfrak{P}}_\eta} : \varphi^*(\widetilde{\mathfrak{P}}_\eta)[1/E(u)] \cong \widetilde{\mathfrak{P}}_\eta[1/E(u)]$$

such that, for any $x : R_0[1/p] \to B$, *the base change*

$$\big(\widetilde{\mathfrak{P}}_\eta \otimes_{\widehat{\mathfrak{S}}_{R_0}[1/p]} \mathfrak{S}_B, \phi_{\widetilde{\mathfrak{P}}_\eta} \otimes_{\widehat{\mathfrak{S}}_{R_0}[1/p,1/E(u)]} \mathfrak{S}_B[1/E(u)]\big)$$

is $(\mathfrak{P}_x, \phi_x)$.

Proof. Let $X_n := X^{[a,b]}_{\eta_n}$ be the projective $R_0/m^n_{R_0}$-scheme as in Section 4.3. Take $Y_n := X_n \times_{\operatorname{Spec} R_0/m^n_{R_0}} \operatorname{Spec} \mathfrak{S}_{R_0/m^n_{R_0}}$, a projective $\mathfrak{S}_{R_0/m^n_{R_0}}$-scheme. Let $X^{[a,b]}_\eta \to \operatorname{Spec} R_0$ be the algebraization of $\varprojlim X_n$ as before. The base change Y of $X^{[a,b]}_\eta$ along the map $R_0 \to \widehat{\mathfrak{S}}_{R_0}$ has the property that

$$Y \bmod m^n_{R_0} \cong Y_n.$$

Furthermore, Y is a proper $\widehat{\mathfrak{S}}_{R_0}$-scheme.

Over each Y_n, we have a universal G-Kisin lattice $(\mathfrak{P}_n, \phi_n)$ with height in $[a, b]$. By [Levin 2013, Corollary 2.3.5], there exists a G-bundle $\mathfrak{P}_\eta$ on Y such that $\mathfrak{P}_\eta \bmod m^n_{R_0} = \mathfrak{P}_n$. We would like to construct a Frobenius ϕ over $Y[1/E(u)]$ which reduces to ϕ_n modulo m^n_R for each $n \geq 1$. A priori, the Frobenius is only defined over the m_{R_0}-adic completion of $\widehat{\mathfrak{S}}_{R_0}[1/E(u)]$, which we denote by $\widehat{S}$.

We have a projective morphism

$$Y_{\widehat{S}} \to \operatorname{Spec} \widehat{S},$$

where $Y_{\widehat{S}}$ is the base change of $Y[1/E(u)]$ along $\operatorname{Spec} \widehat{S} \to \operatorname{Spec} \widehat{\mathfrak{S}}_{R_0}[1/E(u)]$. $Y_{\widehat{S}}$ is faithfully flat over $Y[1/E(u)]$, since $\widehat{\mathfrak{S}}_{R_0}[1/E(u)]$ is Noetherian. Define $\operatorname{Isom}_G := \operatorname{Isom}_G(\varphi^*(\mathfrak{P}_\eta), \mathfrak{P}_\eta)$ to be the affine finite-type Y-scheme of G-bundle isomorphisms. The compatible system $\{\phi_n\}$ lifts to an element

$$\widehat{\phi} \in \operatorname{Isom}_G(Y_{\widehat{S}}).$$

We would like to descend $\widehat{\phi}$ to a $Y[1/E(u)]$-point of Isom_G. Let $i : G \hookrightarrow \mathrm{GL}(V)$ be our chosen faithful representation. Consider the closed immersion

$$i_* : \operatorname{Isom}_G \hookrightarrow \operatorname{Isom}_{\mathrm{GL}(V)}(\varphi^*(\mathfrak{P}_\eta)(V), \mathfrak{P}_\eta(V)).$$

The image $i_*(\widehat{\phi})$ descends to a $Y[1/E(u)]$-point of $\operatorname{Isom}_{\mathrm{GL}(V)}(\varphi^*(\mathfrak{P}_\eta)(V), \mathfrak{P}_\eta(V))$ (twist to reduce to the effective case). Since $Y_{\widehat{S}}$ is faithfully flat over $Y[1/E(u)]$, for any closed immersion $Z \subset Z'$ of Y-schemes we have

$$Z\big(Y[1/E(u)]\big) = Z(Y_{\widehat{S}}) \cap Z'\big(Y[1/E(u)]\big).$$

Applying this with $Z' = \operatorname{Isom}_G$ and $Z = \operatorname{Isom}_{\mathrm{GL}(V)}(\varphi^*(\mathfrak{P}_\eta)(V), \mathfrak{P}_\eta(V))$, we get a universal pair $(\mathfrak{P}_\eta, \phi_\eta)$ over Y and $Y[1/E(u)]$, respectively. Since $R_0 = R^{[a,b]}_{0,\eta}$, $\Theta[1/p] : X^{[a,b]}_\eta[1/p] \to R_0[1/p]$ is an isomorphism and the pair $\widetilde{\mathfrak{P}}_\eta := \mathfrak{P}_\eta[1/p]$ and $\phi_{\mathfrak{P}_\eta}[1/p]$ over $\widehat{\mathfrak{S}}_{R_0}[1/p]$ has the desired properties. □

We now discuss the notion of p-adic Hodge type for G-valued representation and relate this to a filtration associated to a G-Kisin module.

Let B be any finite F-algebra. For any representation of Γ_K on a finite free B-module V_B, set

$$D_{\mathrm{dR}}(V_B) := (V_B \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}})^{\Gamma_K},$$

a filtered $(K \otimes_{\mathbb{Q}_p} B)$-module whose associated graded is projective (see [Balaji 2012, Definition 2.1.6, Lemma 2.4.2]). Furthermore, D_{dR} defines a tensor exact functor from the category of de Rham representations on projective B-modules to the category $\mathrm{Fil}_{K \otimes_{\mathbb{Q}_p} B}$ of filtered $(K \otimes_{\mathbb{Q}_p} B)$-modules (see [Balaji 2012, Lemma 2.4.2]). For any field κ, Fil_κ will be the tensor category of $\mathbb{Z}$-filtered vectors spaces $(V, \{\mathrm{Fil}^i V\})$, where $\mathrm{Fil}^i(V) \supset \mathrm{Fil}^{i+1}(V)$.

We recall a few facts from the Tannakian theory of filtrations:

Definition 2.4.3. Let H be any reductive group over a field κ. For any extension $\kappa' \supset \kappa$, an *H-filtration over κ'* is a tensor exact functor from $\mathrm{Rep}_\kappa(H)$ to $\mathrm{Fil}_{\kappa'}$.

Associated to any cocharacter $\nu : \mathbb{G}_{\mathrm{m}} \to H_{\kappa'}$ is a tensor exact functor from $\mathrm{Rep}_\kappa(H)$ to graded κ'-vector spaces which assigns to each representation W the vector space $W_{\kappa'}$, with its weight grading defined by the $\mathbb{G}_{\mathrm{m}}$-action through ν, which we denote by ω_ν (see [Deligne and Milne 1982, Example 2.30]).

Definition 2.4.4. For any H-filtration $\mathcal{F}$ over κ', a *splitting* of $\mathcal{F}$ is an isomorphism between $\mathrm{gr}(\mathcal{F})$ and ω_ν for some $\nu : \mathbb{G}_{\mathrm{m}} \to H_{\kappa'}$.

By [Saavedra Rivano 1972, Proposition IV.2.2.5], all H-filtrations over κ' are splittable. For any given $\mathcal{F}$, the cocharacters ν for which there exists an isomorphism $\mathrm{gr}(\mathcal{F}) \cong \omega_\nu$ lie in the common $H(\kappa')$-conjugacy class. If κ' is a finite extension of κ contained in $\bar{\kappa}$, then the *type* $[\nu_{\mathcal{F}}]$ of the filtration $\mathcal{F}$ is the geometric conjugacy class of ν for any splitting ω_ν over κ'. For any conjugacy class $[\nu]$ of geometric cocharacters of H, there is a smallest field of definition, contained in a chosen separable closure of κ, called the *reflex field* of $[\nu]$. We denote this by $\kappa_{[\nu]}$.

Let G be as before, so that G_F is a (connected) reductive group over F, and let $\eta : \Gamma_K \to G(B)$ be a continuous representation which is de Rham. Then D_{dR} defines a tensor exact functor from $\mathrm{Rep}_F(G_F)$ to $\mathrm{Fil}_{K \otimes_{\mathbb{Q}_p} B}$ (see Proposition 2.4.2 in [Balaji 2012]), which we denote by $\mathcal{F}_\eta^{\mathrm{dR}}$.

Fix a geometric cocharacter $\mu \in X_*((\mathrm{Res}_{(K \otimes_{\mathbb{Q}_p} F)/F}\, G)_{\overline{F}})$ and denote its conjugacy class by $[\mu]$. The cocharacter μ is equivalent to a set $(\mu_\psi)_{\psi : K \to \overline{F}}$ of cocharacters μ_ψ of $G_{\overline{F}}$ indexed by $\mathbb{Q}_p$-embeddings of K into $\overline{F}$.

Definition 2.4.5. Let $F_{[\mu]}$ be the reflex field of $[\mu]$. For any embedding $\psi : K \to \overline{F}$ over $\mathbb{Q}_p$, let $\mathrm{pr}_\psi : K \otimes_{\mathbb{Q}_p} \overline{F} \to \overline{F}$ denote the projection. If F' is a finite extension of $F_{[\mu]}$, a G-filtration $\mathcal{F}$ over $K \otimes_{\mathbb{Q}_p} F'$ has *type* $[\mu]$ if $\mathrm{pr}_\psi^*(\mathcal{F} \otimes_{F',i} \overline{F})$

has type $[\mu_\psi]$ for any $F_{[\mu]}$-embedding $i : F' \hookrightarrow \overline{F}$. A de Rham representation $\eta : \Gamma_K \to G(F')$ has *p-adic Hodge type* μ if $\mathcal{F}^{\mathrm{dR}}_\eta$ has type $[\mu]$.

Let $\Lambda_{[\mu]}$ denote the ring of integers of $F_{[\mu]}$. For any μ in the conjugacy class $[\mu]$, $\mathbb{G}_{\mathrm{m}}$ acts on $V \otimes_\Lambda \overline{F}$ through μ_ψ for each $\psi : K \to \overline{F}$. We take a and b be the minimal and maximal weights taken over all μ_ψ.

Theorem 2.4.6. *Let R_0 be a complete local Noetherian $\Lambda_{[\mu]}$-algebra with finite residue field and $\eta : \Gamma_K \to G(R_0)$ a continuous homomorphism. Let $R^{[a,b],\mathrm{st}}_{0,\eta}$ be as in Theorem 2.3.12. There exists a quotient $R^{\mathrm{st},\mu}_{0,\eta}$ of $R^{[a,b],\mathrm{st}}_{0,\eta}$ such that, for any finite extension F' of $F_{[\mu]}$, a homomorphism $\zeta : R_0 \to F'$ factors through $R^{\mathrm{st},\mu}_{0,\eta}$ if and only if the $G(F')$-valued representation corresponding to ζ is semistable with p-adic Hodge type $[\mu]$.*

Proof. See [Balaji 2012, Proposition 3.0.9]. □

Remark 2.4.7. One can deduce from the construction in [Balaji 2012, Proposition 3.0.9] or by other arguments [Levin 2013, Theorem 6.1.19] that the p-adic Hodge type on the generic fiber of the semistable deformation ring $R^{[a,b],\mathrm{st}}_{0,\eta}$ is locally constant so that Spec $R^{\mathrm{st},\mu}_{0,\eta}[1/p]$ is a union of connected components of Spec $R^{[a,b],\mathrm{st}}_{0,\eta}[1/p]$.

Finally, we recall how the de Rham filtration is obtained from the Kisin module.

Definition 2.4.8. Let B be a finite $\mathbb{Q}_p$-algebra. Let $(\mathfrak{M}_B, \phi_B)$ be a Kisin module over B with bounded height. Define

$$\mathrm{Fil}^i(\varphi^*(\mathfrak{M}_B)) := \phi_B^{-1}(E(u)^i \mathfrak{M}_B) \cap \varphi^*(\mathfrak{M}_B).$$

Set $\mathfrak{D}_B := \varphi^*(\mathfrak{M}_B)/E(u)\varphi^*(\mathfrak{M}_B)$, a finite projective $(K \otimes_{\mathbb{Q}_p} B)$-module. Define $\mathrm{Fil}^i(\mathfrak{D}_B)$ to be the image of $\mathrm{Fil}^i(\varphi^*(\mathfrak{M}_B))$ in $\mathfrak{D}_B$.

Proposition 2.4.9. *Let B be a finite $\mathbb{Q}_p$-algebra and V_B a finite free B-module with an action of Γ_K which is semistable with Hodge–Tate weights in $[a, b]$. Any $\mathbb{Z}_p$-stable lattice in V_B has finite height. If $\mathfrak{M}_B$ is the $(\mathfrak{S}_B, \varphi)$-module of bounded height attached to V_B, then there is a natural isomorphism $\mathfrak{D}_B \cong D_{\mathrm{dR}}(V_B)$ of filtered $(K \otimes_{\mathbb{Q}_p} B)$-modules.*

Proof. The relevant results are in the proofs of Corollary 2.6.2 and Theorem 2.5.5(2) in [Kisin 2008]. Since Kisin works with contravariant functors, one has to do a small translation. Under Kisin's conventions, $\mathfrak{M}_B$ would be associated to the B-dual V_B^*, and it is shown there that $D_B \cong D^*_{\mathrm{dR}}(V_B^*)$ as filtered $K \otimes_{\mathbb{Q}_p} B$-modules in the case where $[a, b] = [0, h]$. By compatibility with duality [Balaji 2012, Proposition 2.2.9], $D^*_{\mathrm{dR}}(V_B^*) \cong D_{\mathrm{dR}}(V_B)$. The general case follows by twisting. □

3. Deformations of G-Kisin modules

In this section, we study the local structure of the "moduli space" of G-Kisin modules. This generalizes results of [Kisin 2009; Pappas and Rapoport 2009]. G-Kisin modules may have nontrivial automorphisms and so it is more natural, as was done in [Kisin 2009, §2.2], to work with *groupoids*. The goal of the section is to smoothly relate the deformation theory of a G-Kisin module to the local structure of a local model for the group $\mathrm{Res}_{(K \otimes_{\mathbb{Q}_p} F)/F} G_F$.

Intuitively, the smooth modification (a chain of formally smooth morphisms) corresponds to adding a trivialization to the G-Kisin module and then taking the "image of Frobenius" similar to Proposition 2.2.11 of [Kisin 2009]. The target of the modification is a deformation functor for the moduli space $\mathrm{Gr}_G^{E(u),W}$ discussed in Section 3.3, which is a version of the affine Grassmannian that appears in the work of Pappas and Zhu [2013] on local models. Finally, we show that the condition of having p-adic Hodge type μ is related to a (generalized) local model $M(\mu) \subset \mathrm{Gr}_G^{E(u),W}$. In this section, there are no conditions on the cocharacter μ. We will impose conditions on μ only in the next section when we study the analogue of flat deformations.

3.1. ***Definitions and representability results.*** Let $\mathbb{F}$ be the residue field of Λ. Define the categories

$$\mathscr{C}_\Lambda = \{\text{Artin local } \Lambda\text{-algebras with residue field } \mathbb{F}\}$$

and

$$\widehat{\mathscr{C}}_\Lambda = \{\text{complete local Noetherian } \Lambda\text{-algebras with residue field } \mathbb{F}\}.$$

Morphisms are local Λ-algebra maps. Recall that fiber products in the category $\widehat{\mathscr{C}}_\Lambda$ exist and are represented by completed tensor products. A *groupoid* over $\mathscr{C}_\Lambda$ (or $\widehat{\mathscr{C}}_\Lambda$) will be in the sense of Definition A.2.2 of [Kisin 2009]; this is also known as a category cofibered in groupoids over $\mathscr{C}_\Lambda$ (or $\widehat{\mathscr{C}}_\Lambda$). Recall also the notion of a 2-fiber product of groupoids from (A.4) in [Kisin 2009]. See [Kim 2009, §10] for more details related to groupoids.

Choose a bounded-height G-Kisin module $(\mathfrak{P}_{\mathbb{F}}, \phi_{\mathbb{F}}) \in \mathrm{GMod}_{\mathfrak{S}_{\mathbb{F}}}^{\varphi,\mathrm{bh}}$. Define $D_{\mathfrak{P}_{\mathbb{F}}} = \bigcup_{a<b} D_{\mathfrak{P}_{\mathbb{F}}}^{[a,b]}$ to be the deformation groupoid of $\mathfrak{P}_{\mathbb{F}}$ as a G-Kisin module of bounded height over $\widehat{\mathscr{C}}_\Lambda$. The morphisms $D_{\mathfrak{P}_{\mathbb{F}}}^{[a,b]} \subset D_{\mathfrak{P}_{\mathbb{F}}}$ are relatively representable closed immersions, so intuitively $D_{\mathfrak{P}_{\mathbb{F}}}$ is an ind-object built out of the finite-height pieces.

Let $\mathscr{E}^0$ denote the trivial G-bundle over Λ. Throughout we will be choosing various trivializations of the G-bundle $\mathfrak{P}_{\mathbb{F}}$ and other related bundles. This is always possible because $\mathfrak{S}_{\mathbb{F}}$ is a complete semilocal ring with all residue fields finite (see Proposition 2.1.4(2)).

Proposition 3.1.1. *For any $\mathfrak{P}_{\mathbb{F}}$ with height in $[a,b]$, the deformation groupoid $D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}$ admits a formally smooth morphism $\pi : \operatorname{Spf} R \to D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}$ for some $R \in \widehat{\mathscr{C}}_\Lambda$ (i.e., has a versal formal object in the sense of* [SGA 7_{I} 1972]).

Proof. One can check the abstract Schlessinger's criterion in [SGA 7_{I} 1972, Theorem 1.11]. However, it will be useful to have an explicit versal formal object. Fix a trivialization $\beta_{\mathbb{F}}$ of $\mathfrak{P}_{\mathbb{F}}$ mod $E(u)^N$ for any $N \geq 1$, and define

$$\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}(A) := \{(\mathfrak{P}_A, \beta_A) \mid \mathfrak{P}_A \in D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}(A),\ \beta_A : \mathfrak{P}_A \cong \mathscr{E}^0_{\mathfrak{S}_A} \bmod E(u)^N\},$$

where β_A lifts $\beta_{\mathbb{F}}$. Since G is smooth, the forgetful morphism

$$\pi^{(N)} : \widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}} \to D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}$$

is formally smooth for any N.

If $N > (b-a)/(p-1)$, then $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$ is prorepresentable by a complete local Noetherian Λ-algebra. The proof uses Schlessinger's criterion. The two key points are that objects in $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}(A)$ have no nontrivial automorphisms, for which one inducts on the power of p which kills A (see [Levin 2013, Proposition 8.1.6]), and that the tangent space of the underlying functor is finite-dimensional, which uses a successive approximation argument (see [Levin 2013, Proposition 8.1.8]). ☐

It will also be useful to have an infinite version of $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$. Fix a trivialization $\beta_{\mathbb{F}} : \mathfrak{P}_{\mathbb{F}} \cong \mathscr{E}^0_{\mathfrak{S}_{\mathbb{F}}}$. Define a groupoid on $\mathscr{C}_\Lambda$ by

$$\widetilde{D}^{[a,b],(\infty)}_{\mathfrak{P}_{\mathbb{F}}}(A) := \{(\mathfrak{P}_A, \beta_A) \mid \mathfrak{P}_A \in D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}(A),\ \beta_A : \mathfrak{P}_A \cong \mathscr{E}^0_{\mathfrak{S}_A}\},$$

where β_A lifts $\beta_{\mathbb{F}}$. Define $\widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}} := \bigcup_{a<b} \widetilde{D}^{[a,b],(\infty)}_{\mathfrak{P}_{\mathbb{F}}}$.

3.2. ***Local models for Weil-restricted groups.*** In this section, we associate to any geometric conjugacy class $[\mu]$ of cocharacters of $\operatorname{Res}_{(K\otimes_{\mathbb{Q}_p}F)/F} G_F$ a local model $M(\mu)$ (Definition 3.2.3) over the ring of integers $\Lambda_{[\mu]}$ of the reflex field $F_{[\mu]}$ of $[\mu]$ (the relevant parahoric here is $\operatorname{Res}_{(\mathbb{O}_K\otimes_{\mathbb{Z}_p}\Lambda)/\Lambda} G$). By construction, $M(\mu)$ is a flat projective $\Lambda_{[\mu]}$-scheme. The principal result (Theorem 3.2.4) says that $M(\mu)$ is normal and its special fiber is reduced.

The details of the proof of Theorem 3.2.4 are in [Levin 2013, §10], where we follow the strategy introduced in [Pappas and Zhu 2013]. We cannot apply Pappas and Zhu's result directly because the group $\operatorname{Res}_{(K\otimes_{\mathbb{Q}_p}F)/F} G_F$ usually does not split over a tame extension of F. In [Levin 2014], we generalize [Levin 2013, §10] and [Pappas and Zhu 2013] to groups of the form $\operatorname{Res}_{L/F} H$, where H is reductive group over L which splits over a tame extension of L, and allow arbitrary parahoric level structure. Here we recall the relevant definitions and results, leaving the details to [Levin 2013; 2014].

For any Λ-algebra R, set $R_W := R \otimes_{\mathbb{Z}_p} W$. Our local models are constructed inside the following moduli space:

Definition 3.2.1. For any Λ-algebra R, let $\widehat{R_W[u]}_{(E(u))}$ denote the $E(u)$-adic completion of $R_W[u]$. Define

$$\mathrm{Gr}_G^{E(u),W}(R) := \{\text{isomorphism classes of pairs } (\mathscr{E}, \alpha)\},$$

where $\mathscr{E}$ is a G-bundle on $\widehat{R_W[u]}_{(E(u))}$ and

$$\alpha : \mathscr{E}|_{\widehat{R_W[u]}_{(E(u))}[E(u)^{-1}]} \cong \mathscr{E}^0_{\widehat{R_W[u]}_{(E(u))}[E(u)^{-1}]}.$$

Proposition 3.2.2. *The functor* $\mathrm{Gr}_G^{E(u),W}$ *is an ind-scheme which is ind-projective over* Λ. *Furthermore*:

(1) *The generic fiber* $\mathrm{Gr}_G^{E(u),W}[1/p]$ *is naturally isomorphic to the affine Grassmannian of* $\mathrm{Res}_{(K \otimes_{\mathbb{Q}_p} F)/F} G_F$ *over the field* F.

(2) *If* k_0 *is the residue field of* W, *then the special fiber* $\mathrm{Gr}_G^{E(u),W} \otimes_\Lambda \mathbb{F}$ *is naturally isomorphic to the affine Grassmannian of* $\mathrm{Res}_{(k_0 \otimes_{\mathbb{F}_p} \mathbb{F})/\mathbb{F}}(G_{\mathbb{F}})$.

Proof. See §10.1 in [Levin 2013]. □

Let H be any reductive group over F and Gr_H be the affine Grassmannian of H. Associated to any geometric conjugacy class $[\mu]$ of cocharacters, there is an affine Schubert variety $S(\mu)$ in $(\mathrm{Gr}_H)_{F_{[\mu]}}$, where $F_{[\mu]}$ is the reflex field of $[\mu]$. These are the closures of orbits for the positive loop group L^+H.

The geometric conjugacy classes of cocharacters of H can be identified with the set of dominant cocharacters for a choice of maximal torus and Borel subgroup over $\overline{F}$. The dominant cocharacters have partial ordering defined by $\mu \geq \lambda$ if and only if $\mu - \lambda$ is a nonnegative sum of positive coroots. Then $S(\mu)_{\overline{F}}$ is the union of the locally closed affine Schubert cells for all $\mu' \leq \mu$ [Richarz 2013, Proposition 2.8].

Definition 3.2.3. Let $F_{[\mu]}/F$ be the reflex field of $[\mu]$ with ring of integers $\Lambda_{[\mu]}$. If $S(\mu) \subset \mathrm{Gr}_{\mathrm{Res}_{(K \otimes_{\mathbb{Q}_p} F)/F} G_F} \otimes_F F_{[\mu]}$ is the closed affine Schubert variety associated to μ, then the *local model* $M(\mu)$ associated to μ is the flat closure of $S(\mu)$ in $\mathrm{Gr}_G^{E(u),W} \otimes_\Lambda \Lambda_{[\mu]}$. It is a flat projective scheme over $\operatorname{Spec} \Lambda_{[\mu]}$.

The main theorem on the geometry of local models is:

Theorem 3.2.4. *Suppose that* $p \nmid |\pi_1(G^{\mathrm{der}})|$, *where* G^{der} *is the derived subgroup of* G. *Then* $M(\mu)$ *is normal. The special fiber* $M(\mu) \otimes_{\Lambda_\mu} \overline{\mathbb{F}}$ *is reduced*, *irreducible*, *normal*, *Cohen–Macaulay and Frobenius-split.*

For the next subsection, it will useful to recall a group which acts on $\mathrm{Gr}_G^{E(u),W}$ and $M(\mu)$. Define

$$L^{+,E(u)}G(R) := G(\widehat{R_W[u]}_{(E(u))}) = \varprojlim_{i\geq 1} G(R_W[u]/(E(u)^i))$$

for all Λ-algebras R. $L^{+,E(u)}G$ is represented by a group scheme that is the projective limit of the affine, flat, finite-type group schemes $\mathrm{Res}_{((\Lambda\otimes_{\mathbb{Z}_p}W)[u]/E(u)^i)/\Lambda}G$.

The group $L^{+,E(u)}G$ acts on $\mathrm{Gr}_G^{E(u),W}$ by changing the trivialization. This action is *nice* in the sense of [Gaitsgory 2001, A.3], i.e., $\mathrm{Gr}_G^{E(u),W} \cong \varinjlim_i Z_i$, where Z_i are $L^{+,E(u)}G$-stable closed subschemes on which $L^{+,E(u)}G$ acts through the quotient $\mathrm{Res}_{((\Lambda\otimes_{\mathbb{Z}_p}W)[u]/E(u)^i)/\Lambda}G$.

Corollary 3.2.5. *For any μ, the local model $M(\mu)$ is stable under the action of $L^{+,E(u)}G$.*

Proof. Since everything is flat, it suffices to show that $M(\mu)[1/p]$ is stable under $L^{+,E(u)}G[1/p]$. The functor $L^{+,E(u)}G[1/p]$ on F-algebras is naturally isomorphic to the positive loop group $L^+\mathrm{Res}_{(K\otimes_{\mathbb{Q}_p}F)/F}(G)$, so that the isomorphism in Proposition 3.2.2(1) is equivariant. $M(\mu)[1/p]$ is the closed affine Schubert variety $S(\mu)$ which is stable under the action of this group. □

3.3. ***Smooth modification.*** We begin by defining the deformation functor which will be the target of our modification.

Definition 3.3.1. Choose a G-bundle $Q_{\mathbb{F}}$ over $\mathfrak{S}_{\mathbb{F}}$ together with a trivialization δ_0 of $Q_{\mathbb{F}}$ over $\mathfrak{S}_{\mathbb{F}}[1/E(u)]$. Define a deformation functor on $\mathscr{C}_\Lambda$ by

$$\overline{D}_{Q_{\mathbb{F}}}(A) := \{\text{isomorphism classes of triples } (\mathscr{E}, \delta, \psi)\},$$

where $\mathscr{E}$ is a G-bundle on $\mathfrak{S}_A$, $\delta : \mathscr{E}|_{\mathfrak{S}_A[E(u)^{-1}]} \cong \mathscr{E}^0_{\mathfrak{S}_A[E(u)^{-1}]}$, and the map $\psi : \mathscr{E}\otimes_{\mathfrak{S}_A}\mathfrak{S}_{\mathbb{F}} \cong Q_{\mathbb{F}}$ is compatible with δ and δ_0.

Example 3.3.2. Let $G = \mathrm{GL}(V)$. For any $(Q_A, \delta_A) \in \overline{D}_{Q_{\mathbb{F}}}(A)$, δ_A identifies Q_A with a "lattice" in $(V\otimes_\Lambda \mathfrak{S}_A)[1/E(u)]$, that is, a finitely generated projective $\mathfrak{S}_A$-module L_A such that $L_A[1/E(u)] = (V\otimes_\Lambda\mathfrak{S}_A)[1/E(u)]$.

The main result of this section is the following:

Theorem 3.3.3. *Let Λ be a $\mathbb{Z}_p$-finite, flat, local domain with residue field $\mathbb{F}$. Let G be a connected reductive group over Λ and $\mathfrak{P}_{\mathbb{F}}$ a G-Kisin module with coefficients in $\mathbb{F}$. Fix a trivialization $\beta_{\mathbb{F}}$ of $\mathfrak{P}_{\mathbb{F}}$ as a G-bundle. There exists a diagram of* *groupoids over* $\mathscr{C}_\Lambda$,

$$\begin{array}{ccc} & \widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}} & \\ {}^{\pi^{(\infty)}}\swarrow & & \searrow^{\Psi} \\ D_{\mathfrak{P}_{\mathbb{F}}} & & \overline{D}_{Q_{\mathbb{F}}}, \end{array}$$

where $Q_{\mathbb{F}} := (\varphi^*(\mathfrak{P}_{\mathbb{F}}), \beta_{\mathbb{F}}[1/E(u)] \circ \phi_{\mathfrak{P}_{\mathbb{F}}})$. *Both* $\pi^{(\infty)}$ *and* Ψ *are formally smooth.*

Later in the section, we will refine this modification by imposing appropriate conditions on both sides. Intuitively, the above modification corresponds to adding a trivialization to the G-Kisin module and then taking the "image of Frobenius". The groupoid $\widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}}$ is defined at the end of Section 3.1 and $\pi^{(\infty)}$ is formally smooth since G is smooth. Next, we construct the morphism Ψ and show that it is formally smooth. To avoid excess notation, we sometimes omit the data of the residual isomorphisms modulo m_A. One can check that the everything is compatible with such isomorphisms.

Definition 3.3.4. For any $(\mathfrak{P}_A, \phi_{\mathfrak{P}_A}, \beta_A) \in \widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}}(A)$, we set

$$\Psi((\mathfrak{P}_A, \phi_{\mathfrak{P}_A}, \beta_A)) = (\varphi^*(\mathfrak{P}_A), \delta_A),$$

where δ_A is the composite

$$\varphi^*(\mathfrak{P}_A)[1/E(u)] \xrightarrow{\phi_{\mathfrak{P}_A}} \mathfrak{P}_A[1/E(u)] \xrightarrow{\beta_A[1/(E(u))]} \mathscr{E}^0_{\mathfrak{S}_A}[1/E(u)].$$

Proposition 3.3.5. *The morphism* Ψ *of groupoids is formally smooth.*

Proof. Choose $A \in \mathscr{C}_\Lambda$ and an ideal I of A. Consider a pair $(Q_A, \delta_A) \in \overline{D}_{Q_{\mathbb{F}}}(A)$ over a pair $(Q_{A/I}, \delta_{A/I})$. Let $(\mathfrak{P}_{A/I}, \phi_{A/I}, \beta_{A/I})$ be an element in the fiber over $(Q_{A/I}, \delta_{A/I})$. The triple $(\mathfrak{P}_{A/I}, \phi_{A/I}, \beta_{A/I})$ is isomorphic to a triple of the form $(\mathscr{E}^0_{\mathfrak{S}_{A/I}}, \phi'_{A/I}, \mathrm{Id}_{A/I})$. Let $\gamma_{A/I}$ be the isomorphism between $\varphi^*(\mathscr{E}^0_{\mathfrak{S}_{A/I}})$ and $Q_{A/I}$. We want to construct a lift $(\mathfrak{P}_A, \phi_A, \beta_A)$ such that $\Psi(\mathfrak{P}_A, \phi_A, \beta_A) = (Q_A, \delta_A)$. Take $\mathfrak{P}_A = \mathscr{E}^0_{\mathfrak{S}_A}$ to be the trivial bundle and β_A to be the identity.

Now, pick any lift $\gamma_A : \varphi^*(\mathscr{E}^0_{\mathfrak{S}_A}) \cong Q_A$, of $\gamma_{A/I}$ which exists since G is smooth. We can define the Frobenius by

$$\phi_A = \delta_A \circ \gamma_A[1/E(u)].$$

It is easy to check that $\Psi(\mathfrak{P}_A, \phi_A, \beta_A) \cong (Q_A, \delta_A)$. □

We would now like to relate $\overline{D}_{Q_{\mathbb{F}}}$ to $\mathrm{Gr}^{E(u),W}_G$ from the previous section.

Proposition 3.3.6. *A pair* $(Q_{\mathbb{F}}, \delta_0)$ *as in Definition 3.3.1 defines a point* $x_{\mathbb{F}}$ *in* $\mathrm{Gr}^{E(u),W}_G(\mathbb{F})$. *Furthermore, for any* $A \in \mathscr{C}_\Lambda$, *there is a natural functorial bijection between* $\overline{D}_{Q_{\mathbb{F}}}(A)$ *and the set of* $x_A \in \mathrm{Gr}^{E(u),W}_G(A)$ *such that* $x_A \bmod m_A = x_{\mathbb{F}}$.

Proof. Recall that $\mathfrak{S}_A = (W \otimes_{\mathbb{Z}_p} A)[\![u]\!]$ because A is finite over $\mathbb{Z}_p$. Also, $\mathrm{Gr}_G^{E(u),W}(A)$ is the set of isomorphism classes of bundles on the $E(u)$-adic completion of $(W \otimes_{\mathbb{Z}_p} A)[u]$ together with a trivialization after inverting $E(u)$. Since p is nilpotent in A, we can identify $(W \otimes_{\mathbb{Z}_p} A)[\![u]\!]$ and the $E(u)$-adic completion $\widehat{(W \otimes_{\mathbb{Z}_p} A)[u]}_{(E(u))}$. This identifies $\overline{D}_{Q_{\mathbb{F}}}(A)$ with the desired subset of $\mathrm{Gr}_G^{E(u),W}(A)$. □

For any $\mathbb{Z}_p$-algebra A, let $\widehat{S}_A$ denote the $E(u)$-adic completion of $(W \otimes_{\mathbb{Z}_p} A)[u]$.

Lemma 3.3.7. *For any finite flat $\mathbb{Z}_p$-algebra Λ', there is a $(W \otimes_{\mathbb{Z}_p} \Lambda')[u]$-algebra isomorphism*

$$\mathfrak{S}_{\Lambda'} \to \widehat{S}_{\Lambda'}.$$

Proof. For any $n \geq 1$, we have an isomorphism

$$\mathfrak{S}_{\Lambda'}/p^n \cong \widehat{S}_{\Lambda'}/p^n$$

since $(E(u))$ and u define the same adic topologies modulo p^n. Passing to the limit, we get an isomorphism of their p-adic completions. Both $\mathfrak{S}_{\Lambda'}$ and $\widehat{S}_{\Lambda'}$ are already p-adically complete and separated. □

Fix a geometric cocharacter μ of $\mathrm{Res}_{(K \otimes_{\mathbb{Q}_p} F)/F} G_F$, which we can write as $\mu = (\mu_\psi)_{\psi: K \to \overline{F}}$, where the μ_ψ are cocharacters of $G_{\overline{F}}$. *Assume* that $F = F_{[\mu]}$, so that the generalized local model $M(\mu)$ is a closed subscheme of $\mathrm{Gr}_G^{E(u),W}$ over Λ; see Definition 3.2.3. Recall that V is a fixed faithful representation of G. For each ψ, μ_ψ induces an action of $\mathbb{G}_{\mathrm{m}}$ on $V_{\overline{F}}$. Define a (resp. b) to be the smallest (resp. largest) weight appearing in $V_{\overline{F}}$ over all μ_ψ.

Definition 3.3.8. Define a closed subfunctor $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$ of $\overline{D}_{Q_{\mathbb{F}}}$ by

$$\overline{D}^{\mu}_{Q_{\mathbb{F}}}(A) := \{(Q_A, \delta_A) \in \overline{D}_{Q_{\mathbb{F}}}(A) \mid (Q_A, \delta_A) \in M(\mu)(A)\}$$

under the identification in Proposition 3.3.6. Define $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ to be the base change of $\overline{D}^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ along Ψ. It is a closed subgroupoid of $\widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}}$.

The following proposition says that $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ descends to a closed subgroupoid $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ of $D_{\mathfrak{P}_{\mathbb{F}}}$:

Proposition 3.3.9. *Let a and b be as in the discussion before Definition 3.3.8. There is a closed subgroupoid $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}} \subset D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}} \subset D_{\mathfrak{P}_{\mathbb{F}}}$ such that $\pi^{(\infty)}|_{\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}}$ factors through $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ and*

$$\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} \to D^{\mu}_{\mathfrak{P}_{\mathbb{F}}} \times_{D_{\mathfrak{P}_{\mathbb{F}}}} \widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}}$$

is an equivalence of closed subgroupoids. Furthermore, $\pi^{\mu} : \widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} \to D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ is formally smooth.

Proof. For any $A \in \mathscr{C}_\Lambda$ define $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$ to be the full subcategory whose objects are $\pi^{(\infty)}(\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}(A))$. Observe that for any $x \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$ the group $G(\mathfrak{S}_A)$ acts transitively on the fiber $(\pi^{(\infty)})^{-1}(x) \subset \widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}}(A)$ by changing the trivialization. The key point is that $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$ is stable under $G(\mathfrak{S}_A)$, by Corollary 3.2.5. Hence,

$$(\pi^{(\infty)})^{-1}(x) \subset \widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}(A). \tag{3-3-9-1}$$

It is not hard to see then that the map to the fiber product is an isomorphism and that π^{μ} is formally smooth.

It remains to show that $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}} \to D_{\mathfrak{P}_{\mathbb{F}}}$ is closed. Let $\mathfrak{P}_A \in D_{\mathfrak{P}_{\mathbb{F}}}(A)$ and choose a trivialization β_A of $\mathfrak{P}_A$, i.e., a lift to $\widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}}(A)$. We want a quotient $A \to A'$ such that, for any $f : A \to B$, $\mathfrak{P}_A \otimes_{A,f} B \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(B)$ if and only if f factors through A'. Let $A \to A'$ represent the closed condition $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} \subset \widetilde{D}^{(\infty)}_{\mathfrak{P}_{\mathbb{F}}}$. Clearly, $\mathfrak{P}_A \otimes_A A' \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(A')$ and so any further base change is as well. Now, let $f : A \to B$ be such that $\mathfrak{P}_A \otimes_{A,f} B \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(B)$. The trivialization β_A induces a trivialization β_B on $\mathfrak{P}_B$. The pair $(\mathfrak{P}_B, \beta_B)$ lies in $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}(B)$ by (3-3-9-1). □

We have constructed a diagram of formally smooth morphisms

$$\begin{array}{ccc} & \widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} & \\ {\scriptstyle \pi^{\mu}} \swarrow & & \searrow {\scriptstyle \Psi^{\mu}} \\ D^{\mu}_{\mathfrak{P}_{\mathbb{F}}} & & \overline{D}^{\mu}_{Q_{\mathbb{F}}}, \end{array} \tag{3-3-9-2}$$

where $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$ is represented by the completed local ring at the $\mathbb{F}$-point of $M(\mu)$ corresponding to $(Q_{\mathbb{F}}, \delta_{\mathbb{F}})$. Next, we would like to replace $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ by a "smaller" groupoid which is representable.

Let a and b be as in the discussion before Definition 3.3.8 and choose $N > b-a$. Recall the representable groupoid $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$ (Proposition 3.1.1). Define a closed subgroupoid

$$\widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}} := D^{\mu}_{\mathfrak{P}_{\mathbb{F}}} \times_{D_{\mathfrak{P}_{\mathbb{F}}}} \widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$$

of $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$. By Proposition 3.3.9, the morphism $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} \to D^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ is formally smooth.

Proposition 3.3.10. *For any $N > b-a$, the morphism $\Psi^{\mu} : \widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} \to \overline{D}^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ factors through $\widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$. Furthermore, $\widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ is formally smooth over $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$.*

Proof. By our assumption on N, $\widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ is representable, so it suffices to define the factorization $\Psi^{\mu}_N : \widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}} \to \overline{D}^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ on underlying functors. For any $x \in \widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$, set

$$\Psi^{(N),\mu}(x) := \Psi^{\mu}(\tilde{x})$$

for any lift $\tilde{x}$ of x to $\widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$. The image is independent of the choice of lift by Corollary 3.2.5. The map $\Psi^{(N),\mu}$ is formally smooth since Ψ^{μ} is. □

In the remainder of this section, we discuss the relationship between $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ and p-adic Hodge type μ. For this, it will useful to work in a larger category than $\widehat{\mathscr{C}}_{\Lambda}$. All of our deformation problems can be extended to the category of complete local Noetherian Λ-algebras R with finite residue field. For any such R, we define $D^{\star}_{\mathfrak{P}_{\mathbb{F}}}(R)$ (and, similarly, $\widetilde{D}^{\star}_{\mathfrak{P}_{\mathbb{F}}}(R)$, $\overline{D}^{\star}_{Q_{\mathbb{F}}}(R)$) to be the category of deformations to R of $\mathfrak{P}_{\mathbb{F}} \otimes_{\mathbb{F}} R/m_R$ with condition $\star$, where $\star$ is any of our various conditions. For any finite local Λ-algebra Λ', the category $\widehat{\mathscr{C}}_{\Lambda'}$ is a subcategory of the category of complete local Noetherian Λ-algebras with finite residue field.

The functors $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$, $\widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ and $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$ are all representable on $\widehat{\mathscr{C}}_{\Lambda}$. It is easy to check, using the criterion in [Chai et al. 2014, Proposition 1.4.3.6], that these functors commute with change in coefficients, i.e., if $\widetilde{R}^{[a,b],(N)}$ represents $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$ over $\mathscr{C}_{\Lambda}$ then $\widetilde{R}^{[a,b],(N)} \otimes_{\Lambda} \Lambda'$ represents the extension of $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}$ restricted to the category $\widehat{\mathscr{C}}_{\Lambda'}$, and similarly for $\widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ and $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$.

An argument as in Theorem 2.4.2 shows that, in $D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}(R)$, an object of $D^{[a,b]}$ is the same as a G-bundle $\mathfrak{P}_R$ on $\widehat{\mathfrak{S}}_R$ together with a Frobenius

$$\phi_{\mathfrak{P}_R} : \varphi^*(\mathfrak{P}_R)[1/E(u)] \cong \mathfrak{P}_R[1/E(u)]$$

deforming $\mathfrak{P}_{\mathbb{F}} \otimes_{\mathbb{F}} R/m_R$ and having height in $[a,b]$. The condition on the height is essential in order to define the Frobenius over R. We would like to give a criterion that says when $(\mathfrak{P}_R, \phi_{\mathfrak{P}_R})$ lies in $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(R)$.

Choose $(\mathfrak{P}_R, \phi_{\mathfrak{P}_R}) \in D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}(R)$. For any finite extension F' of F and any homomorphism $x : R \to F'$, denote the base change of $\mathfrak{P}_R$ to $\mathfrak{S}_{F'}$ by $(\mathfrak{P}_x, \phi_x)$. Associated to $(\mathfrak{P}_x, \phi_x)$ is a functor $\mathfrak{D}_x$ from $\mathrm{Rep}_F(G_F)$ to filtered $(K \otimes_{\mathbb{Q}_p} F')$-modules given by $\mathfrak{D}_x(W) = \varphi^*(\mathfrak{P}_x)(W)/E(u)\varphi^*(\mathfrak{P}_x)(W)$ with the filtration defined as in Definition 2.4.8.

Lemma 3.3.11. *For any finite extension F' of F and any $x : R \to F'$, the functor $\mathfrak{D}_x$ is a tensor exact functor.*

Proof. Any such x factors through the ring of integers Λ' of F', so that $(\mathfrak{P}_x, \phi_x)$ comes from a pair $(\mathfrak{P}_{x_0}, \phi_{x_0})$ over $\mathfrak{S}_{\Lambda'}$. Let $\widehat{S}_{\Lambda'}$ and $\widehat{S}_{F'}$ be the $E(u)$-adic completions of $(W \otimes_{\mathbb{Z}_p} \Lambda')[u]$ and $(W \otimes_{\mathbb{Z}_p} F')[u]$, respectively. By Lemma 3.3.7, we can equivalently think of $(\mathfrak{P}_{x_0}, \phi_{x_0})$ as a pair over $\widehat{S}_{\Lambda'}$.

Choose a trivialization β_0 of $\mathfrak{P}_{x_0}$ and set $Q_{x_0} := \varphi^*(\mathfrak{P}_{x_0})$ with trivialization $\delta_{x_0} := \beta_0[1/E(u)] \circ \phi_{x_0}$. Define (Q_x, δ_x) to be $(Q_{x_0}, \delta_{x_0}) \otimes_{\widehat{S}_{\Lambda'}} \widehat{S}_{F'}$ and define a filtration on $\mathfrak{D}_{Q_x} := Q_x \bmod E(u)$ by

$$\mathrm{Fil}^i(\mathfrak{D}_{Q_x}(W)) = (Q_x(W) \cap E(u)^i (W \otimes \widehat{S}_{F'}))/(E(u) Q_x(W) \cap E(u)^i (W \otimes \widehat{S}_{F'}))$$

for any $W \in \mathrm{Rep}_F(G_F)$. Since $\widehat{S}_{\Lambda'}[1/p]/(E(u)) = \widehat{S}_{F'}/(E(u))$, there is an isomorphism

$$\mathfrak{D}_x \cong \mathfrak{D}_{Q_x}$$

of tensor exact functors to $\mathrm{Mod}_{K\otimes_{\mathbb{Q}_p}F'}$ identifying the filtrations.

It suffices then to show that $\mathfrak{D}_{Q_x}$ is a tensor exact functor to the category of filtered $(K \otimes_{\mathbb{Q}_p} F')$-modules. Without loss of generality, we assume that F' contains a Galois closure of K. Then

$$\widehat{S}_{F'} \cong \prod_{\psi} F'[\![u - \psi(\pi)]\!]$$

over embeddings $\psi : K \to F'$ (first decompose $W \otimes_{\mathbb{Z}_p} F'$ and then decompose $E(u)$ in each factor). Thus, (Q_x, δ_x) decomposes as a product $\prod_\psi (Q_x^\psi, \delta_x^\psi)$, where each pair defines a point z_ψ of the affine Grassmannian of $G_{F'}$. The quotient $\mathfrak{D}_{Q_x}$ decomposes compatibly as $\prod_\psi \mathfrak{D}_{Q_x^\psi}$. We are reduced then to a computation for a point $z_\psi \in \mathrm{Gr}_{G_{F'}}(F')$. Without loss of generality, we can assume $G_{F'}$ is split. Up to translation by the positive loop group (which induces an isomorphism on filtrations), z_ψ is the image $[g]$ for some $g \in T(F'((t)))$ where T is maximal split torus of $G_{F'}$. Using the weight space decomposition for T on any representation W, one can compute directly that $\mathfrak{D}_{Q_x^\psi}$ is a tensor exact functor. For more details, see [Levin 2013, Proposition 3.5.11, Lemma 8.2.15]. □

Definition 3.3.12. Let F' be any finite extension of F with ring of integers Λ'. We say a G-Kisin module $(\mathfrak{P}_{\Lambda'}, \phi_{\Lambda'})$ over Λ' has *p-adic Hodge type* μ if the G_F-filtration associated to $\mathfrak{P}_{\Lambda'}[1/p]$ as above has type μ.

Theorem 3.3.13. *Assume that $F = F_{[\mu]}$. Let R be any complete local Noetherian Λ-algebra with finite residue field which is Λ-flat and reduced. Then $\mathfrak{P}_R \in D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}(R)$ lies in $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(R)$ if and only if, for all finite extensions F'/F and all homomorphisms $x : R \to F'$, the G_F-filtration $\mathfrak{D}_x$ has type less than or equal to $[\mu]$.*

Proof. Choose a lift $\tilde{y}$ of $\mathfrak{P}_R$ to $\widetilde{D}^{[a,b],(N)}_{\mathfrak{P}_{\mathbb{F}}}(R)$. Clearly, $\mathfrak{P}_R \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(R)$ if and only if $\tilde{y} \in \widetilde{D}^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}(R)$, which happens if and only $\Psi(\tilde{y}) \in \overline{D}^{\mu}_{Q_{\mathbb{F}}}(R)$. Let R^μ be the quotient of R representing the fiber product

$$\mathrm{Spf}\, R \times_{\overline{D}^{[a,b]}_{Q_{\mathbb{F}}}} \overline{D}^{\mu}_{Q_{\mathbb{F}}}.$$

To show that $R^\mu = R$, it suffices to show that $\mathrm{Spec}\, R^\mu[1/p]$ contains all closed points of $\mathrm{Spec}\, R[1/p]$, since R is flat and $R[1/p]$ is reduced and Jacobson.

The groupoid $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$ is represented by a completed stalk on the local model $M(\mu) \subset \mathrm{Gr}^{E(u),W}_G$, so that, for any $x : R \to F'$, $\Psi(\tilde{y})[1/p]$ defines an F'-point (Q_x, δ_x) of $\mathrm{Gr}^{E(u),W}_G$. Since $M(\mu)(F') = S(\mu)(F')$, $(Q_x, \delta_x) \in S(\mu)(F')$ if and only if the filtration $\mathfrak{D}_{Q_x}$ has type less than or equal to $[\mu]$ [Levin 2013, Proposition 3.5.11]. The proof of Lemma 3.3.11 shows that the two filtrations agree, i.e.,

$$\mathfrak{D}_x \cong \mathfrak{D}_{Q_x}.$$

Thus, x factors through R^{μ} exactly when the type of the filtration $\mathfrak{D}_x$ is less than or equal to $[\mu]$. □

Fix a continuous representation $\bar{\eta} : \Gamma_K \to G(\mathbb{F})$. Let $R^{[a,b],\mathrm{cris}}_{\bar{\eta}}$ be the universal framed G-valued crystalline deformation ring with Hodge–Tate weights in $[a, b]$, and let $\Theta : X^{[a,b],\mathrm{cris}}_{\bar{\eta}} \to \operatorname{Spec} R^{[a,b],\mathrm{cris}}_{\bar{\eta}}$ be as in Proposition 2.3.3.

Definition 3.3.14. Assume $F = F_{[\mu]}$. Define $R^{\mathrm{cris},\leq\mu}_{\bar{\eta}}$ to be the flat closure of the connected components of

$$\operatorname{Spec} R^{[a,b],\mathrm{cris}}_{\bar{\eta}}[1/p]$$

with type less than or equal to μ (see Theorem 2.4.6). Define $X^{\mathrm{cris},\leq\mu}_{\bar{\eta}}$ to be the flat closure in $X^{[a,b],\mathrm{cris}}_{\bar{\eta}}$ of the same connected components (since $\Theta[1/p]$ is an isomorphism).

Corollary 3.3.15. *Let $X^{\mathrm{cris},\leq\mu}_{\bar{\eta}}$ be as in Definition 3.3.14. A point $\bar{x} \in X^{\mathrm{cris},\leq\mu}_{\bar{\eta}}(\mathbb{F}')$ corresponds to a G-Kisin lattice $\mathfrak{P}_{\mathbb{F}'}$ over $\mathfrak{S}_{\mathbb{F}'}$. The deformation problem $D^{\mathrm{cris},\mu}_{\bar{x}}$ which assigns to any $A \in \mathscr{C}_{\Lambda\otimes_{\mathbb{Z}_p}W(\mathbb{F}')}$ the set of isomorphisms classes of triples*

$$\{(y, \mathfrak{P}_A, \delta_A) \mid y : R^{\mathrm{cris},\leq\mu}_{\bar{\eta}} \to A,\ \mathfrak{P}_A \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}'}}(A),\ \delta_A : T_{G,\mathfrak{S}_A}(\mathfrak{P}_A) \cong \eta_y|_{\Gamma_\infty}\}$$

is representable. Furthermore, if $\widehat{\mathscr{O}}^{\mu}_{\bar{x}}$ is the completed local ring of $X^{\mathrm{cris},\leq\mu}_{\bar{\eta}}$ at $\bar{x}$, then the natural map $\operatorname{Spf}\widehat{\mathscr{O}}^{\mu}_{\bar{x}} \to D^{\mathrm{cris},\mu}_{\bar{x}}$ is a closed immersion which is an isomorphism modulo p-power torsion.

Proof. Without loss of generality, we can replace Λ by $\Lambda \otimes_{W(\mathbb{F})} W(\mathbb{F}')$. By construction and Proposition 2.3.5, for any $A \in \mathscr{C}_\Lambda$, the deformation functor

$$D^{\mathrm{cris},\mu,\mathrm{bc}}_{\bar{x}}(A) = \{y : R^{\mathrm{cris},\leq\mu}_{\bar{\eta}} \to A, \mathfrak{P}_A \in D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}'}}(A), \delta_A : T_{G,\mathfrak{S}_A}(\mathfrak{P}_A) \cong \eta_y|_{\Gamma_\infty}\}/\cong$$

is representable. That is, $D^{\mathrm{cris},\mu,\mathrm{bc}}_{\bar{x}}$ represents the completed stalk at a point of the fiber product $X^{[a,b],\mathrm{cris}}_{\bar{\eta}} \times_{\operatorname{Spec} R^{[a,b],\mathrm{cris}}_{\bar{\eta}}} \operatorname{Spec} R^{\mathrm{cris},\leq\mu}_{\bar{\eta}}$. Since $D^{\mu}_{\mathfrak{P}_{\mathbb{F}'}} \subset D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}'}}$ is closed, so is $D^{\mathrm{cris},\mu}_{\bar{x}} \subset D^{\mathrm{cris},\mu,\mathrm{bc}}_{\bar{x}}$ and hence $D^{\mathrm{cris},\mu}_{\bar{x}}$ is representable by $R^{\mathrm{cris},\mu}_{\bar{x}}$. To see that the closed immersion $\operatorname{Spf}\widehat{\mathscr{O}}^{\mu}_{\bar{x}} \to D^{\mathrm{cris},\mu,\mathrm{bc}}_{\bar{x}}$ factors through $D^{\mathrm{cris},\mu}_{\bar{x}}$, it suffices to show that the "universal" lattice $\mathfrak{P}_{\widehat{\mathscr{O}}^{\mu}_{\bar{x}}} \in D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}'}}(\widehat{\mathscr{O}}^{\mu}_{\bar{x}})$ lies in $D^{\mu}_{\mathfrak{P}_{\mathbb{F}'}}(\widehat{\mathscr{O}}^{\mu}_{\bar{x}})$.

By Proposition 2.3.9 and Theorem 2.3.12, $\Theta[1/p]$ is an isomorphism. Furthermore, by [Balaji 2012, Proposition 4.1.5], $R^{[a,b],\mathrm{cris}}_{\bar{\eta}}[1/p]$ and $R^{\mathrm{cris},\leq\mu}_{\bar{\eta}}[1/p]$ are formally smooth over F. Hence, $\widehat{\mathscr{O}}^{\mu}_{\bar{x}}$ satisfies the hypotheses of Theorem 3.3.13.

By Theorem 3.3.13, we are reduced to showing that for any finite F'/F and any homomorphism $x : \widehat{\mathscr{O}}^{\mu}_{\bar{x}} \to F'$ the filtration $\mathfrak{D}_x$ corresponding to the base change

$\mathfrak{P}_x := \mathfrak{P}_{\widehat{\mathcal{O}}^{\mu}_{\bar{x}}} \otimes_x F'$ has type less than or equal to μ. The homomorphism x corresponds to a closed point of Spec $R^{\text{cris},\leq\mu}_{\bar{\eta}}[1/p]$, i.e., a crystalline representation ρ_x with p-adic Hodge type less than or equal to μ. Furthermore, $\mathfrak{P}_x$ is the unique $(\mathfrak{S}_{F'}, \varphi)$-module of bounded height associated to ρ_x. By Proposition 2.4.9, the de Rham $\mathscr{F}^{\text{dR}}_{\rho_x}$ filtration associated to ρ_x is isomorphic to the filtration $\mathfrak{D}_x$ associated to $(\mathfrak{P}_x, \phi_x)$. Thus, $\mathfrak{D}_x$ has type less than or equal to μ for all points x and so $\mathfrak{P}_{\widehat{\mathcal{O}}^{\mu}_{\bar{x}}} \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}'}}(\widehat{\mathcal{O}}^{\mu}_{\bar{x}})$, by Theorem 3.3.13.

By the argument above, Spec $\widehat{\mathcal{O}}^{\mu}_{\bar{x}}$ and Spec $R^{\text{cris},\mu}_{\bar{x}}$ have the same F'-points for any finite extension of F. Since $R^{\text{cris},\leq\mu}_{\bar{\eta}}[1/p]$ is formally smooth over F, the kernel of $R^{\text{cris},\mu}_{\bar{x}} \to \widehat{\mathcal{O}}^{\mu}_{\bar{x}}$ is p-power torsion. □

Remark 3.3.16. In fact, Corollary 3.3.15 holds as well for semistable deformation rings with p-adic Hodge type less than or equal to μ. To apply Theorem 3.3.13 and make the final deduction, we needed that the generic fiber of the crystalline deformation ring was reduced (to argue at closed points). This is true for G-valued semistable deformation rings by the main result of [Bellovin 2014].

4. Local analysis

In this section, we analyze finer properties of crystalline G-valued deformation rings with minuscule p-adic Hodge type. The techniques in this section are inspired by [Kisin 2009; Liu 2013]. We develop a theory of $(\varphi, \widehat{\Gamma})$-modules with G-structure and our main result, Theorem 4.3.6, is stated in these terms. However, the idea is the following: given a G-Kisin module $(\mathfrak{P}_A, \phi_A)$ over some finite Λ-algebra A, we get a representation of Γ_∞ via the functor $T_{G,\mathfrak{S}_A}$. In general, this representation need not extend (and certainly not in a canonical way) to a representation of the full Galois group Γ_K. When $G = \mathrm{GL}_n$ and $\mathfrak{P}_A$ has height in $[0, 1]$ then, via the equivalence between Kisin modules with height in $[0, 1]$ and finite flat group schemes [Kisin 2006, Theorem 2.3.5], one has a canonical extension to Γ_K which is flat. We show (at least when A is a Λ-flat domain) that the same holds for G-Kisin modules of minuscule type: there exists a canonical extension to Γ_K which is crystalline. This is stated precisely in Corollary 4.3.8. We end by applying this result to identify the connected components of G-valued crystalline deformation rings with the connected components of a moduli space of G-Kisin modules (Corollary 4.4.2).

4.1. ***Minuscule cocharacters.*** We begin with some preliminaries on minuscule cocharacters and adjoint representations which we use in our finer analysis with $(\varphi, \widehat{\Gamma})$-modules in the subsequent sections.

Let H be a reductive group over field κ. The conjugation action of H on itself gives a representation

$$\mathrm{Ad} : H \to \mathrm{GL}(\mathrm{Lie}(H)). \tag{4-1-0-1}$$

This is algebraic, so, for any κ-algebra R, $H(R)$ acts on $\mathrm{Lie}(H_R) = \mathrm{Lie}\, H \otimes_\kappa R$. We will use Ad to denote these actions as well. We can define Ad for G over $\mathrm{Spec}\, \Lambda$ in the same way.

Definition 4.1.1. Any cocharacter $\lambda : \mathbb{G}_{\mathrm{m}} \to H$ gives a grading on $\mathrm{Lie}\, H$ defined by

$$\mathrm{Lie}\, H(i) := \{Y \in \mathrm{Lie}\, H \mid \mathrm{Ad}(\lambda(a))Y = a^i Y\}.$$

A cocharacter λ is called *minuscule* if $\mathrm{Lie}\, H(i) = 0$ for $i \notin \{-1, 0, 1\}$.

Minuscule cocharacters were studied by Deligne [1979] in connection with the theory of Shimura varieties. A detailed exposition of their main properties can be found in §1 of [Gross 2000].

Assume now that H is split and fix a maximal split torus T contained in a Borel subgroup B. This gives rise to a set of simple roots Δ and a set of simple coroots $\Delta^\vee$. In each conjugacy class of cocharacters, there is a unique dominant cocharacter valued in T. The set of dominant cocharacters is denoted by $X_*(T)^+$.

Recall the Bruhat (partial) ordering on $X_*(T)^+$: given dominant cocharacters $\mu, \mu' : \mathbb{G}_{\mathrm{m}} \to T$, we say $\mu' \le \mu$ if $\mu - \mu' = \sum_{\alpha \in \Delta^\vee} n_\alpha \alpha$ with $n_\alpha \ge 0$.

Proposition 4.1.2. *Let μ be a dominant minuscule cocharacter. Then there is no dominant μ' such that $\mu' < \mu$ in the Bruhat order.*

Proof. See Exercise 24 from Chapter IV.1 of [Bourbaki 2002]. □

Proposition 4.1.3. *If μ is a minuscule cocharacter, then the (open) affine Schubert variety $S^0(\mu)$ is equal to $S(\mu)$. Furthermore, $S(\mu)$ is smooth and projective. In fact, $S(\mu) \cong H/P(\mu)$, where $P(\mu)$ is a parabolic subgroup associated to the cocharacter μ.*

Proof. Since the closure $S(\mu) = \bigcup_{\mu' \le \mu} S^0(\mu')$ [Richarz 2013, Proposition 2.8], the first part follows from Proposition 4.1.2. For the remaining facts, we refer to discussion after [Pappas et al. 2013, Definition 1.3.5] and [Levin 2013, Proposition 3.5.7]. □

For any $\mu : \mathbb{G}_{\mathrm{m}} \to T$, we get an induced map $\mathbb{G}_{\mathrm{m}}(\kappa((t))) \to T(\kappa((t))) \subset H(\kappa((t)))$ on loop groups. We let $\mu(t)$ denote the image of $t \in \kappa((t))^\times$.

Proposition 4.1.4. *For any $X \in \mathrm{Lie}\, H \otimes_\kappa \kappa[\![t]\!]$, we have*

$$\mathrm{Ad}(\mu(t))(X) \in \frac{1}{t}(\mathrm{Lie}\, H \otimes_\kappa \kappa[\![t]\!]).$$

Proof. As in Definition 4.1.1, we can decompose

$$\mathrm{Lie}\, H = \mathrm{Lie}\, H(-1) \oplus \mathrm{Lie}\, H \oplus \mathrm{Lie}\, H(1).$$

Then $\mathrm{Ad}(\mu(t))$ acts on $\mathrm{Lie}\, H(i) \otimes \kappa((t))$ by multiplication by t^i. The largest denominator is then t^{-1}. □

4.2. *Theory of $(\varphi, \widehat{\Gamma})$-modules with G-structure.* We review Liu's theory [2010; Caruso and Liu 2011] of $(\varphi, \widehat{G})$. We call them $(\varphi, \widehat{\Gamma})$-modules to avoid confusion with the algebraic group G. The theory of $(\varphi, \widehat{\Gamma})$-modules is an adaptation of the theory of (φ, Γ)-modules to the non-Galois extension $K_\infty = K(\pi^{1/p}, \pi^{1/p^2}, \dots)$. The $\widehat{\Gamma}$ refers to an additional structure added to a Kisin module which captures the full action of Γ_K as opposed to just the subgroup $\Gamma_\infty := \mathrm{Gal}(\overline{K}/K_\infty)$. The main theorem in [Liu 2010] is an equivalence of categories between (torsion-free) $(\varphi, \widehat{\Gamma})$-modules and Γ_K-stable lattices in semistable $\mathbb{Q}_p$-representations.

Let $\widetilde{\boldsymbol{E}}^+$ denote the perfection of $\mathcal{O}_{\overline{K}}/(p)$. There is a unique surjective map

$$\Theta : W(\widetilde{\boldsymbol{E}}^+) \to \widehat{\mathcal{O}}_{\overline{K}}$$

which lifts the projection $\widetilde{\boldsymbol{E}}^+ \to \mathcal{O}_{\overline{K}}/(p)$. The compatible system $(\pi^{1/p^n})_{n \geq 0}$ of the p^n-th roots of π defines an element $\underline{\pi}$ of $\widetilde{\boldsymbol{E}}^+$. Let $[\underline{\pi}]$ denote the Teichmüller representative in $W(\widetilde{\boldsymbol{E}}^+)$. There is an embedding

$$\mathfrak{S} \hookrightarrow W(\widetilde{\boldsymbol{E}}^+),$$

defined by $u \mapsto [\underline{\pi}]$, which is compatible with the Frobenii. If $\widetilde{\boldsymbol{E}}$ is the fraction field of $\widetilde{\boldsymbol{E}}^+$, then $W(\widetilde{\boldsymbol{E}}^+) \subset W(\widetilde{\boldsymbol{E}})$. The embedding $\mathfrak{S} \hookrightarrow W(\widetilde{\boldsymbol{E}}^+)$ extends to an embedding

$$\mathcal{O}_{\mathcal{E}} \hookrightarrow W(\widetilde{\boldsymbol{E}}).$$

As before, let $K_\infty = \bigcup K(\pi^{1/p^n})$. Set $K_{p^\infty} := \bigcup K(\zeta_{p^n})$, where ζ_{p^n} is a primitive p^n-th root of unity. Denote the compositum of K_∞ and K_{p^∞} by K_{∞,p^∞}; K_{∞,p^∞} is Galois over K.

Definition 4.2.1. Define

$$\widehat{\Gamma} := \mathrm{Gal}(K_{\infty,p^\infty}/K) \quad \text{and} \quad \widehat{\Gamma}_\infty := \mathrm{Gal}(K_{\infty,p^\infty}/K_\infty).$$

There is a subring $\widehat{R} \subset W(\widetilde{\boldsymbol{E}}^+)$ which plays a central role in the theory of $(\varphi, \widehat{\Gamma})$-modules. The definition can be found on p. 5 of [Liu 2010]. The relevant properties of $\widehat{R}$ are

(1) $\widehat{R}$ is stable by the Frobenius on $W(\widetilde{\boldsymbol{E}}^+)$;

(2) $\widehat{R}$ contains $\mathfrak{S}$;

(3) $\widehat{R}$ is stable under the action of the Galois group Γ_K and Γ_K acts through the quotient $\widehat{\Gamma}$.

For any $\mathbb{Z}_p$-algebra A, set $\widehat{R}_A := \widehat{R} \otimes_{\mathbb{Z}_p} A$ with a Frobenius induced by the Frobenius on $\widehat{R}$. Similarly, define $W(\widetilde{\boldsymbol{E}}^+)_A := W(\widetilde{\boldsymbol{E}}^+) \otimes_{\mathbb{Z}_p} A$ and $W(\widetilde{\boldsymbol{E}})_A := W(\widetilde{\boldsymbol{E}}) \otimes_{\mathbb{Z}_p} A$. For any $\mathfrak{S}_A$-module $\mathfrak{M}_A$, define

$$\widehat{\mathfrak{M}}_A := \widehat{R}_A \otimes_{\varphi, \mathfrak{S}_A} \mathfrak{M}_A = \widehat{R}_A \otimes_{\mathfrak{S}_A} \varphi^*(\mathfrak{M}_A)$$

and

$$\widetilde{\mathfrak{M}}_A := W(\widetilde{\boldsymbol{E}}^+)_A \otimes_{\varphi,\mathfrak{S}_A} \mathfrak{M}_A = W(\widetilde{\boldsymbol{E}}^+)_A \otimes_{\hat{R}_A} \widehat{\mathfrak{M}}_A.$$

Recall that $\varphi^*(\mathfrak{M}_A) := \mathfrak{S}_A \otimes_{\varphi,\mathfrak{S}_A} \mathfrak{M}_A$ and that the linearized Frobenius is a map $\phi_{\mathfrak{M}_A} : \varphi^*(\mathfrak{M}_A) \to \mathfrak{M}_A$ (when $\mathfrak{M}_A$ has height in $[0, \infty)$).

If $\mathfrak{M}_A$ is a projective $\mathfrak{S}_A$-module then, by Lemma 3.1.1 in [Caruso and Liu 2011], $\varphi^*(\mathfrak{M}_A) \subset \widehat{\mathfrak{M}}_A \subset \widetilde{\mathfrak{M}}_A$. Although the map $m \mapsto 1 \otimes m$ from $\mathfrak{M}_A$ to $\widehat{\mathfrak{M}}_A$ is not $\mathfrak{S}_A$-linear, it is injective when $\mathfrak{M}_A$ is $\mathfrak{S}_A$-projective. The image is a $\varphi(\mathfrak{S}_A)$-submodule of $\widehat{\mathfrak{M}}_A$. We will think of $\mathfrak{M}_A$ inside of $\widehat{\mathfrak{M}}_A$ in this way. Finally, for any étale $(\mathcal{O}_{\mathcal{E},A}, \varphi)$-module $\mathcal{M}_A$, we define

$$\widetilde{\mathcal{M}}_A := W(\widetilde{\boldsymbol{E}})_A \otimes_{\varphi,\mathcal{O}_{\mathcal{E},A}} \mathcal{M}_A = W(\widetilde{\boldsymbol{E}})_A \otimes_{\mathcal{O}_{\mathcal{E},A}} \varphi^*(\mathcal{M}_A)$$

with semilinear Frobenius extending the Frobenius on $\mathcal{M}_A$. To summarize, for any Kisin module $(\mathfrak{M}_A, \phi_A)$, we have the diagram

$$\begin{array}{ccccc} (\mathfrak{M}_A, \phi_A) & \rightsquigarrow & \widehat{\mathfrak{M}}_A & \rightsquigarrow & \widetilde{\mathfrak{M}}_A \\ \wr\downarrow & & & & \wr\downarrow \\ (\mathcal{M}_A, \phi_A) & & \rightsquigarrow & & (\widetilde{\mathcal{M}}_A, \tilde{\phi}_A). \end{array}$$

Now, let $\gamma \in \hat{\Gamma}$ and let $\widehat{\mathfrak{M}}_A$ be an $\hat{R}_A$-module. A map $g : \widehat{\mathfrak{M}}_A \to \widehat{\mathfrak{M}}_A$ is γ*-semilinear* if

$$g(am) = \gamma(a)g(m)$$

for any $a \in \hat{R}_A$, $m \in \widehat{\mathfrak{M}}_A$. A (semilinear) $\hat{\Gamma}$-action on $\widehat{\mathfrak{M}}_A$ is a γ-semilinear map g_γ for each $\gamma \in \hat{\Gamma}$ such that

$$g_{\gamma'} \circ g_\gamma = g_{\gamma'\gamma}$$

as $(\gamma'\gamma)$-semilinear morphisms. A (semilinear) $\hat{\Gamma}$-action on $\widehat{\mathfrak{M}}_A$ extends in the natural way to a (semilinear) Γ_K-action on $\widetilde{\mathfrak{M}}_A$ and on $\widetilde{\mathcal{M}}_A$.

For any local Artinian $\mathbb{Z}_p$-algebra A, choose a $\mathbb{Z}_p$-module isomorphism $A \cong \bigoplus \mathbb{Z}/p^{n_i}\mathbb{Z}$ so that, as a $W(\widetilde{\boldsymbol{E}})$-module, $W(\widetilde{\boldsymbol{E}})_A \cong \bigoplus W_{n_i}(\widetilde{\boldsymbol{E}})$. We equip $W(\widetilde{\boldsymbol{E}})_A$ with the product topology, where $W_{n_i}(\widetilde{\boldsymbol{E}})$ has a topology induced by the isomorphism $W_{n_i}(\widetilde{\boldsymbol{E}}) \cong \widetilde{\boldsymbol{E}}^{n_i}$ given by Witt components (see §4.3 of [Brinon and Conrad 2009] for more details on the topology of $\widetilde{\boldsymbol{E}}$). We can similarly define a topology on $W(\widetilde{\boldsymbol{E}}^+)_A$ using the topology on $\widetilde{\boldsymbol{E}}^+$, and it is clear that this is the same as the subspace topology from the inclusion $W(\widetilde{\boldsymbol{E}}^+)_A \subset W(\widetilde{\boldsymbol{E}})_A$. Finally, we give $\hat{R}_A$ the subspace topology from the inclusion $\hat{R}_A \subset W(\widetilde{\boldsymbol{E}}^+)_A$. The same procedure works for A finite flat over $\mathbb{Z}_p$.

A $\widehat{\Gamma}$-action on $\widehat{\mathfrak{M}}_A$ is *continuous* if, for any basis (equivalently for all bases) of $\widehat{\mathfrak{M}}_A$, the induced map $\widehat{\Gamma} \to \mathrm{GL}_r(\widehat{R}_A)$ is continuous, where r is the rank of $\widehat{\mathfrak{M}}_A$ (such a basis exists by [Kisin 2009, Lemma 1.2.2(4)]).

Definition 4.2.2. Let A be a finite $\mathbb{Z}_p$-algebra. A $(\varphi, \widehat{\Gamma})$*-module with height in* $[a, b]$ over A is a triple $(\mathfrak{M}_A, \phi_{\mathfrak{M}_A}, \widehat{\Gamma})$, where

(1) $(\mathfrak{M}_A, \phi_{\mathfrak{M}_A}) \in \mathrm{Mod}^{\varphi,[a,b]}_{\mathfrak{S}_A}$;

(2) $\widehat{\Gamma}$ is a continuous (semilinear) $\widehat{\Gamma}$-action on $\widehat{\mathfrak{M}}_A$;

(3) the Γ_K-action on $\widetilde{\mathfrak{M}}_A$ commutes with $\tilde{\phi}_{\mathfrak{M}_A}$ (as endomorphisms of $\widetilde{\mathcal{M}}_A$);

(4) regarding $\mathfrak{M}_A$ as a $\varphi(\mathfrak{S}_A)$-submodule of $\widehat{\mathfrak{M}}_A$, we have $\mathfrak{M}_A \subset \widehat{\mathfrak{M}}_A^{\widehat{\Gamma}_\infty}$;

(5) $\widehat{\Gamma}$ acts trivially on $\widehat{\mathfrak{M}}_A / I_+(\widehat{\mathfrak{M}}_A)$ (see §3.1 of [Caruso and Liu 2011] for the definition of $I_+(\widehat{\mathfrak{M}}_A)$).

We often refer to the additional data of a $(\varphi, \widehat{\Gamma})$-module on a Kisin module as a $\widehat{\Gamma}$*-structure*.

Remark 4.2.3. Although we allow arbitrary height $[a, b]$ (in particular, negative height), the ring $\widehat{R}$ is still sufficient for defining the $\widehat{\Gamma}$-action. This follows from the fact that the $\widehat{\Gamma}$-action on $\mathfrak{S}(1)$ is given by $\hat{c}$ (see [Liu 2010, Example 3.2.3]), which is a unit in $\widehat{R}$. See also [Levin 2013, Example 9.1.9].

Proposition 4.2.4. *Choose* $(\mathfrak{M}_A, \phi_{\mathfrak{M}_A}) \in \mathrm{Mod}^{\varphi,[a,b]}_{\mathfrak{S}_A}$ *of rank* r. *Fix a basis* $\{f_i\}$ *of* $\mathfrak{M}_A$. *Let* C' *be the matrix for* $\phi_{\mathfrak{M}_A}$ *with respect to* $\{1 \otimes_\varphi f_i\}$. *Then a* $\widehat{\Gamma}$*-structure on* $\mathfrak{M}_A$ *is the same as a continuous map*

$$B_\bullet : \widehat{\Gamma} \to \mathrm{GL}_r(\widehat{R}_A)$$

such that

(i) $C' \cdot \varphi(B_\gamma) = B_\gamma \cdot \gamma(C')$ *in* $\mathrm{Mat}(W(\widetilde{\boldsymbol{E}})_A)$ *for all* $\gamma \in \widehat{\Gamma}$;

(ii) $B_\gamma = \mathrm{Id}$ *for all* $\gamma \in \widehat{\Gamma}_\infty$;

(iii) $B_\gamma \equiv \mathrm{Id} \bmod I_+(\widehat{R})_A$ *for all* $\gamma \in \widehat{\Gamma}$;

(iv) $B_{\gamma\gamma'} = B_\gamma \cdot \gamma(B_{\gamma'})$ *for all* $\gamma, \gamma' \in \widehat{\Gamma}$.

Let $\mathrm{Mod}^{\varphi,[a,b],\widehat{\Gamma}}_{\mathfrak{S}_A}$ denote the category of $(\varphi, \widehat{\Gamma})$-modules with height in $[a, b]$ over A. A morphism between $(\varphi, \widehat{\Gamma})$-modules is a morphism in $\mathrm{Mod}^{\varphi,[a,b]}_{\mathfrak{S}_A}$ that is $\widehat{\Gamma}$-equivariant when extended to $\widehat{R}_A$.

Let $\mathrm{Mod}^{\varphi,\mathrm{bh},\widehat{\Gamma}}_{\mathfrak{S}_A} := \bigcup_{h>0} \mathrm{Mod}^{\varphi,[-h,h],\widehat{\Gamma}}_{\mathfrak{S}_A}$, so $\mathrm{Mod}^{\varphi,\mathrm{bh},\widehat{\Gamma}}_{\mathfrak{S}_A}$ has a natural tensor product operation which at the level of $\mathrm{Mod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_A}$ is the tensor product of bounded height Kisin modules. The $\widehat{\Gamma}$-structure on the tensor product is defined via

$$\widehat{R}_A \otimes_{\varphi,\mathfrak{S}_A} (\mathfrak{M}_A \otimes_{\mathfrak{S}_A} \mathfrak{N}_A) \cong (\widehat{R}_A \otimes_{\varphi,\mathfrak{S}_A} \mathfrak{M}_A) \otimes_{\widehat{R}_A} (\widehat{R}_A \otimes_{\varphi,\mathfrak{S}_A} \mathfrak{N}_A) = \widehat{\mathfrak{M}}_A \otimes_{\widehat{R}_A} \widehat{\mathfrak{N}}_A.$$

One also defines a $\widehat{\Gamma}$-structure on the dual $\mathfrak{M}_A^{\vee} := \mathrm{Hom}_{\mathfrak{S}_A}(\mathfrak{M}_A, \mathfrak{S}_A)$ in the natural way (see the discussion after [Levin 2013, Proposition 9.1.5]). Note that, unlike in other references (for example [Ozeki 2013]), we do not include any Tate twist in our definition of duals.

We will now relate these $(\varphi, \widehat{\Gamma})$-modules to Γ_K-representations. For this, we require that A be $\mathbb{Z}_p$-finite and either $\mathbb{Z}_p$-flat or Artinian. Define a functor $\widehat{T}_A$ from $\mathrm{Mod}_{\mathfrak{S}_A}^{\varphi,\mathrm{bh},\widehat{\Gamma}}$ to Galois representations by

$$\widehat{T}_A(\widehat{\mathfrak{M}}_A) := (W(\widetilde{\boldsymbol{E}}) \otimes_{\widehat{R}} \widehat{\mathfrak{M}}_A)^{\tilde{\phi}_A=1} = (\widetilde{\mathcal{M}}_A)^{\tilde{\phi}_A=1}.$$

The semilinear Γ_K-action on $\widetilde{\mathcal{M}}_A$ commutes with $\tilde{\phi}_A$, so $\widehat{T}_A(\widehat{\mathfrak{M}}_A)$ is a Γ_K-stable A-submodule of $W(\widetilde{\boldsymbol{E}}) \otimes_{\widehat{R}} \widehat{\mathfrak{M}}_A$.

We now recall the basic facts we will need about $\widehat{T}_A$:

Proposition 4.2.5. *Let A be $\mathbb{Z}_p$-finite and either $\mathbb{Z}_p$-flat or Artinian.*

(1) *If $\widehat{\mathfrak{M}}_A \in \mathrm{Mod}_{\mathfrak{S}_A}^{\varphi,\mathrm{bh},\widehat{\Gamma}}$, then there is a natural $A[\Gamma_\infty]$-module isomorphism*

$$\theta_A : T_{\mathfrak{S}_A}(\mathfrak{M}_A) \to \widehat{T}_A(\widehat{\mathfrak{M}}_A).$$

Furthermore, θ_A is functorial with respect to morphisms in $\mathrm{Mod}_{\mathfrak{S}_A}^{\varphi,\mathrm{bh},\widehat{\Gamma}}$.

(2) *$\widehat{T}_A$ is an exact tensor functor from $\mathrm{Mod}_{\mathfrak{S}_A}^{\varphi,\mathrm{bh},\widehat{\Gamma}}$ to $\mathrm{Rep}_A(\Gamma_K)$ which is compatible with duals.*

Proof. See [Levin 2013, Propositions 9.1.6 and 9.1.7]. □

We are now ready to add G-structure to $(\varphi, \widehat{\Gamma})$-modules. Let G be a connected reductive group over a $\mathbb{Z}_p$-finite and flat local domain Λ as in previous sections.

Definition 4.2.6. Define $\mathrm{GMod}_{\mathfrak{S}_A}^{\varphi,\widehat{\Gamma}}$ to be the category of faithful exact tensor functors $[{}^f\mathrm{Rep}_\Lambda(G), \mathrm{Mod}_{\mathfrak{S}_A}^{\varphi,\mathrm{bh},\widehat{\Gamma}}]^{\otimes}$. We will refer to these as *$(\varphi, \widehat{\Gamma})$-modules with G-structure*.

Recall the category $\mathrm{GRep}_A(\Gamma_K)$ from Definition 2.2.3. By Proposition 4.2.5(2), $\widehat{T}_A$ induces a functor

$$\widehat{T}_{G,A} : \mathrm{GMod}_{\mathfrak{S}_A}^{\varphi,\widehat{\Gamma}} \to \mathrm{GRep}_A(\Gamma_K).$$

Furthermore, if $\omega_{\Gamma_\infty} : \mathrm{GRep}_A(\Gamma_K) \to \mathrm{GRep}_A(\Gamma_\infty)$ is the forgetful functor then there is an natural isomorphism

$$T_{G,\mathfrak{S}_A} \cong \omega_{\Gamma_\infty} \circ \widehat{T}_{G,A}.$$

The functor $\widehat{T}_{G,A}$ behaves well with respect to base change along finite maps $A \to A'$ by the same argument as in Proposition 2.2.4.

We end this section by adding G-structure to the main result of [Liu 2010]. For A finite flat over Λ, an element (P_A, ρ_A) of $\mathrm{GRep}_A(\Gamma_K)$ is *semistable* (resp. *crystalline*) if $\rho_A[1/p] : \Gamma_K \to \mathrm{Aut}_G(P_A)(A[1/p])$ is semistable (resp. crystalline). For A a local domain and ρ_A semistable, we say ρ_A has *p-adic Hodge type μ* if $\rho_A[1/p]$ does for any trivialization of P_A (see Definition 2.4.5).

Theorem 4.2.7. *Let F'/F be a finite extension with ring of integers Λ'. The functor $\widehat{T}_{G,\Lambda'}$ induces an equivalence of categories between $\mathrm{GMod}_{\mathfrak{S}_{\Lambda'}}^{\varphi,\widehat{\Gamma}}$ and the full subcategory of semistable representations of* $\mathrm{GRep}_{\Lambda'}(\Gamma_K)$.

Proof. Using the Tannakian description of both categories, it suffices to show that $\widehat{T}_{\Lambda'}$ defines a tensor equivalence between $\mathrm{Mod}_{\mathfrak{S}_{\Lambda'}}^{\varphi,\mathrm{bh},\widehat{\Gamma}}$ and semistable representations of Γ_K on finite free Λ'-modules. When $F = \mathbb{Q}_p$ and the Hodge–Tate weights are negative (in our convention), this is Theorem 2.3.1 in [Liu 2010]. Note that Liu uses contravariant functors, so that our $\widehat{T}_{\Lambda'}$ is obtained by taking duals. The restriction on Hodge–Tate weights can be removed by twisting by $\widehat{\mathfrak{S}}(1)$, the $(\varphi, \widehat{\Gamma})$-module corresponding to the inverse of the p-adic cyclotomic character.

To define a quasi-inverse to $\widehat{T}_{\Lambda'}$, let L be a semistable Γ_K-representation on a finite free Λ'-module. Forgetting the coefficients, Liu [2010] constructs a $\widehat{\Gamma}$-structure $\widehat{T}^{-1}(L)$ on the unique Kisin lattice in $\underline{M}(L)$. This $(\varphi, \widehat{\Gamma})$-module over $\mathbb{Z}_p$ has an action of Λ', by functoriality of the construction. By an argument as in [Kisin 2008, Proposition 1.6.4(2)], the resulting $\mathfrak{S}_{\Lambda'}$-module is projective, so this defines an object of $\mathrm{Mod}_{\mathfrak{S}_{\Lambda'}}^{\varphi,\mathrm{bh},\widehat{\Gamma}}$, which we call $\widehat{T}_{\Lambda'}^{-1}(L)$.

Finally, we appeal to Proposition I.4.4.2 in [Saavedra Rivano 1972] to conclude that $\widehat{T}_{\Lambda'}$ and $\widehat{T}_{\Lambda'}^{-1}$ define a tensor equivalence of categories given that $\widehat{T}_{\Lambda'}$ respects tensor products (Proposition 4.2.5). □

4.3. *Faithfulness and existence result.* Fix an element $\tau \in \widehat{\Gamma}$ such that $\tau(\underline{\pi}) = \underline{\varepsilon} \cdot \underline{\pi}$, where $\underline{\varepsilon}$ is a compatible system of primitive p^n-th roots of unity. If $p \neq 2$, then τ is a topological generator for $\widehat{\Gamma}_{p^\infty} := \mathrm{Gal}(K_{\infty,p^\infty}/K_{p^\infty})$. If $p = 2$, then some power of τ will generate $\widehat{\Gamma}_{p^\infty}$. In both cases, τ together with $\widehat{\Gamma}_\infty$ topologically generate $\widehat{\Gamma}$ (see [Liu 2010, §4.1]). Given condition (4) in Definition 4.2.2, the $\widehat{\Gamma}$-action is determined by the action of τ.

Recall the element $\mathfrak{t} \in W(\widetilde{\boldsymbol{E}}^+)$, which is the period for $\mathfrak{S}(1)$ in the sense that $\varphi(\mathfrak{t}) = c_0^{-1} E(u)\mathfrak{t}$. We will need a few structural results about $W(\widetilde{\boldsymbol{E}}^+)$.

Lemma 4.3.1. *For any $\tilde{\gamma} \in \Gamma_K$, we have the following divisibilities in $W(\widetilde{\boldsymbol{E}}^+)$:*

$$\tilde{\gamma}(u) \mid u, \quad \tilde{\gamma}(\varphi(\mathfrak{t})) \mid \varphi(\mathfrak{t}), \quad \textit{and} \quad \tilde{\gamma}(E(u)) \mid E(u).$$

Proof. See [Levin 2013, Lemma 9.3.1]. □

The $(\varphi, \widehat{\Gamma})$-modules which give rise to crystalline representations satisfy an extra divisibility condition on the action of τ [Gee et al. 2014, Corollary 4.10; Levin 2013, Proposition 9.3.4]. We call this the *crystalline condition*.

Definition 4.3.2. An object $\widehat{\mathfrak{M}}_A \in \mathrm{Mod}_{\mathfrak{S}_A}^{\varphi,[a,b],\widehat{\Gamma}}$ is *crystalline* if, for any $x \in \mathfrak{M}_A$, there exists $y \in \widetilde{\mathfrak{M}}_A$ such that $\tau(x) - x = \varphi(\mathfrak{t}) u^p y$.

Proposition 4.3.3. *If $\widehat{\mathfrak{M}}_A$ is crystalline then, for all $x \in \mathfrak{M}_A$ and $\gamma \in \widehat{\Gamma}$, there exists $y \in \widetilde{\mathfrak{M}}_A$ such that $\gamma(x) - x = \varphi(\mathfrak{t}) u^p y$.*

Proof. This is an easy calculation using that $\widehat{\Gamma}$ is topologically generated by $\widehat{\Gamma}_\infty$ and τ [Levin 2013, Proposition 9.3.3]. □

Definition 4.3.4. We say an object $\widehat{\mathfrak{P}}_A \in \mathrm{GMod}_{\mathfrak{S}_A}^{\varphi,[a,b],\widehat{\Gamma}}$ is *crystalline* if $\widehat{\mathfrak{P}}_A(W)$ is crystalline for all $W \in {}^f\mathrm{Rep}_\Lambda(G)$. For an object $\widehat{\mathfrak{P}}_{\mathbb{F}} \in \mathrm{GMod}_{\mathfrak{S}_{\mathbb{F}}}^{\varphi,[a,b],\widehat{\Gamma}}$, define the *crystalline $(\varphi, \widehat{\Gamma})$-module deformation groupoid* over $\mathscr{C}_\Lambda$ by

$$D_{\widehat{\mathfrak{P}}_{\mathbb{F}}}^{\mathrm{cris},[a,b]}(A) = \{(\widehat{\mathfrak{P}}_A, \psi_0) \in D_{\widehat{\mathfrak{P}}_{\mathbb{F}}}^{[a,b]}(A) \mid \widehat{\mathfrak{P}}_A \text{ is crystalline}\}$$

for any $A \in \mathscr{C}_\Lambda$.

Proposition 4.3.5. *Let F' be a finite extension of F with ring of integers Λ'. The equivalence from Theorem 4.2.7 induces an equivalence between the full subcategory of crystalline objects in $\mathrm{GMod}_{\mathfrak{S}_{\Lambda'}}^{\varphi,\widehat{\Gamma}}$ with the category of crystalline representations in $\mathrm{GRep}_{\Lambda'}(\Gamma_K)$.*

Proof. It suffices to show that if $\widehat{T}_A(\widehat{\mathfrak{P}}_A(W))$ is a lattice in a crystalline representation then $\widehat{\mathfrak{P}}_A(W)$ satisfies the crystalline condition. This only depends on the underlying $(\varphi, \widehat{\Gamma})$-module so we can take $A = \mathbb{Z}_p$. When $p > 2$, this is proven in Corollary 4.10 in [Gee et al. 2014]. The argument for $p = 2$ is essentially the same and was omitted only because in [Gee et al. 2014] they need further divisibilities on $(\tau - 1)^n$, for which $p = 2$ becomes more complicated. Details can be found in [Levin 2013, Proposition 9.3.4]. □

Choose a crystalline object $\widehat{\mathfrak{P}}_{\mathbb{F}} \in \mathrm{GMod}_{\mathfrak{S}_{\mathbb{F}}}^{\varphi,[a,b],\widehat{\Gamma}}$. If $\mathfrak{P}_{\mathbb{F}}$ is the underlying G-Kisin module of $\widehat{\mathfrak{P}}_{\mathbb{F}}$, then we would like to study the forgetful functor

$$\widehat{\Delta} : D_{\widehat{\mathfrak{P}}_{\mathbb{F}}}^{\mathrm{cris},[a,b]} \to D_{\mathfrak{P}_{\mathbb{F}}}^{[a,b]}.$$

More specifically, if μ and a, b are as in the discussion before Definition 3.3.8, and $F = F_{[\mu]}$, we consider

$$\widehat{\Delta}^\mu : D_{\widehat{\mathfrak{P}}_{\mathbb{F}}}^{\mathrm{cris},\mu} := D_{\widehat{\mathfrak{P}}_{\mathbb{F}}}^{\mathrm{cris},[a,b]} \times_{D_{\mathfrak{P}_{\mathbb{F}}}^{[a,b]}} D_{\mathfrak{P}_{\mathbb{F}}}^{\mu} \to D_{\mathfrak{P}_{\mathbb{F}}}^{\mu}.$$

We can now state our main theorem:

Theorem 4.3.6. *Assume that p does not divide $\pi_1(G^{\mathrm{der}})$, where G^{der} is the derived group of G, and that $F = F_{[\mu]}$. If μ is a minuscule geometric cocharacter of* $\mathrm{Res}_{(K \otimes_{\mathbb{Q}_p} F)/F} G_F$ *then*

$$\widehat{\Delta}^{\mu} : D^{\mathrm{cris},\mu}_{\widehat{\mathfrak{P}}_{\mathbb{F}}} \to D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$$

is an equivalence of groupoids over $\mathscr{C}_{\Lambda}$.

Remark 4.3.7. This generalizes [Levin 2013, Theorem 9.3.13], where we worked with G-Kisin modules with height in $[0, 1]$. See Remark 1.1.1 for more information.

Corollary 4.3.8. *Assume $F = F_{[\mu]}$ and that μ is minuscule. Let F' be a finite extension of F with ring of integers Λ'. There is an equivalence of categories between G-Kisin modules over $\mathfrak{S}_{\Lambda'}$ with p-adic Hodge type μ and the subcategory of* $\mathrm{GRep}_{\Lambda'}(\Gamma_K)$ *consisting of crystalline representations with p-adic Hodge type μ.*

Corollary 4.3.8 follows from the proof of Theorem 4.3.6. It generalizes the equivalence between Kisin modules of Barsotti–Tate type and lattices in crystalline representations with Hodge–Tate weights in $\{-1, 0\}$ [Kisin 2006, Theorem 2.2.7]. Note that we do not require $p \nmid |\pi_1(G^{\mathrm{der}})|$ here. For the relevant definitions, see Definition 3.3.12 and the discussion before Theorem 4.2.7. Before proving Theorem 4.3.6 and Corollary 4.3.8, we begin with some preliminaries on crystalline $(\varphi, \widehat{\Gamma})$-modules with G-structure.

Definition 4.3.9. Define $G(u^{p^i})$ to be the kernel of the reduction map

$$G(W(\widetilde{\boldsymbol{E}}^{+})_A) \to G(W(\widetilde{\boldsymbol{E}}^{+})_A/(\varphi(\mathrm{t})u^{p^i})).$$

Proposition 4.3.10. *Choose $(\mathfrak{P}_A, \phi_{\mathfrak{P}_A}) \in \mathrm{GMod}^{\varphi,\mathrm{bh}}_{\mathfrak{S}_A}$. Fix a trivialization β_A of $\mathfrak{P}_A$. Let $C' \in G(\mathfrak{S}_A[1/\varphi(E(u))])$ be $\phi_{\mathfrak{P}_A}$ with respect to the trivialization $1 \otimes_{\varphi} \beta_A$. Then a crystalline $\widehat{\Gamma}$-structure on $\mathfrak{P}_A$ is the same as a continuous map*

$$B_{\bullet} : \widehat{\Gamma} \to G(\widehat{R}_A)$$

satisfying the following properties:

(a) $C' \cdot \varphi(B_\gamma) = B_\gamma \cdot \gamma(C')$ *in* $G(W(\widetilde{\boldsymbol{E}})_A)$ *for all* $\gamma \in \widehat{\Gamma}$;

(b) $B_\gamma = \mathrm{Id}$ *for all* $\gamma \in \widehat{\Gamma}_\infty$;

(c) $B_\gamma \in G(u^p)$ *for all* $\gamma \in \widehat{\Gamma}$;

(d) $B_{\gamma\gamma'} = B_\gamma \cdot \gamma(B_{\gamma'})$ *for all* $\gamma, \gamma' \in \widehat{\Gamma}$.

Proof. Everything follows directly from Proposition 4.2.4. The only point to note is that $(u^p \varphi(\mathrm{t})) \subset I_+(\widehat{R})_A$ because $u \in I_+(\widehat{R})$. Hence, the crystalline condition, which is equivalent to condition (c), implies condition (5) of Definition 4.2.2. □

Before we begin the proof of Theorem 4.3.6, we have two important lemmas.

Lemma 4.3.11. *Let $\mathfrak{P}_A \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$ and choose a trivialization β_A of the bundle $\mathfrak{P}_A$. If $C \in G(\mathfrak{S}_A[1/E(u)])$ is the Frobenius with respect to β_A then, for any $Y \in G(u^{p^i})$,*

$$\varphi(C)\varphi(Y)\varphi(C)^{-1} \in G(u^{p^{i+1}}),$$

where $\varphi(C) = C' \in G(W(\widetilde{\boldsymbol{E}})_A)$ is the Frobenius with respect to $1 \otimes_{\varphi} \beta_A$.

Proof. Let $\mathcal{O}_G$ denote the coordinate ring of G and let I_e be the ideal defining the identity, so that $\mathcal{O}_G/I_e = \Lambda$ and $I_e/I_e^2 \cong (\mathrm{Lie}(G))^{\vee}$. Then $G(u^{p^i})$ is identified with

$$\{Y \in \mathrm{Hom}_{\Lambda}(\mathcal{O}_G, W(\widetilde{\boldsymbol{E}}^+)_A) \mid Y(I_e) \subset (\varphi(\mathrm{t})u^{p^i})\}.$$

Conjugation by C induces an automorphism of $G_{\mathfrak{S}_A[1/E(u)]}$. Let

$$\mathrm{Ad}_{\mathcal{O}_G}(C)^* : \mathcal{O}_G \otimes_{\Lambda} \mathfrak{S}_A[1/E(u)] \to \mathcal{O}_G \otimes_{\Lambda} \mathfrak{S}_A[1/E(u)]$$

be the corresponding map on coordinate rings. The key observation is that

$$\mathrm{Ad}_{\mathcal{O}_G}(C)^*(I_e \otimes 1) \subset \sum_{j \geq 1} I_e^j \otimes_{\Lambda} E(u)^{-j}\mathfrak{S}_A. \tag{4-3-11-1}$$

By successive approximation, one is reduced to studying the induced automorphism of

$$\bigoplus_{j \geq 0} \big(I_e^j/I_e^{j+1} \otimes_{\Lambda} \mathfrak{S}_A[1/E(u)]\big).$$

The j-th graded piece is $\mathrm{Sym}^j(\mathrm{Lie}(G)^{\vee}) \otimes_{\Lambda} \mathfrak{S}_A[1/E(u)]$ as a representation of $G(\mathfrak{S}_A[1/E(u)])$. Since μ is minuscule, $\mathrm{Lie}(G) \otimes_{\Lambda} \mathfrak{S}_A$ has height in $[-1, 1]$ and so $\mathrm{Sym}^j(\mathrm{Lie}(G)^{\vee} \otimes_{\Lambda} \mathfrak{S}_A)$ has height in $[-j, j]$. Thus,

$$\mathrm{Ad}_{\mathcal{O}_G}(C)^*\big(\mathrm{Sym}^j(\mathrm{Lie}(G)^{\vee} \otimes_{\Lambda} \mathfrak{S}_A)\big) \subset E(u)^{-j}(\mathrm{Sym}^j(\mathrm{Lie}(G)^{\vee}) \otimes_{\Lambda} \mathfrak{S}_A),$$

from which one deduces (4-3-11-1).

Let $Y \in G(u^{p^i})$. Then $\varphi(Y)(I_e) \subset \varphi(\varphi(\mathrm{t})u^{p^i}) \subset \big(\varphi(E(u))\varphi(\mathrm{t})u^{p^{i+1}}\big)$. For any $x \in I_e$,

$$(\varphi(C)\varphi(Y)\varphi(C)^{-1})(x) = (\varphi(Y) \otimes 1)\big((1 \otimes \varphi)(\mathrm{Ad}_{\mathcal{O}_G}(C)^*(x))\big),$$

which is a priori only in $W(\widetilde{\boldsymbol{E}})_A$. But since for any $b \in I_e^j$, $\varphi(Y)(b)$ is divisible by $\varphi(E(u))^j \varphi(\mathrm{t})^j u^{jp^{i+1}}$, we have $\mathrm{Ad}(\varphi(C))(\varphi(Y))(x) \in (\varphi(\mathrm{t})u^{p^{i+1}})$ so $\varphi(C)\varphi(Y)\varphi(C)^{-1}$ lies in $G(u^{p^{i+1}})$. □

By [Kisin 2006, Corollary 1.3.15], a Γ_{∞}-representation coming from a finite-height, torsion-free Kisin module $\mathfrak{M}$ extends to a crystalline Γ_K-representation if and only if the canonical Frobenius equivariant connection on $\mathfrak{M} \otimes_{\mathfrak{S}} \mathcal{O}[1/\lambda]$ has at most logarithmic poles. Kisin [2006, Proposition 2.2.2] states furthermore that if $\mathfrak{M}$ has height in [0, 1] then the condition of logarithmic poles is always satisfied.

The following lemma is a version of that proposition for G-Kisin modules with minuscule type:

Lemma 4.3.12. *Let F'/F be a finite extension containing $F_{[\mu]}$ and let $(\mathfrak{P}_{F'}, \phi_{F'})$ be a G-Kisin module over F'. Fix a trivialization of $\mathfrak{P}_{F'}$; let $C \in G(\mathfrak{S}_{F'}[1/E(u)])$ be the Frobenius with respect to this trivialization. If the G-filtration $\mathfrak{D}_{\mathfrak{P}_{F'}}$ over $K \otimes_{\mathbb{Q}_p} F'$ defined before Lemma* 3.3.11 *has type μ, then the right logarithmic derivative $(dC/du)\cdot C^{-1} \in (\mathrm{Lie}\, G \otimes \mathfrak{S}_{F'}[1/E(u)])$ has at most logarithmic poles along $E(u)$, i.e., lies in $E(u)^{-1}(\mathrm{Lie}\, G \otimes \mathfrak{S}_{F'})$.*

Proof. Choose an embedding $\sigma : K_0 \to F'$. Without loss of generality, we assume that $\sigma(E(u))$ splits in F' and write $\sigma(E(u)) = \prod_{i=1}^{e}(u - \psi_i(\pi))$ over embeddings $\psi_i : K \to F'$ which extend σ. Let C_σ denote the σ-component of C under the decomposition of $\mathfrak{S}_{F'}[1/E(u)]$ as a $W \otimes_{\mathbb{Z}_p} F' \cong \prod_{K_0 \to F'} F'$-algebra. We can furthermore compute the "pole" at $\psi_i(\pi)$ by working in the completion at $u - \psi_i(\pi)$, which is isomorphic to $F'[\![t]\!]$ with $t = u - \psi_i(\pi)$.

Let $\mu_{\psi_i} \in X_*(G_F)$ be the ψ_i-component of μ. Fix a maximal torus T of $G_{F'}$ such that μ_{ψ_i} factors through T. The Cartan decomposition for $G(F'((t)))$ combined with the assumption that $\mathfrak{D}_{\mathfrak{P}_{F'}}$ has type μ implies that

$$C_\sigma = B_i \mu_{\psi_i}(t) D_i,$$

where B_i and D_i are in $G(F'[\![t]\!])$ (see the discussion before Proposition 4.1.4 for the definition of $\mu_{\psi_i}(t)$). Finally, we compute that $(dC_\sigma/du)C_\sigma^{-1}$ equals

$$\frac{dB_i}{dt}B_i^{-1} + \mathrm{Ad}(B_i)\left(\frac{d\mu_{\psi_i}(t)}{dt}\mu_{\psi_i}(t)^{-1}\right) + \mathrm{Ad}(B_i)\left(\mathrm{Ad}(\mu_{\psi_i}(t))\left(\frac{dD_i}{dt}D_i^{-1}\right)\right).$$

We have $(dB_i/dt)B_i^{-1} \in (\mathrm{Lie}\, G \otimes F'[\![t]\!])$. Using a faithful representation on which T acts diagonally, we have $(d\mu_{\psi_i}(t)/dt)\mu_{\psi_i}(t)^{-1} \in (1/t)(\mathrm{Lie}\, G \otimes F'[\![t]\!])$. Finally, since μ_{ψ_i} is minuscule, $\mathrm{Ad}(\mu_{\psi_i}(t))(X) \in (1/t)(\mathrm{Lie}\, G \otimes F'[\![t]\!])$ for any $X \in \mathrm{Lie}\, G$ so in particular for $(dD_i/dt)D_i^{-1}$, by Proposition 4.1.4. □

Proof of Theorem 4.3.6. The faithfulness of $\widehat{\Delta}^\mu$ is clear. For fullness, let $\widehat{\mathfrak{P}}_A$ and $\widehat{\mathfrak{P}}'_A$ be in $D^{\mathrm{cris},\mu}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}(A)$ and let $\psi : \mathfrak{P}_A \cong \mathfrak{P}'_A$ be an isomorphism of underlying G-Kisin modules. To show ψ is equivariant for the $\widehat{\Gamma}$-actions, we can identify $\mathfrak{P}_A$ and $\mathfrak{P}'_A$ using ψ and choose a trivialization of $\mathfrak{P}_A$. Then it suffices to show that $(\mathfrak{P}_A, \phi_{\mathfrak{P}_A})$ has at most one crystalline $\widehat{\Gamma}$-structure. Let B_τ and B'_τ in $G(W(\widetilde{E}^+)_A)$ define the action of τ with respect to the chosen trivialization of $\varphi^*(\mathfrak{P}_A)$ for the two $\widehat{\Gamma}$-structures. By the crystalline property, $B_\tau(B'_\tau)^{-1} \in G(u^p)$. By Proposition 4.2.4, if Frobenius is given by C' with respect to the trivialization, then

$$B_\tau(B'_\tau)^{-1} = C'\varphi(B_\tau(B'_\tau)^{-1})(C')^{-1}.$$

But then, by Lemma 4.3.11, $B_\tau(B'_\tau)^{-1} = I$ since it is in $G(u^{p^i})$ for all $i \geq 1$.

We next attempt to construct a crystalline $\widehat{\Gamma}$-structure on any $\mathfrak{P}_A \in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$. Along the way, we will have to impose certain closed conditions on $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ to make our construction work. In the end, we will reduce to A flat over $\mathbb{Z}_p$ to show that these conditions are always satisfied. Fix a trivialization β_A of $\mathfrak{P}_A$. We want elements $\{B_\gamma\} \in G(\widehat{R}_A)$ for all $\gamma \in \widehat{\Gamma}$ satisfying the conditions of Proposition 4.3.10. Choose an element $\gamma \in \widehat{\Gamma}$. Let C denote the Frobenius with respect to β_A and let $C' = \varphi(C)$ be the Frobenius with respect to $1 \otimes_\varphi \beta_A$.

We use the topology on $G(W(\widetilde{\boldsymbol{E}})_A)$ induced from the topology on $W(\widetilde{\boldsymbol{E}})_A$ (see the discussion before Definition 4.2.2). Take $B_0 = I$. For all $i \geq 1$, define

$$B_i := C'\varphi(B_{i-1})\gamma(C')^{-1} \in G(W(\widetilde{\boldsymbol{E}})_A). \tag{4-3-12-1}$$

If $\mathfrak{P}_A$ admits a $\widehat{\Gamma}$-structure, then the B_i converge to B_γ in $G(\widehat{R}_A)$ or, equivalently, in $G(W(\widetilde{\boldsymbol{E}})_A)$.

Base case: $B_1 = C'\gamma(C')^{-1} \in G(u^p)$. Let V be a faithful n-dimensional representation of G such that $\mathfrak{P}_A(V)$ has height in $[a, b]$. Set $r = b - a$. Consider C as an element of $\mathrm{GL}_n\big(\mathfrak{S}_A[1/E(u)]\big)$ such that

$$C'' := E(u)^{-a} C \in \mathrm{Mat}_n(\mathfrak{S}_A) \quad \text{and} \quad D'' := E(u)^{b} C^{-1} \in \mathrm{Mat}_n(\mathfrak{S}_A)$$

with $C''D'' = E(u)^r I$. Working in $\mathrm{Mat}_n(W(\widetilde{\boldsymbol{E}})_A)$, we compute that

$$C'\gamma(C')^{-1} - I = \varphi\left(\frac{1}{E(u)^{-a}\gamma(E(u))^{b}}\big(C''\gamma(D'') - E(u)^{-a}\gamma(E(u))^{b} I\big)\right).$$

It would thus suffice to show $u\varphi(\mathfrak{t})E(u)^{r-1}$ divides $C''\gamma(D'') - E(u)^{-a}\gamma(E(u))^{b} I$ in $\mathrm{Mat}_n(W(\widetilde{\boldsymbol{E}}^+)_A)$, as then $u\,\mathfrak{t}$ divides

$$\frac{1}{E(u)^{-a}\gamma(E(u))^{b}}\big(C''\gamma(D'') - E(u)^{-a}\gamma(E(u))^{b} I\big)$$

using Lemma 4.3.1.

Consider $P(u_1, u_2) = C''(u_1)D''(u_2)$, where we replace u by u_1 in C'', which is in $\mathrm{Mat}_n(\mathfrak{S}_A)$, and u by u_2 in D''. Let $P_{ij}(u_1, u_2) = \sum_{k \geq 0} c^{ij}_k(u_1)u_2^k$ be the (i, j)-th entry, where $c^{ij}_k(u_1)$ is a power series in u_1 with coefficients in $W \otimes_{\mathbb{Z}_p} A$. We have that $P_{ij}(u, u) = \delta_{ij} E(u)^r$. The (i, j)-th entry of $C''\gamma(D'')$ is

$$P_{ij}(u, [\underline{\varepsilon}]u) = \sum_{k \geq 0} [\underline{\varepsilon}]^k c^{ij}_k(u)u^k,$$

where $\underline{\varepsilon} = (\zeta_{p^i})_{i \geq 0}$ is the sequence of p^n-th roots of unity such that $\gamma(\pi^{1/p^n}) = \zeta_{p^n}\pi^{1/p^n}$. Note that $\varphi(\mathfrak{t})$ divides $[\underline{\varepsilon}] - 1$ since $[\underline{\varepsilon}] - 1 \in I^{[1]}W(\widetilde{\boldsymbol{E}}^+)$ (see [Fontaine 1994, Proposition 5.1.3]) and $\varphi(\mathfrak{t})$ is a generator for this ideal. Then

$$P_{ij}(u, [\underline{\varepsilon}]u) = \sum_{k \geq 0} ([\underline{\varepsilon}]^k - 1)c^{ij}_k(u)u^k + \delta_{ij} E(u)^r.$$

Since $u([\underline{\varepsilon}]-1)E(u)^{r-1}$ divides $E(u)^r - E(u)^{-a}\gamma(E(u))^b$, it suffices to show that $u([\underline{\varepsilon}]-1)E(u)^{r-1}$ divides $\sum_k([\underline{\varepsilon}]^k-1)c_k^{ij}(u)u^k$. Using the Taylor expansion for x^k-1 at $x=1$, we have

$$[\underline{\varepsilon}]^k - 1 = \sum_{\ell=1}^{k}\binom{k}{\ell}([\underline{\varepsilon}]-1)^{\ell},$$

from which we deduce that

$$\sum_{k\geq 0}([\underline{\varepsilon}]^k-1)c_k^{ij}(u)u^k = u([\underline{\varepsilon}]-1)\bigg(\sum_{\ell\geq 1}([\underline{\varepsilon}]-1)^{\ell-1}u^{\ell-1}\sum_{k\geq 0}\binom{k+\ell}{\ell}c_{k+\ell}^{ij}(u)u^k\bigg)$$

Since $E(u)$ divides $[\underline{\varepsilon}]-1$, we are reducing to showing that

$$E(u)^{r-\ell}\ \bigg|\ u^{\ell-1}\sum_{k\geq 0}\binom{k+\ell}{\ell}c_{k+\ell}^{ij}(u)u^k$$

for $1\leq \ell\leq r-1$ where the expression on the right is exactly

$$\frac{u^{\ell-1}}{\ell!}\bigg(\frac{d^{\ell}P_{ij}(u_1,u_2)}{du_2^{\ell}}\bigg|_{(u,u)}\bigg).$$

Let $(\star_1)$ be the condition that $E(u)^{r-\ell}$ divides $d^{\ell}P_{ij}(u_1,u_2)/du_2^{\ell}|_{(u,u)}$ for all (i,j) and $1\leq \ell\leq r-1$. This is a closed condition on $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$.

Induction step: Let $\mathfrak{P}_A\in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$ satisfy $(\star_1)$ with trivialization as above, so that $B_1 = C'\gamma(C')^{-1}\in G(u^p)$. We have

$$B_{i+1}B_i^{-1} = C\varphi(B_iB_{i-1}^{-1})C^{-1}.$$

As $C=\varphi(C')$, we can apply Lemma 4.3.11 to conclude that $B_{i+1}B_i^{-1}\in G(u^{p^{i+1}})$, i.e., $B_{i+1}B_i^{-1}\equiv I \mod \varphi(\mathfrak{t})u^{p^{i+1}}W(\widetilde{\boldsymbol{E}}^+)_A$. Since $W(\widetilde{\boldsymbol{E}}^+)_A$ is separated and complete, $\varinjlim B_i = B_\gamma\in G(W(\widetilde{\boldsymbol{E}}^+)_A)$ and B_γ satisfies $B_\gamma\gamma(C)=C\varphi(B_\gamma)$. It is easy to see that $B_\gamma\gamma'(B_\gamma)=B_{\gamma\gamma'}$ for any γ and γ', by continuity, so we have a $\widehat{\Gamma}$-action. If $\gamma\in\widehat{\Gamma}_\infty$, then γ acts trivially on $\mathfrak{S}_A$ and so on C as well, so $B_\gamma = I$.

Let $(\star_2)$ denote the condition that $B_\gamma\in G(\widehat{R}_A)$ for all $\gamma\in\widehat{\Gamma}$. We claim this is also a closed condition on $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$. Since $W(\widetilde{\boldsymbol{E}}^+)/\widehat{R}$ is $\mathbb{Z}_p$-flat, the sequence

$$0\to \widehat{R}_A\to W(\widetilde{\boldsymbol{E}}^+)_A\to (W(\widetilde{\boldsymbol{E}}^+)/\widehat{R})\otimes_{\mathbb{Z}_p}A\to 0$$

is exact for any A. Any flat module over an Artinian ring is free, so the vanishing of an element $f\in (W(\widetilde{\boldsymbol{E}}^+)/\widehat{R})\otimes_{\mathbb{Z}_p}A$ is a closed condition on Spec A.

We have shown that any element $\mathfrak{P}_A\in D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(A)$ which satisfies $(\star_1)$ and $(\star_2)$ admits a crystalline $\widehat{\Gamma}$-structure and so lies in $D^{\mathrm{cris},\mu}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}(A)$. It suffices then to show that the closed subgroupoid defined by the conditions $(\star_1)$ and $(\star_2)$ is all of $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$. Recall that $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$ admits a formally smooth representable hull $D^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}} = \mathrm{Spf}\, R^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$, where $R^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ is flat and reduced by Theorem 3.2.4 and Proposition 3.3.10. Since $R^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ is flat and $R^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}[1/p]$ is reduced and Jacobson, any closed subscheme of $\operatorname{Spec} R^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}$ which contains $\operatorname{Hom}_{\Lambda}(R^{(N),\mu}_{\mathfrak{P}_{\mathbb{F}}}, F')$ for all F'/F finite is the whole space. It suffices then to show that, for any F'/F finite and Λ' the ring of integers of F', every object of $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}(\Lambda')$ satisfies $(\star_1)$ and $(\star_2)$.

First, for $(\star_1)$, choose $\gamma \in \widehat{\Gamma}$. Then set $Q_\ell(u) := \big(d^\ell P_{ij}(u_1,u_2)/du_2^\ell|_{(u,u)}\big)$, which is in $\operatorname{Mat}_n(\mathfrak{S}_{\Lambda'})$ (we ignore $u^{\ell-1}/\ell!$ since we are in the torsion-free setting). We can check that $E(u)^{r-\ell} \mid Q_\ell(u)$, working over $F' = \Lambda'[1/p]$ or any finite extension thereof. In particular, we can put ourselves in the situation of Lemma 4.3.12. We compute then that

$$\begin{aligned} Q_\ell(u) &= (E(u)^{-a}C)\frac{d^\ell}{du^\ell}(E(u)^b C^{-1}) \\ &= (E(u)^{-a}C)\sum_{m=0}^{\ell}\binom{\ell}{m}\frac{d^m E(u)^b}{du^m}\frac{d^{\ell-m}C^{-1}}{du^{\ell-m}} \\ &= \sum_{m=0}^{\ell}\binom{\ell}{m}\bigg(E(u)^{-a}\frac{d^m E(u)^b}{du^m}\bigg)\bigg(C\frac{d^{\ell-m}C^{-1}}{du^{\ell-m}}\bigg). \end{aligned}$$

Since $E(u)^{r-m}$ divides $E(u)^{-a}\, d^m E(u)^b/du^m$, it suffices to show that

$$Y_k := E(u)^k\bigg(C\frac{d^k C^{-1}}{du^k}\bigg) \in \operatorname{Mat}_n(\mathfrak{S}_{F'})$$

for all $k \geq 0$ (applied with $k = \ell - m$). The case $k = 0$ is trivial. By Lemma 4.3.12, $X_C := E(u)(dC/du)C^{-1} = -E(u)C\, d(C^{-1})/du$ is an element of $\operatorname{Lie} G \otimes \mathfrak{S}_{F'}$ considered as subset of $\operatorname{Lie}(\operatorname{GL}(V)) \otimes \mathfrak{S}_{F'}$ so, in particular, $Y_1 \in \operatorname{Mat}_n(\mathfrak{S}_{F'})$. The product rule applied to $(d/du)(E(u)^k C\, d^{k-1}C^{-1}/du)$ implies that

$$Y_k = \frac{d}{du}(E(u)Y_{k-1}) - k\frac{dE(u)}{du}Y_{k-1} + Y_1 Y_{k-1}$$

so, by induction on k, $Y_k \in \operatorname{Mat}_n(\mathfrak{S}_{F'})$ for all $k \geq 0$.

For $(\star_2)$, recall that $\widehat{R} = R_{K_0} \cap W(\widetilde{E}^+)$ (see p. 5 of [Liu 2010]) so it suffices to show that $B_\gamma \in G(R_{K_0} \otimes_{\mathbb{Z}_p} \Lambda')$ or, equivalently, $B_\gamma \in \operatorname{GL}_n(R_{K_0} \otimes_{\mathbb{Z}_p} \Lambda')$ with respect to V. Denote by $\mathfrak{M}_V$ the Kisin module $\mathfrak{P}_{\Lambda'}(V)$ of rank n. Since $\varphi(E(u))$ is invertible in S_{K_0}, C' lies in $\operatorname{GL}_n(S_{K_0} \otimes_{\mathbb{Z}_p} \Lambda')$ and defines a Frobenius on the Breuil module $\mathcal{M}_V := S_{K_0} \otimes_{\mathfrak{S},\varphi} \mathfrak{M}_V$. Using a similar argument to above, one can construct the monodromy operator $N_{\mathcal{M}_V}$ on $\mathcal{M}_V$ inductively, taking $N_0 = 0$ and setting

$$N_{i+1} := pC'\varphi(N_i)(C')^{-1} + u\frac{dC'}{du}(C')^{-1}. \tag{4-3-12-2}$$

The sequence $\{N_i\}$ converges to an element of $\mathrm{Mat}_n(u^p S_{K_0})$. For each N_i, let $\widetilde{N}_i$ be the induced derivation on $\mathcal{M}_V$ over $-u\,d/du$ which, on the chosen basis, is given by N_i. Equation (4-3-12-2) is equivalent to

$$\widetilde{N}_{i+1}\phi_{\mathcal{M}_V} = p\phi_{\mathcal{M}_V}\widetilde{N}_i. \tag{4-3-12-3}$$

Let $\underline{\varepsilon}(\gamma) := \gamma([\underline{\pi}])/[\underline{\pi}]$. Define a γ-semilinear map $\widetilde{B}_i$ on $R_{K_0} \otimes_{S_{K_0}} \mathcal{M}_V$ by

$$\widetilde{B}_i(x) = \sum_{j\geq 0} \frac{(-\log \underline{\varepsilon}(\gamma))^j}{j!} \otimes (\widetilde{N}_i)^j(x)$$

for all $x \in \mathcal{M}_V$. Equation (4-3-12-3) implies that

$$\widetilde{B}_{i+1}\phi_{\mathcal{M}_V} = \phi_{\mathcal{M}_V}\widetilde{B}_i.$$

By induction on i, one deduces that $\widetilde{B}_i$ is exactly the γ-semilinear morphism induced by the matrix B_i defined in (4-3-12-1).

If $N_{\mathcal{M}_V}$ is the limit of the $\widetilde{N}_i$ and $\widetilde{B}_\gamma$ is the γ-semilinear morphism induced by B_γ, then we have the formula

$$\widetilde{B}_\gamma(x) := \sum_{j\geq 0} \frac{(-\log \underline{\varepsilon}(\gamma))^j}{j!} \otimes N_{\mathcal{M}}^j(x)$$

for all $x \in \mathcal{M}_V$. Working with respect to the chosen basis for $\mathcal{M}_V$, we deduce that $B_\gamma \in \mathrm{GL}_n(R_{K_0} \otimes_{\mathbb{Z}_p} \Lambda')$, as desired. ☐

4.4. ***Applications to G-valued deformation rings.*** Let $\bar{\eta} : \Gamma_K \to G(\mathbb{F})$ be a continuous representation. As before, μ is a minuscule geometric cocharacter of $\mathrm{Res}_{(K\otimes_{\mathbb{Q}_p} F)/F}\, G_F$. Let $R_{\bar{\eta}}^{\mathrm{cris},\mu}$ be the universal G-valued framed crystalline deformation ring with p-adic Hodge type μ over $\Lambda_{[\mu]}$. Let $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ be the projective $R_{\bar{\eta}}^{\mathrm{cris},\mu}$-scheme as in Corollary 3.3.15. The following theorem on the geometry of $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ has a number of important corollaries. The proof uses the main results from Sections 3.2 and 4.2. We can say more about the connected components when K is unramified over $\mathbb{Q}_p$ (see Theorem 4.4.6).

Theorem 4.4.1. *Assume $p \nmid \pi_1(G^{\mathrm{der}})$. Let μ be a minuscule geometric cocharacter of* $\mathrm{Res}_{(K\otimes_{\mathbb{Q}_p} F)/F}\, G_F$. *Then $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ is normal and $X_{\bar{\eta}}^{\mathrm{cris},\mu} \otimes_{\Lambda_{[\mu]}} \mathbb{F}_{[\mu]}$ is reduced.*

Corollary 4.4.2. *Assume $p \nmid \pi_1(G^{\mathrm{der}})$. Let $X_{\bar{\eta},0}^{\mathrm{cris},\mu}$ denote the fiber of $X_{\bar{\eta}}^{\mathrm{cris},\mu}$ over the closed point of* $\mathrm{Spec}\, R_{\bar{\eta}}^{\mathrm{cris},\mu}$. *The connected components of* $\mathrm{Spec}\, R_{\bar{\eta}}^{\mathrm{cris},\mu}[1/p]$ *are in bijection with the connected components of $X_{\bar{\eta},0}^{\mathrm{cris},\mu}$.*

Proof. By Theorem 2.3.12, $\mathrm{Spec}\, R_{\bar{\eta}}^{\mathrm{cris},\mu}[1/p] = X_{\bar{\eta}}^{\mathrm{cris},\mu}[1/p]$. Since $X_{\bar{\eta}}^{\mathrm{cris},\mu} \otimes_\Lambda \mathbb{F}$ is reduced by Theorem 4.4.1, the bijection between $\pi_0(X_{\bar{\eta}}^{\mathrm{cris},\mu}[1/p])$ and $\pi_0(X_{\bar{\eta},0}^{\mathrm{cris},\mu})$ follows from the "reduced fiber trick" [Kisin 2009, Corollary (2.4.10)]. ☐

Remark 4.4.3. Theorem 4.4.1 and Corollary 4.4.2 hold for unframed G-valued crystalline deformation functors when they are representable, by exactly the same arguments.

Before we begin the proof, we introduce a few auxiliary deformation groupoids. The relationship between the various deformation spaces is described in (4-4-5-1). Let $D^{\square}_{\bar{\eta}}$ be the deformation functor of $\bar{\eta}$, so $D^{\square}_{\bar{\eta}}(A)$ is the set of homomorphisms $\eta : \Gamma_K \to G(A)$ lifting $\bar{\eta}$. Let $\mathfrak{P}_{\mathbb{F}}$ be the G-Kisin module associated to a $\mathbb{F}$-point $\bar{x}$ of $X^{\mathrm{cris},\mu}_{\bar{\eta}}$.

Definition 4.4.4. Define $D^{[a,b]}_{\bar{x}}(A)$ to be the category of triples

$$\{(\eta_A, \mathfrak{P}_A, \delta_A) \mid \eta_A \in D^{\square}_{\bar{\eta}}(A),\ \mathfrak{P}_A \in D^{[a,b]}_{\mathfrak{P}_{\mathbb{F}}}(A),\ \delta_A : T_{G,\mathfrak{S}_A}(\mathfrak{P}_A) \cong \eta_A|_{\Gamma_\infty}\}.$$

Let $\widehat{\mathfrak{P}}_{\mathbb{F}}$ denote a crystalline $\widehat{\Gamma}$-structure on $\mathfrak{P}_{\mathbb{F}}$ together with an isomorphism $\widehat{T}_{G,\mathbb{F}}(\widehat{\mathfrak{P}}_{\mathbb{F}}) \cong \bar{\eta}$. Define $D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}(A)$ to be the category of triples

$$\{(\eta_A, \widehat{\mathfrak{P}}_A, \delta_A) \mid \eta_A \in D^{\square}_{\bar{\eta}}(A),\ \widehat{\mathfrak{P}}_A \in D^{\mathrm{cris},\mu}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}(A),\ \delta_A : \widehat{T}_{G,A}(\widehat{\mathfrak{P}}_A) \cong \eta_A\}.$$

Proposition 4.4.5. *For any $\widehat{\mathfrak{P}}_{\mathbb{F}}$, the forgetful functor from $D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}$ to $D^{[a,b]}_{\bar{x}}$ is fully faithful.*

Proof. One reduces immediately to the case of GL_n and then we have the following more general fact: Choose any $\widehat{\mathfrak{M}}'_A, \widehat{\mathfrak{M}}_A \in \mathrm{Mod}^{\varphi,\mathrm{bh},\widehat{\Gamma}}_{\mathfrak{S}_A}$. Let $f : \mathfrak{M}'_A \to \mathfrak{M}_A$ be a map of underlying Kisin modules such that $T_{\mathfrak{S}_A}(f)$ is Γ_K-equivariant (under the identification $\widehat{T}_{\mathfrak{S}_A} \cong T_{\mathfrak{S}_A}$). Then f is a map of $(\varphi, \widehat{\Gamma})$-modules. This is proven in [Ozeki 2013, Corollary 4.3] when height is in $[0, h]$, but can be easily extended to bounded height. The key input is a weak form of Liu's comparison isomorphism [2007, Proposition 3.2.1], which is also in [Levin 2013, Proposition 9.2.1]. $\square$

The diagram below illustrates some of the relationships between the different deformation problems. The diagonal maps on the left and the map labeled sm are formally smooth. Maps labeled with $c \sim$ indicate that the complete stalk at a point of the target represents that deformation functor. The horizontal equivalences are consequences of Theorem 4.3.6 and the proof of Theorem 4.4.1, respectively.

$$\begin{array}{ccccccccc} & \widetilde{D}^{(\infty),\mu}_{\mathfrak{P}_{\mathbb{F}}} & & & D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}} & \xrightarrow{\sim} & D^{\mathrm{cris},\mu}_{\bar{x}} & \xrightarrow{c\sim} & X^{\mathrm{cris},\mu}_{\bar{\eta}} \\ {\scriptstyle \pi^\mu}\swarrow & & \searrow{\scriptstyle \Psi^\mu} & & \downarrow{\scriptstyle \mathrm{sm}} & \searrow & \downarrow & & \downarrow \\ \overline{D}^{\mu}_{Q_{\mathbb{F}}} & & D^{\mu}_{\mathfrak{P}_{\mathbb{F}}} & \xleftarrow{\sim} & D^{\mathrm{cris},\mu}_{\widehat{\mathfrak{P}}_{\mathbb{F}}} & & D^{[a,b]}_{\bar{x}} & \xrightarrow{c\sim} & X^{[a,b]}_{\bar{\eta}} \end{array} \qquad (4\text{-}4\text{-}5\text{-}1)$$

Proof of Theorem 4.4.1. Let $\bar{x}$ be a point of the special fiber of $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ defined over a finite field $\mathbb{F}'$. Since $X^{\mathrm{cris},\mu}_{\bar{\eta}}[1/p] = \mathrm{Spec}\, R^{\mathrm{cris},\mu}_{\bar{\eta}}[1/p]$ is formally smooth over F [Balaji 2012, Proposition 4.1.5], it suffices to show that the completed stalk $\widehat{\mathcal{O}}^{\mu}_{\bar{x}}$

at $\bar{x}$ is normal and that $\widehat{\mathbb{O}}^{\mu}_{\bar{x}} \otimes_{\Lambda_{[\mu]}} \mathbb{F}_{[\mu]}$ is reduced. To accomplish this, we compare $\widehat{\mathbb{O}}^{\mu}_{\bar{x}}$ with $\overline{D}^{\mu}_{Q_{\mathbb{F}'}}$ from Section 3.3 and then use as input the corresponding results for the local model $M(\mu)$.

These properties can be checked after an étale extension of $\Lambda_{[\mu]}$. $R^{\mathrm{cris},\mu}_{\bar{\eta}}$ commutes with changing coefficients using the abstract criterion in [Chai et al. 2014, Proposition 1.4.3.6] as does the formation of $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ by Proposition 2.3.5. We can assume then, without loss of generality, that $\Lambda = \Lambda_{[\mu]}$ and $\mathbb{F}' = \mathbb{F}$. Let $\mathfrak{P}_{\mathbb{F}}$ be the G-Kisin module defined by $\bar{x}$. Since μ is minuscule, $X^{\mathrm{cris},\mu}_{\bar{\eta}} = X^{\mathrm{cris},\leq\mu}_{\bar{\eta}}$ (see Proposition 4.1.3).

Since $\widehat{\mathbb{O}}^{\mu}_{\bar{x}}$ is nonempty and Λ-flat (assuming that $R^{\mathrm{cris},\mu}_{\bar{\eta}}$ is nonempty), it has an F'-point for some finite extension F'/F. Any such point gives rise to a crystalline lift ρ of $\bar{x}$ to $\mathbb{O}_{F'}$ such that the unique Kisin lattice in $\underline{M}_{G,\mathbb{O}_{F'}}(\rho)$ reduces to $\mathfrak{P}_{\mathbb{F}} \otimes_{\mathbb{F}} \mathbb{F}'$. Replace $\mathbb{F}'$ by $\mathbb{F}$. Then, by Proposition 4.3.5, the corresponding $G(\mathbb{O}_{F'})$-valued representation is isomorphic to $\widehat{T}_{G,\mathbb{O}_{F'}}(\widehat{\mathfrak{P}}_{\mathbb{O}_{F'}})$ for some crystalline $(\varphi, \widehat{\Gamma})$-module with G-structure. Reducing modulo the maximal ideal, we obtain a crystalline $\widehat{\Gamma}$-structure $\widehat{\mathfrak{P}}_{\mathbb{F}}$ on $\mathfrak{P}_{\mathbb{F}}$. By Proposition 4.4.5, this is the unique such structure.

Recall the deformation problem $D^{\mathrm{cris},\mu}_{\bar{x}}$ from Corollary 3.3.15 and $D^{[a,b]}_{\bar{x}}$ from Definition 4.4.4. The natural map

$$D^{\mathrm{cris},\mu}_{\bar{x}} \to D^{[a,b]}_{\bar{x}}$$

is a closed immersion (by Theorem 2.3.12). By Corollary 3.3.15, $\mathrm{Spf}\, \mathbb{O}^{\mu}_{\bar{x}}$ is closed in $D^{\mathrm{cris},\mu}_{\bar{x}}$.

Fix the isomorphism $\beta_{\mathbb{F}} : \widehat{T}_{G,\mathbb{F}}(\widehat{\mathfrak{P}}_{\mathbb{F}}) \cong \bar{\eta}$. Consider the groupoid $D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}$ in Definition 4.4.4. There is a natural morphism from $D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}$ to $D^{[a,b]}_{\bar{x}}$, given by forgetting the $\widehat{\Gamma}$-structure. By Proposition 4.4.5, this morphism is fully faithful, hence a closed immersion by considering tangent spaces.

We claim that

$$D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}} = \mathrm{Spf}\, \mathbb{O}^{\mu}_{\bar{x}}$$

as closed subfunctors of $D^{[a,b]}_{\bar{x}}$. Since they are both representable, we look at their F'-points for any finite extension F' of F. By Theorem 4.2.7 and Corollary 3.3.15,

$$D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}(F') = D^{\mathrm{cris},\mu}_{\bar{x}}(F') = \mathrm{Spf}\, \mathbb{O}^{\mu}_{\bar{x}}(F').$$

Since $\mathbb{O}^{\mu}_{\bar{x}}$ is Λ-flat and $\mathbb{O}^{\mu}_{\bar{x}}[1/p]$ is formally smooth over F, we deduce that

$$\mathrm{Spf}\, \mathbb{O}^{\mu}_{\bar{x}} \subset D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}.$$

Finally, $D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}$ is formally smooth over $D^{\mu}_{\mathfrak{P}_{\mathbb{F}}}$, by Theorem 4.3.6. By (3-3-9-2), there is a diagram

$$\begin{array}{ccc} & \operatorname{Spf} S^{\mu} & \\ \swarrow & & \searrow \\ D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}} & & \overline{D}^{\mu}_{Q_{\mathbb{F}}}, \end{array}$$

where $S^{\mu} \in \widehat{\mathscr{C}}_{\Lambda}$ and both morphisms are formally smooth ($Q_{\mathbb{F}}$ is as in Section 3.2). The functor $\overline{D}^{\mu}_{Q_{\mathbb{F}}}$ is represented by a completed stalk $R^{\mu}_{Q_{\mathbb{F}}}$ on $M(\mu)$. In particular, $R^{\mu}_{Q_{\mathbb{F}}}$ is Λ-flat so the same is true of $D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}}$. Thus,

$$D^{\mathrm{cris},\mu,\square}_{\widehat{\mathfrak{P}}_{\mathbb{F}}} = \operatorname{Spf} \mathbb{O}^{\mu}_{\bar{x}}.$$

By Theorem 3.2.4, $R^{\mu}_{Q_{\mathbb{F}}}$ is normal and Cohen–Macaulay, and $R^{\mu}_{Q_{\mathbb{F}}} \otimes_{\Lambda} \mathbb{F}$ is reduced, so the same holds true for $\widehat{\mathbb{O}}^{\mu}_{x}$.

□

Theorem 4.4.6. *Assume $K/\mathbb{Q}_p$ is unramified, $p > 3$, and $p \nmid \pi_1(G^{\mathrm{ad}})$. Then the universal crystalline deformation ring $R^{\mathrm{cris},\mu}_{\bar{\eta}}$ is formally smooth over $\Lambda_{[\mu]}$.*

Proof. First, replace Λ by $\Lambda_{[\mu]}$. Without loss of generality, we can assume that F contains all embeddings of K, since this can be arranged by a finite étale base change. When $K/\mathbb{Q}_p$ is unramified, $\mathrm{Gr}^{E(u),W}_{G}$ is a product of $[K : \mathbb{Q}_p]$ copies of the affine Grassmannian Gr_G (see [Levin 2013, Proposition 10.1.11]). If $\mu = (\mu_{\psi})_{\psi : K \to F}$ then $M(\mu)_F = \prod_{\psi} S(\mu_{\psi})$, where $S(\mu_{\psi})$ are affine Schubert varieties of Gr_{G_F}. Under the assumption that $p \nmid \pi_1(G^{\mathrm{der}})$, there is a flat closed Λ-subscheme of Gr_G which, abusing notation, we denote by $S(\mu_{\psi})$, whose fibers are the affine Schubert varieties for μ_{ψ} (see Theorem 8.4 in [Pappas and Rapoport 2008], especially the discussions in §§8.e.3–8.e.4). Thus,

$$M(\mu) = \prod_{\psi : K \to F} S(\mu_{\psi}).$$

Since μ_{ψ} is minuscule, $S(\mu_{\psi})$ is isomorphic to a flag variety for G, hence $M(\mu)$ is smooth (see Proposition 4.1.3). The proof of Theorem 4.4.1 shows that the local structure of $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ is smoothly equivalent to the local structure of $M(\mu)$. Thus, $X^{\mathrm{cris},\mu}_{\bar{\eta}}$ is formally smooth over Λ.

Finally, we have to show that

$$\Theta : X^{\mathrm{cris},\mu}_{\bar{\eta}} \to \operatorname{Spec} R^{\mathrm{cris},\mu}_{\bar{\eta}}$$

is an isomorphism. Since $\Theta[1/p]$ is an isomorphism and $R^{\mathrm{cris},\mu}_{\bar{\eta}}$ is Λ-flat, it suffices to show that Θ is a closed immersion. Let m_R be the maximal ideal of $R^{\mathrm{cris},\mu}_{\bar{\eta}}$.

Consider the reductions

$$\Theta_n : X^{\mathrm{cris},\mu}_{\bar{\eta},n} \to \operatorname{Spec} R^{\mathrm{cris},\mu}_{\bar{\eta}}/m^n_R.$$

We appeal to an analogue of Raynaud's uniqueness result [1974, Theorem 3.3.3] for finite flat models. For any Artin local $\mathbb{Z}_p$-algebra A and any finite A-algebra B, let $\mathfrak{P}_B$ and $\mathfrak{P}'_B$ be two distinct points in the fiber of Θ_n over $x : R^{\mathrm{cris},\mu}_{\bar{\eta}} \to A$, i.e., G-Kisin lattices in $P_x \otimes_A B$. Let V^{ad} denote the adjoint representation of G. Under the assumption that $p > 3$, [Liu 2007, Theorem 2.4.2] (which generalizes Raynaud's result) implies that $\mathfrak{P}_A(V^{\mathrm{ad}}) = \mathfrak{P}'_A(V^{\mathrm{ad}})$ as Kisin lattices in $(P_x \otimes_A B)(V^{\mathrm{ad}})$, using that μ is minuscule.

Since B is Artinian, without loss of generality we can assume it is local ring. Choose a trivialization of $\mathfrak{P}_B$. There exists $g \in G(\mathcal{O}_{\mathscr{E},B})$ such that $\mathfrak{P}'_B = g \cdot \mathfrak{P}_B$ (working inside the affine Grassmannian as in Theorem 2.3.2). The results above implies that $\mathrm{Ad}(g) \in G^{\mathrm{ad}}(\mathfrak{S}_A)$. By assumption, $Z := \ker(G \to G^{\mathrm{ad}})$ is étale so, after possibly extending the residue field $\mathbb{F}$, we can lift $\mathrm{Ad}(g)$ to an element $\tilde{g} \in G(\mathfrak{S}_A)$ such that $g = \tilde{g}z$, where $z \in Z(\mathcal{O}_{\mathscr{E},A})$. We want to show that $z \in Z(\mathfrak{S}_A)$. We can write Z as a product $Z_{\mathrm{tors}} \times (\mathbb{G}_{\mathrm{m}})^s$ for some $s \geq 0$. Since Z_{tors} has order prime to p by assumption, $Z_{\mathrm{tors}}(\mathcal{O}_{\mathscr{E},A}) = Z_{\mathrm{tors}}(\mathfrak{S}_A)$, so we can assume

$$z \in (\mathbb{G}_{\mathrm{m}}(\mathcal{O}_{\mathscr{E},A}))^s = \big((A \otimes_{\mathbb{Z}_p} W)((u))^{\times}\big)^s.$$

For any embedding $\psi : W \to \mathcal{O}_F$, we associate to z the s-tuple λ_ψ of integers of the degrees of the leading terms of each component base changed by ψ. To show that $\lambda_\psi = 0$, we can work over $A/m_A = \mathbb{F}$. We think of λ_ψ as a cocharacter of Z. Consider the quotient of G by its derived group $Z' := G/G^{\mathrm{der}}$. The map $X_*(Z) \to X_*(Z')$ is injective. Any character χ of Z' defines a one-dimensional representation L_χ of G so, in particular, we can consider $\mathfrak{P}_B(L_\chi)$ and $\mathfrak{P}'_B(L_\chi)$ as Kisin lattices in $P_x(L_\chi)$. Writing $\mathfrak{S}_{\mathbb{F}} \cong \bigoplus_{\psi : W \to \mathcal{O}_F} \mathbb{F}[\![u_\psi]\!]$, a Kisin lattice of $P_x(L_\chi)$ has type (h_ψ) exactly when $\phi_{P_x}(e) = (a_\psi u^{h_\psi})e$ for a basis element e and $a_\psi \in \mathbb{F}$. Since both $\mathfrak{P}_B$ and $\mathfrak{P}'_B$ have type μ, $\mathfrak{P}_B(L_\chi)$ and $\mathfrak{P}'_B(L_\chi)$ both have type $h_\psi := \langle \chi, \mu_\psi \rangle$. However, a direct computation shows that $\mathfrak{P}'_B(L_\chi)$ has type $h_\psi + \langle \chi, p\lambda_{\psi'} - \lambda_\psi \rangle$, where $\psi' = \varphi \circ \psi$. Thus, $\lambda_\psi = p\lambda_{\psi'}$. We deduce that $p^{[K:\mathbb{Q}_p]}\lambda_\psi = \lambda_\psi$ and so $\lambda_\psi = 0$.

We are reduced to the following general situation: $X \to \operatorname{Spec} A$ is proper morphism which is injective on B-points for all A-finite algebras B, where A is a local Artinian ring. By consideration of the one geometric fiber, $X \to \operatorname{Spec} A$ is quasifinite, hence finite. Thus, $X = \operatorname{Spec} A'$. By Nakayama, it suffices to show $A/m_A \to A'/(m_A)A'$ is surjective so we can assume $A = k$ is a field. Surjectivity follows from considering the two morphisms $A' \rightrightarrows A' \otimes_k A'$, which agree by injectivity of $X \to \operatorname{Spec} A$ on A-finite points. □

Acknowledgments

The enormous influence of the work of Mark Kisin and Tong Liu in this paper will be evident to the reader. This paper is based on the author's Stanford Ph.D. thesis advised by Brian Conrad, to whom the author owes a debt of gratitude for his generous guidance and his feedback on multiple drafts of the thesis. It is a pleasure to thank Tong Liu, Xinwen Zhu, George Pappas, Bhargav Bhatt, and Mark Kisin for many helpful discussions and exchanges related to this project. The author is additionally grateful for the support of the National Science Foundation and the Department of Defense in the form of NSF and NDSEG fellowships. Part of this work was completed while the author was a visitor at the Institute for Advanced Study, supported by the National Science Foundation grant DMS-1128155. The author is grateful to the IAS for its support and hospitality. Finally, we would like to thank the referee for a number of valuable suggestions.

References

[Balaji 2012] S. Balaji, *G-valued potentially semi-stable deformation rings*, Ph.D. thesis, The University of Chicago, Ann Arbor, MI, 2012, http://search.proquest.com/docview/1346024943. MR 3152673

[Bellovin 2014] R. Bellovin, "Generic smoothness for G-valued potentially semistable deformation rings", preprint, 2014. arXiv 1403.1411

[Bourbaki 2002] N. Bourbaki, *Lie groups and Lie algebras, Chapters 4–6*, Springer, Berlin, 2002. MR 2003a:17001 Zbl 0983.17001

[Brinon and Conrad 2009] O. Brinon and B. Conrad, "CMI summer school notes on p-adic Hodge theory notes", lecture notes, 2009, http://math.stanford.edu/∼conrad/.

[Broshi 2008] M. A. Broshi, *Moduli of finite flat group schemes with G-structure*, Ph.D. thesis, http://search.proquest.com/docview/304407562, Ann Arbor, MI, 2008, http://search.proquest.com/docview/304407562. MR 2717544

[Broshi 2013] M. Broshi, "G-torsors over a Dedekind scheme", *J. Pure Appl. Algebra* **217**:1 (2013), 11–19. MR 2965898 Zbl 1271.14062

[Caruso and Liu 2011] X. Caruso and T. Liu, "Some bounds for ramification of p^n-torsion semi-stable representations", *J. Algebra* **325** (2011), 70–96. MR 2012b:11090 Zbl 1269.14001

[Chai et al. 2014] C.-L. Chai, B. Conrad, and F. Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs **195**, American Mathematical Society, Providence, RI, 2014. MR 3137398 Zbl 1298.14001

[Deligne 1979] P. Deligne, "Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques", pp. 247–289 in *Automorphic forms, representations and L-functions, II* (Corvallis, OR, 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, R.I., 1979. MR 81i:10032 Zbl 0437.14012

[Deligne and Milne 1982] P. Deligne and J. S. Milne, "Tannakian categories", pp. 101–228 in *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics **900**, Springer, New York, 1982. MR 84m:14046 Zbl 0477.14004

[EGA III_1 1961] A. Grothendieck, "Eléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, I", *Inst. Hautes Études Sci. Publ. Math.* **11** (1961), 5–167. MR 0163910 Zbl 0118.36206

[Fontaine 1994] J.-M. Fontaine, *Le corps des périodes p-adiques*, Astérisque **223**, 1994. MR 95k:11086 Zbl 0940.14012

[Gaitsgory 2001] D. Gaitsgory, "Construction of central elements in the affine Hecke algebra via nearby cycles", *Invent. Math.* **144**:2 (2001), 253–280. MR 2002d:14072 Zbl 1072.14055

[Gee 2006] T. Gee, "A modularity lifting theorem for weight two Hilbert modular forms", *Math. Res. Lett.* **13**:5–6 (2006), 805–811. MR 2007m:11065 Zbl 1185.11030

[Gee et al. 2014] T. Gee, T. Liu, and D. Savitt, "The Buzzard–Diamond–Jarvis conjecture for unitary groups", *J. Amer. Math. Soc.* **27**:2 (2014), 389–435. MR 3164985 Zbl 1288.11045

[Gross 2000] B. H. Gross, "On minuscule representations and the principal SL_2", *Represent. Theory* **4** (2000), 225–244. MR 2001j:20066 Zbl 0986.22011

[Hellmann 2011] E. Hellmann, "Connectedness of Kisin varieties for GL_2", *Adv. Math.* **228** (2011), 219–240. MR 2822232 Zbl 1268.11074

[Imai 2010] N. Imai, "On the connected components of moduli spaces of finite flat models", *Amer. J. Math.* **132**:5 (2010), 1189–1204. MR 2012a:11064 Zbl 1205.14025

[Imai 2012] N. Imai, "On the connected components of moduli spaces of Kisin modules", *J. Algebra* **349** (2012), 1–7. MR 2012k:11072 Zbl 1242.14043

[Kim 2009] W. Kim, *Galois deformation theory for norm fields and its arithmetic applications*, Ph.D. thesis, University of Michigan, 2009, http://search.proquest.com/docview/304931137. MR 2713872

[Kisin 2006] M. Kisin, "Crystalline representations and F-crystals", pp. 459–496 in *Algebraic geometry and number theory*, edited by V. Ginzburg, Progr. Math. **253**, Birkhäuser, Boston, 2006. MR 2007j:11163 Zbl 1184.11052

[Kisin 2008] M. Kisin, "Potentially semi-stable deformation rings", *J. Amer. Math. Soc.* **21**:2 (2008), 513–546. MR 2009c:11194 Zbl 1205.11060

[Kisin 2009] M. Kisin, "Moduli of finite flat group schemes, and modularity", *Ann. of Math.* (2) **170**:3 (2009), 1085–1180. MR 2011g:11107 Zbl 1201.14034

[Levin 2013] B. Levin, *G-valued flat deformations and local models*, Ph.D. thesis, Stanford University, 2013, http://www.math.ias.edu/~bwlevin/LevinThesis.pdf.

[Levin 2014] B. Levin, "Local models for Weil-restricted groups", preprint, 2014. arXiv 1412.7135

[Liu 2007] T. Liu, "Torsion p-adic Galois representations and a conjecture of Fontaine", *Ann. Sci. École Norm. Sup.* (4) **40**:4 (2007), 633–674. MR 2010h:11191 Zbl 1163.11043

[Liu 2010] T. Liu, "A note on lattices in semi-stable representations", *Math. Ann.* **346**:1 (2010), 117–138. MR 2011d:11272 Zbl 1208.14017

[Liu 2012] T. Liu, "Lattices in filtered (ϕ, N)-modules", *J. Inst. Math. Jussieu* **11**:3 (2012), 659–693. MR 2931320 Zbl 1249.14006

[Liu 2013] T. Liu, "The correspondence between Barsotti–Tate groups and Kisin modules when $p = 2$", *J. Théor. Nombres Bordeaux* **25**:3 (2013), 661–676. MR 3179680 Zbl 06291371

[Ozeki 2013] Y. Ozeki, "Torsion representations arising from $(\varphi, \hat{G})$-modules", *J. Number Theory* **133**:11 (2013), 3810–3861. MR 3084302 Zbl 1297.11146

[Pappas and Rapoport 2008] G. Pappas and M. Rapoport, "Twisted loop groups and their affine flag varieties", *Adv. Math.* **219** (2008), 118–198. MR 2009g:22039 Zbl 1159.22010

[Pappas and Rapoport 2009] G. Pappas and M. Rapoport, "Φ-modules and coefficient spaces", *Mosc. Math. J.* **9**:3 (2009), 625–663, back matter. MR 2011c:14074 Zbl 1194.14032

[Pappas and Zhu 2013] G. Pappas and X. Zhu, "Local models of Shimura varieties and a conjecture of Kottwitz", *Invent. Math.* **194**:1 (2013), 147–254. MR 3103258 Zbl 1294.14012

[Pappas et al. 2013] G. Pappas, M. Rapoport, and B. Smithling, "Local models of Shimura varieties, I: Geometry and combinatorics", pp. 135–217 in *Handbook of moduli, III*, edited by G. Farkas and I. Morrison, Adv. Lect. Math. **26**, International Press, 2013. MR 3135437

[Rapoport and Zink 1996] M. Rapoport and T. Zink, *Period spaces for p-divisible groups*, Annals of Mathematics Studies **141**, Princeton University Press, NJ, 1996. MR 97f:14023 Zbl 0873.14039

[Raynaud 1974] M. Raynaud, "Schémas en groupes de type $(p, \dots, p)$", *Bull. Soc. Math. France* **102** (1974), 241–280. MR 54 #7488 Zbl 0325.14020

[Richarz 2013] T. Richarz, "Schubert varieties in twisted affine flag varieties and local models", *J. Algebra* **375** (2013), 121–147. MR 2998951 Zbl 1315.14066

[Richarz 2015] T. Richarz, "Affine grassmanians and geometric Satake equivalences", preprint, 2015. arXiv 1311.1008

[Saavedra Rivano 1972] N. Saavedra Rivano, *Catégories Tannakiennes*, Lecture Notes in Mathematics **265**, Springer, New York, 1972. MR 49 #2769 Zbl 0241.14008

[Serre 1958] J.-P. Serre, "Espaces fibres algébriques", *Séminaire Claude Chevalley* **3** (1958), Exposé No. 1, 1–37. Zbl 03159916

[SGA 7_{I} 1972] D. S. Rim, "Formal deformation theory", pp. 32–132 in *Groupes de monodromie en géométrie algébrique, I: Exposés I–II, VI–IX* (Séminaire de Géométrie Algébrique du Bois Marie 1967–1969), Lecture Notes in Math. **288**, Springer, Berlin, 1972. MR 50 #7134 Zbl 0237.00013

[Springer 1998] T. A. Springer, *Linear algebraic groups*, 2nd ed., Progr. Math. **9**, Birkhäuser, Boston, 1998. MR 99h:20075 Zbl 0927.20024

[Taylor and Wiles 1995] R. Taylor and A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math.* (2) **141**:3 (1995), 553–572. MR 96d:11072 Zbl 0823.11030

Communicated by Mark Kisin
Received 2014-04-04 Revised 2015-06-01 Accepted 2015-07-15

bwlevin@math.uchicago.edu *Department of Mathematics, University of Chicago, 5734 S. University Avenue, Room 208C, Chicago, 60637, United States*

ALGEBRA AND NUMBER THEORY 9:8 (2015)
dx.doi.org/10.2140/ant.2015.9.1793

Indicators of Tambara–Yamagami categories and Gauss sums

Tathagata Basak and Ryan Johnson

We prove that the higher Frobenius–Schur indicators, introduced by Ng and Schauenburg, give a strong-enough invariant to distinguish between any two Tambara–Yamagami fusion categories. Our proofs are based on computation of the higher indicators in terms of Gauss sums for certain quadratic forms on finite abelian groups and rely on the classification of quadratic forms on finite abelian groups, due to Wall.

As a corollary to our work, we show that the state-sum invariants of a Tambara–Yamagami category determine the category as long as we restrict to Tambara–Yamagami categories coming from groups G whose order is not a power of 2. Turaev and Vainerman proved this result under the assumption that G has odd order, and they conjectured that a similar result should hold for groups of even order. We also give an example to show that the assumption that $|G|$ is not a power of 2 cannot be completely relaxed.

1. Introduction

Fusion categories (see [Etingof et al. 2005]) occur in various branches of mathematics: low-dimensional topology, subfactors, and quantum groups, to name a few. Classification of fusion categories, although currently out of reach in general, is a main driving question in the area. A natural method for classifying objects in mathematics is via numerical invariants. Ng and Schauenburg [2007b] introduced a class of invariants of spherical pivotal fusion categories (to be simply called spherical categories) called the higher Frobenius–Schur indicators. Let $\mathcal{C}$ denote a spherical category. For each simple object V of $\mathcal{C}$ and each integer $k \geq 1$, Ng and Schauenburg define a complex number $\nu_k(V)$, called the k-th indicator of V. These build on and generalize many previous works, e.g., [Bantay 1997; Fuchs et al. 1999; Fuchs and Schweigert 2003; Kashina et al. 2006; Linchenko and Montgomery 2000; Mason and Ng 2005]; we refer the reader to the introduction of [Ng and Schauenburg 2007b] for more details. For $k = 2$, these invariants

MSC2010: primary 18D10; secondary 15A63, 11L05, 57M27.
Keywords: fusion category, Tambara–Yamagami category, Frobenius–Schur indicator, discriminant form, quadratic form, Gauss sum.

generalize the classical Frobenius–Schur indicator of a finite group representation. The Frobenius–Schur indicators of the simple objects of $\mathcal{C}$ can be used to define the Frobenius–Schur exponent of $\mathcal{C}$, denoted $\mathrm{FSexp}(\mathcal{C})$. When $\mathcal{C}$ is the representation category of a quasi-Hopf algebra, $\mathrm{FSexp}(\mathcal{C})$ is equal to $\exp(\mathcal{C})$ or $2\exp(\mathcal{C})$ [Ng and Schauenburg 2007a, Theorem 6.2] where $\exp(\mathcal{C})$ denotes the exponent of $\mathcal{C}$ in the sense of Etingof et al. (see [Etingof 2002] and its references).

The higher indicators are powerful tools for studying pivotal categories. For example, they were used in [Ng and Schauenburg 2010] to prove that the projective representation of $\mathrm{SL}_2(\mathbb{Z})$ obtained from a modular tensor category factors through a finite quotient $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ for some n. In this article, we demonstrate that the numbers $\nu_k(V)$, as k varies over natural numbers and V varies over the set of simple objects of $\mathcal{C}$, give a strong-enough numerical invariant of $\mathcal{C}$ that is able to distinguish between any two spherical categories in an interesting class, known as Tambara–Yamagami categories (TY-categories for short).

Susan Montgomery has asked whether the FS-indicators of a semisimple Hopf algebra determine the tensor category of its representations. This was shown to be true for the class of semisimple Hopf algebras of dimension 8 in [Ng and Schauenburg 2008]. The representation categories of these Hopf algebras are TY-categories. Kashina et al. [2012] showed that, for the class of nonsemisimple Hopf algebras called Taft algebras, the second indicator can distinguish between the finite tensor categories of their representations. Along similar lines, Siu-Hung Ng (private communication) has asked whether a spherical fusion category generated by a simple object is completely determined by its FS-indicators. Our results give an affirmative answer to this question for the class of TY-categories.

Let G be a finite group. Let S be a finite set that contains G and one extra element, denoted m. Consider the following fusion rule on S:

$$g\otimes h = gh,\quad m\otimes g = g\otimes m = m,\quad m\otimes m = \bigoplus_{x\in G} x \quad \text{for all } g, h\in G.$$

Tambara and Yamagami [1998] classified all fusion categories that have the above fusion rule; for a conceptual proof of this classification, see [Etingof et al. 2010, Example 9.4]. Such fusion categories exist only if G is abelian and are classified by pairs (χ, τ) where $\chi : G\times G\to\mathbb{C}^*$ is a nondegenerate symmetric bicharacter on G and τ is a square root of $|G|^{-1}$. For each tuple (G, χ, τ) as above, there exists a spherical category, denoted $\mathrm{TY}(G, \chi, \tau)$. Two TY-categories $\mathcal{C} = \mathrm{TY}(G, \chi, \tau)$ and $\mathcal{C}' = \mathrm{TY}(G', \chi', \tau')$ are isomorphic as spherical categories if and only if $\tau = \tau'$ and $(G, \chi)\simeq(G', \chi')$, that is, there exists an isomorphism $f : G\to G'$ such that $\chi'(f(x), f(y)) = \chi(x, y)$ for all $x, y\in G$. Let $\mathrm{Irr}(\mathcal{C}) = G\cup\{m_{\mathcal{C}}\}$ be the simple objects of $\mathcal{C}$. There is a canonical (spherical) pivotal structure on $\mathcal{C}$ such that the pivotal dimension of an object matches the Frobenius–Perron dimension. For an object V of $\mathcal{C}$, let $\mathrm{pdim}(V)$ denote its pivotal dimension for this canonical pivotal structure.

We shall prove the following theorem:

Theorem 1.1. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two* TY*-categories. If*

$$\sum_{V \in \mathrm{Irr}(\mathcal{C})} \nu_k(V) = \sum_{V \in \mathrm{Irr}(\mathcal{C}')} \nu_k(V),$$

$$\sum_{V \in \mathrm{Irr}(\mathcal{C})} \mathrm{pdim}(V)\nu_k(V) = \sum_{V \in \mathrm{Irr}(\mathcal{C}')} \mathrm{pdim}(V)\nu_k(V)$$

for all $k \geq 1$, then $\mathcal{C} \simeq \mathcal{C}'$ as spherical fusion categories.

Now we shall describe our plan for the proof of this theorem and give a summary of contents of the sections. Let $\mathcal{C} = \mathrm{TY}(G, \chi, \tau)$ and $\mathcal{C}' = \mathrm{TY}(G', \chi', \tau')$ be two TY-categories. Assuming G and G' are nontrivial groups, the assumptions of Theorem 1.1 are quickly seen to be equivalent to $\nu_k(m_{\mathcal{C}}) = \nu_k(m_{\mathcal{C}'})$ and $\sum_{x \in G} \nu_k(x) = \sum_{x \in G'} \nu_k(x)$. Based on work done in [Shimizu 2011], we can easily conclude that $G \simeq G'$ and $\tau = \tau'$. Most of our work goes into showing that, if $\nu_k(m_{\mathcal{C}}) = \nu_k(m_{\mathcal{C}'})$ for all k, then $(G, \chi) \simeq (G, \chi')$. Shimizu [2011, Theorems 3.3 and 3.4] calculated $\nu_k(m_{\mathcal{C}})$ using an expression for the indicator in terms of the twist of the Drinfeld center of $\mathcal{C}$ [Ng and Schauenburg 2007a, Theorem 4.1]. This project started for us when Siu-Hung Ng asked us whether the 8-th root of unity in [Shimizu 2011, Theorem 3.5] is related to the signature modulo 8 for some related lattice. This indeed turns out to be the case. A simple restatement of Shimizu's result gives us a formula relating the indicators $\nu_{2k}(m_{\mathcal{C}})$ to certain quadratic Gauss sums; see Lemma 4.1. This formula is the starting point for our calculations, and we want to explain it in precise terms. For this, we need some notation.

Let G be an abelian group, always written additively in this paper unless otherwise stated. Let $q : G \to \mathbb{Q}/\mathbb{Z}$ be a quadratic form on G. Given a pair (G, q), one defines the associated quadratic Gauss sum

$$\Theta(G, q) = |G|^{-1/2} \sum_{x \in G} \boldsymbol{e}(q(x)), \quad \text{where } \boldsymbol{e}(x) = e^{2\pi i x}. \tag{1}$$

For $k \in \mathbb{Z}$, it will be also convenient to define the invariant

$$\xi_k(G, q) = \Theta(G, q)^k \Theta(G, -k \cdot q). \tag{2}$$

Let $\mathcal{C} = \mathrm{TY}(G, \chi, \tau)$ be a TY-category where (G, χ, τ) is a triple as above. We choose a quadratic form q on G such that $\chi(x, y) = \boldsymbol{e}(-\partial q(x, y))$ where $\partial q : G \times G \to \mathbb{Q}/\mathbb{Z}$ denotes the symmetric $\mathbb{Z}$-bilinear form

$$\partial q(x, y) = q(x + y) - q(x) - q(y). \tag{3}$$

One can show that such a q always exists. In Lemma 4.1, we prove that for $k \geq 1$

$$\nu_{2k}(m_{\mathcal{C}}) = \mathrm{sign}(\tau)^k \xi_k(G, q).$$

Much of the calculation in Sections 3 and 5 is geared towards finding explicit formulae for $\xi_k(G, q)$ by using the classification of the irreducible quadratic forms and the known values of Gauss sums of these irreducible forms. The calculations are more complicated when G is a 2-group, which is a well known feature in the theory of quadratic forms on finite abelian groups. When G is a 2-group, and $v_2(k)$ (the two-valuation of k) is at least 1, we relate $\xi_k(G, q)$ to an invariant $\sigma_{v_2(k)}(\partial q)$ of the pair $(G, \partial q)$ (see Lemma 3.8). The invariant $\sigma_n(\partial q)$ is a generalization of the Kervaire–Brown–Peterson–Browder invariant [Brown 1972; Kawauchi and Kojima 1980, p. 33]. Detailed calculation of the values of the Gauss sums and properties of the invariant $\sigma_n(\partial q)$ lets us conclude that the bicharacter χ can be recovered from values of the Gauss sums, thus proving our theorem.

Sections 2 through 4 contain preparatory material. In Section 2, we collect the background material necessary for quadratic and bilinear forms on finite abelian groups and their classification. The results here are mostly due to C. T. C. Wall [1963]; also see [Miranda 1984; Kawauchi and Kojima 1980; Nikulin 1979], wherein the proofs can be found. However, we have chosen to include the proofs of most of what we need in the detailed Appendix. In particular, we give a proof of the existence part of Wall's theorem (see Theorem 2.1) on the classification of nondegenerate quadratic and bilinear forms on finite abelian groups. We have explained our reason for including the Appendix in Section 2, following the statement of Theorem 2.1.

Section 3 contains the background on values of Gauss sums and calculation of $\xi_k(G, q)$ in various cases. Section 4 introduces the TY-categories and relates the indicator values $\nu_{2k}(\mathcal{C})$ with Gauss sums. With these preparations, we prove Theorem 1.1 in Section 5.

Finally, in Section 6, we apply Theorem 1.1 to address a recent conjecture [Turaev and Vainerman 2012] regarding 3-manifold invariants constructed from TY-categories. Given a compact 3-manifold M and a spherical category $\mathcal{C}$, one can define an invariant $|M|_{\mathcal{C}}$, called the state-sum invariant in that paper. Turaev and Virelizier [2013] showed that $|M|_{\mathcal{C}} = \tau_{Z(\mathcal{C})}(M)$, where $Z(\mathcal{C})$ is the Drinfeld center of $\mathcal{C}$ and $\tau_{Z(\mathcal{C})}(M)$ denotes the Reshetikhin–Turaev invariant. For $k \geq 1$, let $L_{k,1} = \{(z_1, z_2) \in \mathbb{C}^2 : |z_1|^2 + |z_2|^2 = 1\}/\langle (z_1, z_2) \sim e^{2\pi i/k}(z_1, z_2)\rangle$ denote the lens spaces. In Theorem 6.3, we show that a TY-category $\mathcal{C} = \mathrm{TY}(G, \chi, \tau)$ is determined by the sequence of state-sum invariants $\{|L_{k,1}|_{\mathcal{C}} : k \geq 1\}$ as long as we restrict to categories such that $|G|$ has an odd factor. Turaev and Vainerman proved this result assuming that $|G|$ is odd and conjectured that a similar result should hold for groups of even order. In Section 6, we exhibit two nonisomorphic tuples (G, χ, τ) and (G', χ', τ') such that $|L_{k,1}|_{\mathrm{TY}(G,\chi,\tau)} = |L_{k,1}|_{\mathrm{TY}(G',\chi',\tau')}$ for all k. In our example, both G and G' have order 64. This example demonstrates that one needs to put some hypothesis on the possible orders of G or else consider state-sum invariants of other 3-manifolds if one has to recover the category from the data of these invariants.

Quadratic and bilinear forms on finite abelian groups appear in various places in topology and geometry. We give some examples:

- The "torsion linking pairing" on the torsion part of the n-th integral homology of a $(2n+1)$-dimensional real compact manifold coming from Poincaré duality and intersection pairing, for example [Kawauchi and Kojima 1980]. For 3-manifolds, we get a pairing on the torsion 1-cycles related to the linking number. For this reason, discriminant forms are called linking pairs in that paper.
- Intersection pairing on the torsion part of middle cohomology of a $(4n+2)$-dimensional manifold and computation of Kervaire–Arf invariants [Brown 1972].
- Study of integral lattices coming from algebraic geometry, for example study of K_3 surfaces [Nikulin 1979]. Let G be a finite abelian group and b be a nondegenerate symmetric bilinear form on G. For each pair (G, b), there exists a pair (L, B), where $L \simeq \mathbb{Z}^n$ and $B : L \times L \to \mathbb{Z}$ is a nondegenerate symmetric $\mathbb{Z}$-bilinear form such that $G = L'/L$ and b is the $\mathbb{Q}/\mathbb{Z}$ valued form induced on L'/L by B; here L' denotes the dual lattice of L. For this reason, we have borrowed the name "discriminant form" from [Nikulin 1979] for pairs (G, b).

We hope that the methods of calculation of Gauss sums will have other uses in computations of Gauss sums coming from the above sources.

2. Bilinear and quadratic forms on finite abelian groups

Definitions. Let G be a finite abelian group (written additively). Let $\exp(G)$ denote the exponent of G. A *discriminant form* is a pair (G, b) where G is a finite abelian group and $b : G \times G \to \mathbb{Q}/\mathbb{Z}$ is a symmetric bilinear form on G. As all the bilinear forms considered in this article are symmetric, the adjective "symmetric" will sometimes be dropped. Say that b or (G, b) is *nondegenerate* if for each nonzero $x \in G$ there exists $y \in G$ such that $b(x, y) \neq 0$.

Let G be a finite abelian group and q be a quadratic form on G. We say that the pair (G, q) is a *premetric* group. We say that q is nondegenerate and (G, q) is a *metric group* if the bilinear form ∂q (see (3)) is nondegenerate.

The morphisms in the categories of discriminant forms and premetric groups are defined as usual. Isomorphisms are often called isometries. There is an obvious notion of an orthogonal direct sum on discriminant forms and premetric groups.

If (G_1, q_1) and (G_2, q_2) are two premetric groups, we let $(G_1, q_1) \perp (G_2, q_2)$ denote their orthogonal direct sum. The map $(G, q) \mapsto (G, \partial q)$ defines a functor from the category of premetric or metric groups to the category of discriminant or nondegenerate discriminant forms, respectively.

Remark. Let G be a finite abelian group. Note that a bilinear form on G takes values in $\exp(G)^{-1}\mathbb{Z}/\mathbb{Z}$. Let (G, q) be a premetric group. Let $a \in G$. Note that $\partial q(a, a) = 2q(a)$, and so q takes value in $(2\exp(G))^{-1}\mathbb{Z}/\mathbb{Z}$. If G has odd order, then $a = 2(\frac{1}{2}(\exp(G)+1))a$. So $q(a) = \frac{1}{2}(\exp(G)+1)\partial q(a, a)$. Hence, q actually takes values in $\exp(G)^{-1}\mathbb{Z}/\mathbb{Z}$ and ∂q determines q. But this fails for groups of even order. For example, consider the nondegenerate bilinear form on $\mathbb{Z}/4\mathbb{Z}$ given by $b(x, y) = xy/4$. Then $q(x) = x^2/8$ and $q'(x) = 5x^2/8$ are two distinct quadratic forms on $\mathbb{Z}/4\mathbb{Z}$ such that $\partial q = \partial q' = b$.

Definitions. Let p be a prime. If a is a rational number, $v_p(a)$ will denote the p-valuation of a. It will be convenient to extend the definition of p-valuation as follows. Let G be an abelian p-group. Define $v_p : G \to \mathbb{Z}_{\leq 0} \cup \{\infty\}$ by $v_p(x) = -\log_p(\text{order}(x))$ if x is a nonzero element of G, and $v_p(0) = \infty$. We say that $v_p(x)$ is the *p-valuation* of x.

This definition of p-valuation is useful to us because of the following example. Let $\mathbb{Q}_{(p)}$ be the ring of all rational numbers of the form m/p^r where $m \in \mathbb{Z}$ and $r \in \mathbb{Z}_{\geq 0}$. If (G, q) is a premetric p-group, then observe that q and ∂q take values in the $\mathbb{Z}$-module $\mathbb{Q}_{(p)}/\mathbb{Z}$. If α is a nonzero element of $\mathbb{Q}_{(p)}/\mathbb{Z}$, then it can be written as $p^{-n}a$ for some $a \in \mathbb{Z}$ relatively prime to p. One has $v_p(\alpha) = -n$.

Let (G, b) be a discriminant form. Let $e_1, \dots, e_k \in G$ and $b_{ij} = b(e_i, e_j)$. The matrix $B = ((b_{ij}))$ is called the *Gram matrix* of $e_1, \dots, e_k$. We shall write $\text{Gram}_b(e_1, \dots, e_n) = B$. One has

$$b\Big(\sum_i g_i e_i, \sum_j h_j e_j\Big) = (g_1, \dots, g_k)B(h_1, \dots, h_k)^{\text{tr}}, \quad g_1, \dots, g_k, h_1, \dots, h_k \in \mathbb{Z}.$$

A discriminant form or premetric group is called *irreducible* if it cannot be written as an orthogonal direct sum of two nonzero discriminant forms or premetric groups, respectively. A finite abelian group is *homogeneous* if it is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^n$ for some prime p and positive integers r and n. For a p-group G, we let $\text{rk}(G)$ denote the minimum number of generators for G or equivalently $\dim_{\mathbb{F}_p}(G/\Phi(G))$ where $\Phi(G)$ is the Frattini subgroup of G. In particular,

$$\text{rk}((\mathbb{Z}/p^r\mathbb{Z})^n) = n.$$

An element of $(\mathbb{Z}/p^r\mathbb{Z})^n$ will often be written as a vector whose entries come from $\mathbb{Z}/p^r\mathbb{Z}$. A discriminant form on a homogeneous finite abelian group will be often written as $((\mathbb{Z}/p^r\mathbb{Z})^n, B)$ where B is an $n \times n$ matrix with entries in $p^{-r}\mathbb{Z}/\mathbb{Z}$

name in [Miranda 1984]	(G, q)	$(G, \partial q)$
A_{p^r}	$\left(\mathbb{Z}/p^r\mathbb{Z}, q(x) = \frac{(p^r+1)/2}{p^r}x^2\right)$	$\left(\mathbb{Z}/p^r\mathbb{Z}, \frac{1}{p^r}\right)$
B_{p^r}	$\left(\mathbb{Z}/p^r\mathbb{Z}, q(x) = \frac{u_p(p^r+1)/2}{p^r}x^2\right)$	$\left(\mathbb{Z}/p^r\mathbb{Z}, \frac{u_p}{p^r}\right)$
A_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x) = \frac{1}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{1}{2^r}\right)$
B_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x) = \frac{-1}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{-1}{2^r}\right)$
C_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x) = \frac{5}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{5}{2^r}\right)$
D_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x) = \frac{-5}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{-5}{2^r}\right)$
E_{2^r}	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, q(x_1, x_2) = \frac{x_1x_2}{2^r}\right)$	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, \left(\begin{smallmatrix} 0 & 2^{-r} \\ 2^{-r} & 0 \end{smallmatrix}\right)\right)$
F_{2^r}	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, q(x_1, x_2) = \frac{x_1^2+x_1x_2+x_2^2}{2^r}\right)$	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, \left(\begin{smallmatrix} 2^{1-r} & 2^{-r} \\ 2^{-r} & 2^{1-r} \end{smallmatrix}\right)\right)$

Table 1. Irreducible quadratic and symmetric bilinear forms. In the first two rows, p represents an odd prime. For the prime 2 and for $r = 1$ or 2, some of the forms above are isometric. For example, $A_2 \simeq C_2$.

such that $b(x, y) = xBy^{\mathrm{tr}}$ for all $x, y \in (\mathbb{Z}/p^r\mathbb{Z})^n$. Let p be an odd prime and u_p denote a quadratic nonresidue modulo p. Table 1 lists the irreducible metric groups (G, q) and corresponding irreducible discriminant forms $(G, \partial q)$.

Theorem 2.1 [Wall 1963; Miranda 1984; Nikulin 1979]. (a) *Each nondegenerate discriminant form is an orthogonal direct sum of the irreducible discriminant forms listed in Table 1.*

(b) *Each metric group is an orthogonal direct sum of the irreducible metric groups listed in Table 1.*

It follows that, given any nondegenerate symmetric bilinear form b on a finite abelian group G, there exists a quadratic form q on G such that $\partial q = b$.

A proof of Theorem 2.1 has been sketched in the Appendix. Here we shall only give a brief indication of our argument. This argument seems to be different from the proofs in the references above, and we believe it is simpler. It is probably well known to experts, but we have not seen it in the literature.

Let (G, b) be a discriminant form. Write $G = \bigoplus_p G_{(p)}$ where $G_{(p)}$ is the p-Sylow subgroup of G. Let $b_{(p)}$ be the restriction of b to $G_{(p)} \times G_{(p)}$. Clearly (G, b) is an orthogonal direct sum of $(G_{(p)}, b_{(p)})$ as p varies over primes. So it suffices to decompose (G, b) into irreducibles when G is a p-group for some prime p.

Let G be a finite abelian p-group and b be a nondegenerate symmetric bilinear form on G. The algorithm for decomposing (G, b) into irreducibles boils down to diagonalizing symmetric matrices with entries in $\mathbb{Q}_{(p)}/\mathbb{Z}$ via conjugation. The algorithm for diagonalization is the same as the well known algorithm for diagonalizing quadratic forms over p-adic integers; see for example [Conway and Sloane 1999, Chapter 15, §4.4]. This algorithm is the core of our argument. We repeat that we could not find this argument in literature for bilinear forms on finite abelian groups. This is our first reason for including the Appendix. A second reason is that the argument is constructive, and so it can be useful in actually decomposing given bilinear forms over finite abelian groups into irreducibles. A third reason is that part (b) of Theorem 2.1 as well as Lemma 2.2 (which we need in our arguments) are not explicitly stated in [Wall 1963]. They can probably be extracted from the arguments in [Wall 1963] or [Miranda 1984; Nikulin 1979]. But this might require some work mainly because each paper has its own rather complicated set of notations.

The following lemma, describing the nondegenerate quadratic forms on $(\mathbb{Z}/2^r\mathbb{Z})^2$, is essential to the proof of Theorem 2.1. It is stated here because we shall also use it in the computation of some Gauss sums. It can be proved using Hensel's lemma. A proof is given in the Appendix.

Lemma 2.2. *Set $G = (\mathbb{Z}/2^r\mathbb{Z})^2$ and let q be an irreducible nondegenerate quadratic form on G. Then there exist integers A, B, C with B odd such that $q(x_1, x_2) = 2^{-r}(Ax_1^2 + Bx_1x_2 + Cx_2^2)$. If AC is even, then $(G, q) \simeq ((\mathbb{Z}/2^r\mathbb{Z})^2, x_1x_2/2^r)$. Otherwise, $(G, q) \simeq ((\mathbb{Z}/2^r\mathbb{Z})^2, (x_1^2 + x_1x_2 + x_2^2)/2^r)$.*

3. Gauss sums and related invariants of a quadratic form

Let G be a finite abelian group and $q : G \to \mathbb{Q}/\mathbb{Z}$ be a quadratic form on G. In Section 1, we defined the quadratic Gauss sums $\Theta(G, q)$ and the related invariant $\xi_k(G, q)$; see (1) and (2). In this section, we shall compute the invariants $\Theta(G, q)$ and $\xi_k(G, q)$ for various pairs (G, q). One verifies that Θ is multiplicative, that is,

$$\Theta((G_1, q_1) \perp (G_2, q_2)) = \Theta(G_1, q_1)\Theta(G_2, q_2).$$

In the same sense, ξ_k is also multiplicative. We start with the following well known result. The proof is omitted.

Theorem 3.1. (a) *Let $\chi : G \to \mathbb{C}^*$ be a character on G. Then $\sum_{x\in G} \chi(x) = |G|$ if $\chi = 1$ and $\sum_{x\in G} \chi(x) = 0$ otherwise.*

(b) *If q is a nondegenerate quadratic form on G, then $\Theta(G, q)\Theta(G, -q) = 1$ and, in particular, $|\Theta(G, q)|^2 = 1$.*

The next lemma gives the values of the Gauss sums of irreducible nondegenerate forms.

Lemma 3.2. (a) *Let p be an odd prime and α be an integer relatively prime to p. Then*

$$\Theta\big(\mathbb{Z}/p^r\mathbb{Z}, \alpha(p^r+1)x^2/2p^r\big) = \Big(\frac{2\alpha}{p}\Big)^r \epsilon_{p^r},$$

where $\big(\frac{2\alpha}{p}\big)$ denotes the Legendre symbol and $\epsilon_m = 1$ if $m \equiv 1 \bmod 4$ and $\epsilon_m = i$ if $m \equiv 3 \bmod 4$.

(b) *Let α be an odd integer. Then*

$$\Theta(\mathbb{Z}/2^r\mathbb{Z}, \alpha x^2/2^{r+1}) = (-1)^{r(\alpha^2-1)/8}\boldsymbol{e}(\alpha/8).$$

(c) *Let α, β, and γ be integers with β odd. Then*

$$\Theta((\mathbb{Z}/2^r\mathbb{Z})^2, (\alpha x_1^2 + \beta x_1 x_2 + \gamma x_2^2)/2^r) = (-1)^{\alpha\gamma r}.$$

Proof. For part (a), see for example [Iwaniec and Kowalski 2004, p. 52]. Let G_r and G'_r denote the left-hand sides of the formulae in parts (b) and (c), respectively. Then one verifies that $G_r = 2G_{r-2}$ and $G'_r = 4G'_{r-2}$ for $r > 2$. Parts (b) and (c) now follow by induction once the formulae for $r = 1$ and 2 are verified. □

Since Θ is multiplicative, one can calculate the Gauss sums of arbitrary nondegenerate forms by first decomposing the forms into orthogonal direct sums of irreducible forms and using Lemma 3.2. We will also need to compute the Gauss sums of some singular forms. This is the purpose of the lemma below.

Lemma 3.3. (a) *Let p be a prime. Let $G = (\mathbb{Z}/p^r\mathbb{Z})^n$, and let q be a $p^{-r}\mathbb{Z}/\mathbb{Z}$-valued quadratic form on G. Let $0 \le s \le r$. Then $p^s q$ induces a quadratic form on $G/p^{r-s}G$ and*

$$\Theta(G, p^s q) = p^{sn/2}\Theta(G/p^{r-s}G, p^s q).$$

(b) *Let α be an odd integer. Then one has*

$$\Theta\Big(\mathbb{Z}/2^r\mathbb{Z}, 2^s\cdot\frac{\alpha x^2}{2^{r+1}}\Big) = \begin{cases} 2^{s/2}(-1)^{(r-s)(\alpha^2-1)/8}\boldsymbol{e}(\alpha/8) & \text{if } 0 \le s < r, \\ 0 & \text{if } s = r, \\ 2^{r/2} & \text{if } s > r. \end{cases}$$

Proof. (a) If $x \equiv x' \bmod p^{r-s}G$, then $p^s q(x) = p^s q(x')$ since q and ∂q take values in $p^{-r}\mathbb{Z}/\mathbb{Z}$. So $p^s q(x)$ induces a form on $G/p^{r-s}G$. One has

$$|G|^{1/2}\Theta(G, p^s q) = \sum_{x\in G}\boldsymbol{e}(p^s q(x)) = |p^{r-s}G| \sum_{y\in G/p^{r-s}G}\boldsymbol{e}(p^s q(y))$$
$$= |p^{r-s}G||G/p^{r-s}G|^{1/2}\Theta(G/p^{r-s}G, p^s q).$$

Part (a) follows since $|p^{r-s}G| = p^{sn}$.

(b) First suppose $r - s \geq 1$. Note that, if $y \equiv x \mod 2^{r-s}$, then $\alpha y^2/2^{r-s+1} \equiv \alpha x^2/2^{r-s+1} \mod \mathbb{Z}$. So

$$2^{r/2}\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, 2^s \cdot \frac{\alpha x^2}{2^{r+1}}\right) = \sum_{x=0}^{2^r-1} \boldsymbol{e}\left(\frac{\alpha x^2}{2^{r-s+1}}\right)$$
$$= 2^s \sum_{x=0}^{2^{r-s}-1} \boldsymbol{e}\left(\frac{\alpha x^2}{2^{r-s+1}}\right) = 2^{(r+s)/2}\Theta\left(\mathbb{Z}/2^{r-s}\mathbb{Z}, \frac{\alpha x^2}{2^{r-s+1}}\right).$$

Part (b) now follows from Lemma 3.2 for $0 \leq s < r$. Now let $s = r$. Note that, if $y \equiv x \mod 2$, then $\alpha x^2/2 \equiv \alpha y^2/2 \mod \mathbb{Z}$. So

$$2^{r/2}\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, 2^s \cdot \frac{\alpha x^2}{2^{r+1}}\right) = \sum_{x=0}^{2^r-1} \boldsymbol{e}(\alpha x^2/2) = 2^{r-1}\sum_{x=0}^{1} \boldsymbol{e}(\alpha x^2/2) = 0.$$

For $s > r$, the quadratic form we have is identically equal to 0, so the result is obvious. □

Lemma 3.4. *Let p be an odd prime, and let both r and k be positive integers. Let q_1 and q_2 be the two nonisometric nondegenerate quadratic forms on $G = \mathbb{Z}/p^r\mathbb{Z}$. Then*

$$\xi_k(G, q_1) = (-1)^{\epsilon^k_{p,r}}\xi_k(G, q_2)$$

where $\epsilon^k_{p,r} = r(k+1) - \min\{r, v_p(k)\}$.

Proof. There are only two distinct nondegenerate quadratic forms on G; see Table 1. Without loss of generality, we may thus assume that $q_j(x) = u_j(p^r+1)x^2/2p^r$ for $j = 1, 2$, where $u_1 = 1$ and $u_2 = u_p$ is a quadratic nonresidue modulo p. Lemma 3.2(a) implies $\Theta(G, q_1) = (-1)^r\Theta(G, q_2)$. If $v_p(k) > r$, the lemma holds by the fact that $\Theta(G, -kq) = \sqrt{|G|}$.

Now assume $0 \leq v_p(k) \leq r$. Write $s = v_p(k)$ and $-k = p^s a$ with $a \in \mathbb{Z}$ relatively prime to s. Then $\Theta(G, -kq_j)$ is equal to

$$\Theta(G, p^s a q_j) = p^{s/2}\Theta(\mathbb{Z}/p^{r-s}\mathbb{Z}, p^s a u_j(p^r+1)x^2/2p^r)$$
$$= p^{s/2}\Theta(\mathbb{Z}/p^{r-s}\mathbb{Z}, (p^{r-s}+1)a u_j x^2/2p^{r-s}).$$

The first equality follows from Lemma 3.3(a). For the second, we need to observe that the quadratic forms $(p^{r-s}+1)\alpha x^2/2p^{r-s}$ and $(p^r+1)\alpha x^2/2p^{r-s}$ are identical on $\mathbb{Z}/p^{r-s}\mathbb{Z}$. From Lemma 3.2(a), we have

$$\Theta\big(\mathbb{Z}/p^{r-s}\mathbb{Z}, (p^{r-s}+1)a u_p x^2/2p^{r-s}\big)$$
$$= (-1)^{r-s}\Theta\big(\mathbb{Z}/p^{r-s}\mathbb{Z}, (p^{r-s}+1)a x^2/2p^{r-s}\big),$$

which implies $\Theta(G, -kq_2) = (-1)^{r-v_p(k)}\Theta(G, -kq_1)$. The lemma follows once we recall that $\Theta(G, q_1) = (-1)^r\Theta(G, q_2)$. □

Next, we shall introduce an invariant $\sigma_k(b)$ of a discriminant form (G, b) defined in [Kawauchi and Kojima 1980] and in Lemma 3.6 compare it to our Gauss sums (discriminant forms are called linking pairs in [Kawauchi and Kojima 1980]).

Definitions. For the convenience of the reader, we shall recall some of the definitions from [Kawauchi and Kojima 1980; Wall 1963]. Let G be a finite abelian group. Let

$$G[n] = \{x \in G : nx = 0\}$$

denote the n-torsion subgroup of G. Let p be a prime. Then $G_{(p)} = \bigcup_n G[p^n]$ is the p-Sylow subgroup of G. For $k \geq 1$, define

$$\widetilde{G}_p^k = G[p^k]/(G[p^{k-1}] + pG[p^{k+1}]).$$

Take a decomposition of G into a direct sum of cyclic groups of prime power order. If such a decomposition has n factors isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$, then $\widetilde{G}_p^k$ is an elementary abelian p-group of rank n. Let b be a nondegenerate symmetric bilinear form on G. Then

$$\tilde{b}_p^k([x], [y]) = p^{k-1} b(x, y)$$

defines a nondegenerate bilinear form on $\widetilde{G}_p^k$. Here x and y denote any two elements of $G[p^k]$ representing $[x], [y] \in \widetilde{G}_p^k$, respectively.

Let $c^k(b)$ be the characteristic element (also called parity element) of the $\mathbb{F}_2$-quadratic space $(\widetilde{G}_2^k, \tilde{b}_2^k)$. Explicitly, $c^k(b)$ is the unique element of $\widetilde{G}_2^k$ such that $\tilde{b}_2^k(x, x) = \tilde{b}_2^k(x, c^k(b))$ for all $x \in \widetilde{G}_2^k$. In other words, $c^k(b)$ is represented by any $c \in G[2^k]$ that satisfies

$$2^{k-1} b(x, x) = 2^{k-1} b(x, c) \quad \text{for all } x \in G[2^k].$$

Note that both sides of the above equality can only take the values 0 or 1/2. Also observe that the characteristic element $c^k(b)$ is zero if and only if $b(x, x) \in 2^{1-k}\mathbb{Z}/\mathbb{Z}$ for all $x \in G[2^k]$.

The invariant $\sigma_k(b)$ takes values in $(\mathbb{Z}/8\mathbb{Z}) \cup \{\infty\}$, which is made into a semigroup by defining $\infty + \infty = n + \infty = \infty$ for $n \in \mathbb{Z}/8\mathbb{Z}$. If $c^k(b) \neq 0$, then $\sigma_n(b) = \infty$ by definition. If $c^k(b) = 0$, then one checks that

$$q_k(x) = 2^{k-1} b(x, x)$$

induces a well defined quadratic form on $G_{(2)}/G[2^k]$ and, following [Kawauchi and Kojima 1980], we can define $\sigma_k(b)$ by

$$|G_{(2)}/G[2^k]|^{1/2} \Theta(G_{(2)}/G[2^k], q_k) = C\boldsymbol{e}(\sigma_k(b)/8),$$

where C is the absolute value of the left-hand side of the equation [Kawauchi and Kojima 1980, §2]; we shall soon see that $C \neq 0$. If $x, y \in G_{(2)}$ represent $[x], [y] \in G_{(2)}/G[2^k]$, then $\partial q_k([x], [y]) = 2^k b(x, y)$. Suppose $[x] \in G_{(2)}/G[2^k]$

such that $\partial q_k([x],[y]) = 0$ for all $[y] \in G_{(2)}/G[2^k]$. Let $x \in G_{(2)}$ be a representative for $[x]$. Then $2^k b(x, y) = 0$ for all $y \in G_{(2)}$. Since b is nondegenerate, it follows that $2^k x = 0$, so $[x] = 0$ in $G_{(2)}/G[2^k]$. So we have argued that, if $c^k(b) = 0$, then $q_k(x)$ is a nondegenerate form on $G_{(2)}/G[2^k]$. Hence, Theorem 3.1(b) gives $C = |G_{(2)}/G[2^k]|^{1/2}$. So $\sigma_k(b)$ is in fact given by the simpler formula

$$\Theta(G_{(2)}/G[2^k], q_k) = \boldsymbol{e}(\sigma_k(b)/8). \tag{4}$$

The following theorem is the reason for our interest in the invariant $\sigma_k(b)$, and it follows from Theorem 4.1 of [Kawauchi and Kojima 1980].

Theorem 3.5. *Let G be a finite abelian 2-group, and let b and b' be two nondegenerate symmetric bilinear forms on G. Then $(G, b) \simeq (G, b')$ if and only if $\sigma_k(b) \simeq \sigma_k(b')$ for all $k \geq 1$.*

Definition. It will be convenient for us to work with the invariant

$$\varsigma_k(b) = \boldsymbol{e}(\sigma_k(b)/8) \tag{5}$$

rather than $\sigma_k(b)$. If $\sigma_k(b) = \infty$, then we define $\varsigma_k(b) = 0$. So ς_k takes values in the multiplicative semigroup $\mu_8 \cup \{0\}$ where μ_8 is the group of 8-th roots of unity. From Corollary 2.2 of [Kawauchi and Kojima 1980], it follows that, if $(G, b) = (G_1, b_1) \perp (G_2, b_2)$, then $\varsigma_k(b) = \varsigma_k(b_1)\varsigma_k(b_2)$. In other words, ς_k is multiplicative, just like the Gauss sums or the invariant ξ_k. The multiplicativity of $\varsigma_k(b)$ also follows from the next lemma.

Lemma 3.6. *Let G be a finite abelian 2-group, and let b be a nondegenerate symmetric bilinear form on G. Let $k \geq 1$. Then*

$$\Theta(G, 2^{k-1}b(x, x)) = |G[2^k]|^{1/2}\varsigma_k(b).$$

Let q be a nondegenerate quadratic form on G. Then with $b = \partial q$, the above equation yields

$$\varsigma_k(\partial q) = |G[2^k]|^{-1/2}\Theta(G, 2^k q). \tag{6}$$

Proof. Let $q_k(x) = 2^{k-1}b(x, x)$. Let w vary over a set of coset representatives of $G/G[2^k]$ and y vary over $G[2^k]$. Then

$$|G|^{1/2}\Theta(G, q_k) = \sum_{w,y} \boldsymbol{e}(q_k(w + y)) = \sum_{w} \boldsymbol{e}(q_k(w)) \sum_{y} \boldsymbol{e}(2^{k-1}b(y, c^k(b))). \tag{7}$$

The second equality follows since $2^k b(w, y) = 0$ and $2^{k-1}b(y, y) = 2^{k-1}b(y, c^k(b))$. If $c^k(b) \neq 0$, then $y \mapsto \boldsymbol{e}(2^{k-1}b(y, c^k(b)))$ is a nontrivial character on $G[2^k]$, so the inner sum in (7) is zero; hence, $\Theta(G, 2^{k-1}b(x, x)) = 0$. Now suppose $c^k(b) = 0$. Then we find that $2^{k-1}b(w, w) = 2^{k-1}b(w', w')$ if $w \equiv w' \bmod G[2^k]$. Thus,

$(w \mapsto q_k(w))$ induces a quadratic form on $G/G[2^k]$. From (7), we get

$$|G|^{1/2}\Theta(G,q_k) = |G[2^k]| \sum_{w\in G/G[2^k]} \boldsymbol{e}(q_k(w)) = |G[2^k]|\sqrt{|G/G[2^k]|}\,\Theta(G/G[2^k],q_k).$$

The lemma follows from (4). □

Lemma 3.7. *Let (G,q) be an irreducible metric 2-group with $\exp(G)=2^r$ (see Table 1). Let β be an odd integer and $n\ge 1$. Then*

$$\varsigma_n(\partial q)^{\beta 2^n} = \begin{cases} 0 & \text{if } n=r \text{ and } \operatorname{rk}(G)=1,\\ (-1)^{\operatorname{rk}(G)\delta_{n,2}\delta_{r,1}}\Theta(G,q)^{\beta 2^n} & \text{otherwise},\end{cases} \tag{8}$$

where $\delta_{i,j}$ is the Kronecker delta, and

$$\Theta(G,\beta 2^n q) = |G[2^n]|^{1/2}(-1)^{\operatorname{rk}(G)\max\{r-n,0\}(\beta^2-1)/8}\varsigma_n(\partial q)^{\beta}. \tag{9}$$

Proof. We treat the cases $\operatorname{rk}(G)=1$ and $\operatorname{rk}(G)=2$ separately. First suppose G has rank 1, that is, $(G,q)\simeq(\mathbb{Z}/2^r\mathbb{Z},\alpha x^2/2^{r+1})$ where $\alpha\in\{\pm1,\pm5\}$. Then from Lemma 3.2(b), we find that $\Theta(G,q)=\pm\boldsymbol{e}(\alpha/8)$. Since $n\ge1$, we have

$$\Theta(G,q)^{\beta 2^n} = \boldsymbol{e}(\alpha/8)^{\beta 2^n}. \tag{10}$$

Now we split the argument into three cases.

Case 1 ($n>r$). Then $\Theta(G,2^n\beta q)=|G|^{1/2}=|G[2^n]|^{1/2}$, and so (6) implies $\varsigma_n(\partial q)=1$. This verifies (9). From (10), we obtain $\Theta(G,q)^{\beta 2^n}=\boldsymbol{e}(\alpha/8)^{\beta 2^n}=(-1)^{\delta_{n,2}\delta_{r,1}}$. This verifies (8).

Case 2 ($n=r$). Lemma 3.3(b) implies that $\Theta(G,2^n\beta q)=0$. From (6), we get $\varsigma_n(\partial q)=|G[2^n]|^{-1/2}\Theta(G,2^n q)=0$ too. This verifies (8) and (9) in this case.

Case 3 ($1\le n<r$). From (6) and Lemma 3.3(b), we have

$$\varsigma_n(\partial q) = |G[2^n]|^{-1/2}\Theta(G,2^n q) = 2^{-n/2}\Theta\Big(\mathbb{Z}/2^r\mathbb{Z}, 2^n\frac{\alpha x^2}{2^{r+1}}\Big) = (-1)^{(r-n)(\alpha^2-1)/8}\boldsymbol{e}(\alpha/8).$$

Since $n\ge1$, using (10), we obtain $\varsigma_n(\partial q)^{\beta 2^n}=\boldsymbol{e}(\alpha/8)^{\beta 2^n}=\Theta(G,q)^{\beta 2^n}$, which verifies (8). To verify the expression for $\Theta(G,\beta 2^n q)$, we compute as follows:

$$\begin{aligned}\Theta(G,2^n\beta q) &= \Theta\Big(\mathbb{Z}/2^r\mathbb{Z}, 2^n\frac{\beta\alpha x^2}{2^{r+1}}\Big)\\ &= 2^{n/2}(-1)^{(r-n)(\alpha^2\beta^2-1)/8}\boldsymbol{e}(\beta\alpha/8)\\ &= 2^{n/2}(-1)^{(r-n)(\beta^2-1)/8}\big((-1)^{(r-n)(\alpha^2-1)/8}\boldsymbol{e}(\alpha/8)\big)^{\beta}\\ &= 2^{n/2}(-1)^{(r-n)(\beta^2-1)/8}\varsigma_n(\partial q)^{\beta},\end{aligned}$$

where the third equality follows from the fact that for odd integers β and α

$$(\alpha^2\beta^2 - 1) - (\beta^2 - 1) - \beta(\alpha^2 - 1) = \beta(\beta - 1)(\alpha^2 - 1) \equiv 0 \bmod 16. \tag{11}$$

This verifies (9) and finishes the argument in the case $\mathrm{rk}(G) = 1$.

Now assume $\mathrm{rk}(G) = 2$. If $n < r$, then (6) and Lemmas 3.3(a) and 3.2(c) give us $\varsigma_n(\partial q) = \pm 1$ (or else see Corollary 2.2 of [Kawauchi and Kojima 1980]). If $n \geq r$, then from (4), we obtain, $\varsigma_n(\partial q) = \Theta(G/G[2^n], 2^n q)$. Since $G[2^n] = G$, the Gauss sum is equal to 1 and thus $\varsigma_n(\partial q) = 1$. Thus, in any case, we find that $\varsigma_n(\partial q) = \pm 1$. Lemma 3.2(c) tells us that $\Theta(G, q) = \pm 1$ as well. Now (8) follows since $n \geq 1$.

Since $\varsigma_n(\partial q) = \pm 1$, the right-hand side of (9) becomes

$$|G[2^n]|^{1/2} \varsigma_n(\partial q).$$

Since G is of type E_{2^r} or F_{2^r}, Lemma 2.2 implies $(G, \beta q) \simeq (G, q)$. So $(G, 2^n\beta q) \simeq (G, 2^n q)$, and (9) follows immediately from (6). □

Lemma 3.8. *Let (G, q) be a metric 2-group. Let $n \geq 1$ and β be an odd positive integer. Let $\varsigma_n(\partial q)$ be the invariant introduced in* (5)*. Then*

$$\xi_{2^n\beta}(G, q) = (-1)^{\Gamma_{G,\beta,n}} |G[2^n]|^{1/2} \varsigma_n(\partial q)^{(2^n-1)\beta}$$

where $\Gamma_{G,\beta,n}$ is an integer dependent on G, β, and n and independent of q. More precisely, if we write $G \simeq \bigoplus_{r=1}^{\infty} (\mathbb{Z}/2^r\mathbb{Z})^{N_r}$, then

$$\Gamma_{G,\beta,n} = \delta_{n,2} N_1 + \sum_{r=1}^{\infty} N_r \max\{r - n, 0\}(\beta^2 - 1)/8.$$

Proof. Observe that both sides of the equation we want to prove are multiplicative invariants of a metric group. Since any metric group (G, q) can be decomposed into irreducibles by Theorem 2.1, it suffices to prove the equation when (G, q) is an irreducible metric group. Assume (G, q) is an irreducible metric group of exponent 2^r; the possibilities for these are given in Table 1. Note that G is isomorphic to $(\mathbb{Z}/2^r\mathbb{Z})$ or $(\mathbb{Z}/2^r\mathbb{Z})^2$ and $N_j = \delta_{j,r}\,\mathrm{rk}(G)$. So the equation we want to prove becomes

$$\Theta(G, q)^{\beta 2^n} \Theta(G, -\beta 2^n q) = (-1)^{\mathrm{rk}(G)\delta_{n,2}\delta_{1,r} + \mathrm{rk}(G)\max\{r-n,0\}(\beta^2-1)/8} |G[2^n]|^{1/2} \varsigma_n(\partial q)^{(2^n-1)\beta}.$$

This equation follows directly from Lemma 3.7. □

4. Indicator of Tambara–Yamagami categories as Gauss sums

Let G be a finite abelian group. A function $\chi : G \times G \to \mathbb{C}^*$ is called a *symmetric bicharacter* on G if $\chi(x, \cdot)$ and $\chi(\cdot, x)$ are characters on G and $\chi(x, y) = \chi(y, x)$

for each $x, y \in G$. A symmetric bilinear form b on G determines a symmetric bicharacter $\chi : G \times G \to \mathbb{C}^*$ given by $\chi(x, y) = \boldsymbol{e}(-b(x, y))$ (the minus sign in front of b is for consistency with notation in [Shimizu 2011]). This sets up a natural correspondence between bilinear forms and bicharacters. We say χ is nondegenerate if b is.

Let G be a finite abelian group, χ be a nondegenerate symmetric bicharacter on G, and τ be a square root of $|G|^{-1}$. Let b be the bilinear form on G given by $\chi(x, y) = \boldsymbol{e}(-b(x, y))$. Given any triple (G, χ, τ), there exists a spherical fusion category $\mathcal{C}$, called the Tambara–Yamagami category or TY-category for short. We shall denote this category by $\mathrm{TY}(G, \chi, \tau)$ or by $\mathrm{TY}(G, b, \tau)$. The simple objects of $\mathcal{C}$ are $G \cup \{m\}$. We shall write $m = m_{\mathcal{C}}$ if there is a chance of confusion. The associativity constraint in $\mathrm{TY}(G, \chi, \tau)$ is dictated by the bicharacter χ and $\mathrm{sign}(\tau)$. See [Tambara and Yamagami 1998] or [Shimizu 2011] for more details on the TY-categories. *Caution*: the abelian groups in [Shimizu 2011] are multiplicative while for our purpose it is convenient to write the group G additively.

For each simple object x of a spherical fusion category and each integer $k \geq 1$, one can associate a complex number $\nu_k(x)$, introduced in [Ng and Schauenburg 2007b], called the k-th Frobenius–Schur indicator of x. The lemma below tells us the indicators of the simple objects of a TY-category. This is an easy translation of results in [Shimizu 2011]. Our main observation is noting that the indicators of the object $m_{\mathcal{C}}$ can be expressed in terms of certain Gauss sums.

Lemma 4.1. *Let $\mathcal{C} = \mathrm{TY}(G, \chi, \tau)$ be a* TY*-category. From* [Shimizu 2011, Theorem 3.2], *we know that $\nu_k(x) = \delta_{x^k,1}$ for $x \in G$. Let b be the bilinear form on G given by $\chi(x, y) = \boldsymbol{e}(-b(x, y))$. Let q be any quadratic form such that $\partial q = b$. Then for all $k \geq 1$, one has $\nu_{2k-1}(m_{\mathcal{C}}) = 0$ and*

$$\nu_{2k}(m_{\mathcal{C}}) = \mathrm{sign}(\tau)^k \Theta(G, q)^k \Theta(G, -kq) = \mathrm{sign}(\tau)^k \xi_k(G, q),$$

and this value does not depend on the choice of q.

Proof. From Theorem 3.3 of [Shimizu 2011], we know that $\nu_{2k-1}(m) = 0$. Let

$$C(\chi) = \{\varphi : G \to \mathbb{C} : \varphi(x)\varphi(y)\varphi(x+y)^{-1} = \chi(x, y) \text{ for } x, y \in G\}.$$

From the proof of that result, we have

$$\nu_{2k}(m_{\mathcal{C}}) = \frac{1}{|G|} \sum_{\varphi \in C(\chi)} \left(\tau \sum_{x \in G} \varphi(x) \right)^k \sqrt{|G|}. \tag{12}$$

By definition, $\boldsymbol{e} \circ q \in C(\chi)$. One checks that G acts simply transitively on $C(\chi)$ by $a \cdot \varphi(x) = \varphi(x)\chi(a, x)^{-1}$. So $C(\chi) = \{\varphi_a : a \in G\}$ where $\varphi_a(x) = \boldsymbol{e}(q(x))\chi(a, x)^{-1}$.

One has

$$\begin{aligned}\tau\sum_{x\in G}\varphi_a(x) &= \frac{\operatorname{sign}(\tau)}{\sqrt{|G|}}\sum_{x\in G}\boldsymbol{e}(q(x)+b(a,x)+q(a)-q(a))\\ &= \frac{\operatorname{sign}(\tau)\boldsymbol{e}(-q(a))}{\sqrt{|G|}}\sum_{x\in G}\boldsymbol{e}(q(x+a))\\ &= \operatorname{sign}(\tau)\boldsymbol{e}(-q(a))\Theta(G,q).\end{aligned}$$

From (12), it follows that

$$\begin{aligned}\nu_{2k}(m_{\mathcal{C}}) &= \frac{\operatorname{sign}(\tau)^k}{\sqrt{|G|}}\sum_{a\in G}\boldsymbol{e}(-kq(a))\Theta(G,q)^k\\ &= \operatorname{sign}(\tau)^k\Theta(G,q)^k\Theta(G,-kq).\end{aligned}$$

To complete the proof, observe that the expression on the right-hand side of (12) only depends on χ and is independent of the choice of q. □

We shall need the following.

Lemma 4.2 [Shimizu 2011, Theorem 3.5]. *Let $\mathcal{C}=\mathrm{TY}(G,b,\tau)$ be a* TY*-category. Let q be a quadratic form such that $\partial q=b$. Then $\nu_{2k}(m)=|G[k]|^{1/2}\psi$ where $\psi\in\mu_8\cup\{0\}$* (*recall that μ_8 denotes the set of* 8*-th roots of unity*). *One has $\psi=0$ if and only if there exists $a\in G[k]$ such that $kq(a)\neq 0$.*

Remark. We should mention that, from the values of the Gauss sums given in the previous section and the decomposition of (G,q) into irreducibles, we can show that $\xi_k(G,q)=0$ if and only if (G,q) contains an irreducible component that equals A_{2^r}, B_{2^r}, C_{2^r}, or D_{2^r} where $r=v_2(k)$ for some even k and that this yields another proof of Lemma 4.2.

Let (G,q) be a premetric group. The invariant $\xi_k(G,q)$ can itself be expressed as a Gauss sum as follows. Let $\mathcal{F}_k(G,q)$ denote the premetric group given by the abelian group $\{(g_1,\dots,g_k)\in G^k:\sum_j g_j=0\}$ with the quadratic form $q(g_1,\dots,g_k)=\sum_j q(g_j)$. Then one can show that $\xi_k(G,q)=\mathcal{F}_k(G,q)$. In view of this formula, the appearance of the 8-th root of unity ψ in the above lemma becomes a consequence of Milgram's formula.

5. Tambara–Yamagami categories are determined by the higher Frobenius–Schur-indicators

In this section, we shall prove Theorem 1.1. Let $\mathcal{C}=\mathrm{TY}(G,\chi,\tau)$ be a TY-category. We shall show that the Frobenius–Schur indicators of the simple objects of $\mathcal{C}$ determine the triple (G,χ,τ). So the indicators can distinguish between any two TY-categories. Most of the work goes into showing that the indicators $\nu_k(m_{\mathcal{C}})$

determine the bicharacter χ. Let q be a quadratic form on G such that $\chi(x, y) = \boldsymbol{e}(-\partial q(x, y))$. Then Lemma 4.1 gives $\nu_k(m_{\mathcal{C}}) = \operatorname{sgn}(\tau)^k \xi_k(G, q)$ where $\xi_k(G, q)$ is a product of quadratic Gauss sums. Based on computations in Section 3, we shall argue that the invariants $\xi_k(G, q)$ determine the bicharacter χ. We need a couple of lemmas before proving Theorem 1.1. The lemmas let us handle special cases.

Lemma 5.1. *Let G be an abelian group of odd order. Let b_1 and b_2 be two nonisometric nondegenerate symmetric bilinear forms on G. Let q_1 and q_2 be quadratic forms such that $\partial q_j = b_j$ for $j = 1, 2$. Then either there exists an odd positive integer k such that $\xi_k(G, q_1) \neq \xi_k(G, q_2)$ or else, for each natural number γ, there exists a positive integer k with $v_2(k) = \gamma$ and $\xi_k(G, q_1) \neq \xi_k(G, q_2)$.*

Proof. Fix a nonsquare u_p modulo p for each odd prime p. Recall from Table 1

$$A_{p^r} = \left(\mathbb{Z}/p^r\mathbb{Z}, q(x) = \frac{2^{-1}x^2}{p^r}\right) \quad \text{and} \quad B_{p^r} = \left(\mathbb{Z}/p^r\mathbb{Z}, q(x) = \frac{2^{-1}u_p x^2}{p^r}\right).$$

We will also use the notation

$$n\cdot A_{p^r} = \left(\mathbb{Z}/p^r\mathbb{Z}, q(x) = \frac{2^{-1}nx^2}{p^r}\right) \quad \text{and} \quad n\cdot B_{p^r} = \left(\mathbb{Z}/p^r\mathbb{Z}, q(x) = \frac{2^{-1}u_p n x^2}{p^r}\right)$$

for $n \in \mathbb{Z}$. Write $G \simeq \bigoplus_{p,r} (\mathbb{Z}/p^r\mathbb{Z})^{N_{p,r}}$ where p ranges over odd primes and $r \geq 1$. Since $A_{p^r} \perp A_{p^r} \simeq B_{p^r} \perp B_{p^r}$ [Wall 1963, Theorem 4], the metric group (G, q_j) is an orthogonal direct sum, over all (p, r) such that $N_{p,r} \neq 0$, of the homogeneous metric groups

$$A_{p^r}^{N_{p,r}-1} \perp C_{p,r}^j,$$

where $C_{p,r}^j$ is either A_{p^r} or B_{p^r}. Since ξ_k is multiplicative, we have

$$\xi_k(G, q_j) = \prod_{p,r:N_{p,r}\neq 0} \xi_k(A_{p^r})^{N_{p,r}-1} \xi_k(C_{p,r}^j). \tag{13}$$

Let

$$\mathcal{A} = \{(p, r) : N_{p,r} \neq 0,\ C_{p,r}^1 \neq C_{p,r}^2\},$$
$$\mathcal{A}_{\max} = \{(p, r) \in \mathcal{A} : (p, r') \notin \mathcal{A} \text{ for all } r' > r\}.$$

If $(p, r) \notin \mathcal{A}$, then the (p, r)-th term in the product in (13) is the same for $j = 1, 2$. If $(p, r) \in \mathcal{A}$, then the (p, r)-th terms differ by a factor $(-1)^{\epsilon_{p,r}^k}$ given in Lemma 3.4. It follows that

$$\xi_k(G, q_1) = (-1)^{\Lambda} \xi_k(G, q_2) \quad \text{where } \Lambda = \sum_{(p,r)\in\mathcal{A}} \epsilon_{p,r}^k.$$

Case 1. If there is a prime p such that $(p, 1) \in \mathcal{A}_{\max}$, then choose such a prime p_0 and let $k = p_0$. We find

$$\sum_{r:(p_0,r)\in\mathcal{A}} \epsilon^k_{p_0,r} = \epsilon^k_{p_0,1} = 1(k+1) - \min\{1, v_{p_0}(k)\} = p_0 \equiv 1 \mod 2.$$

For all prime $(p, r) \in \mathcal{A}$ such that $p \neq p_0$, we have $\epsilon^k_{p,r} = r(p_0+1) \equiv 0 \mod 2$. It follows that $\Lambda \equiv 1 \mod 2$, so $\xi_k(G, q_1) \neq \xi_k(G, q_2)$.

Case 2. Otherwise, choose $(p_0, r_0) \in \mathcal{A}_{\max}$ such that $r_0 > 1$. Choose any $\gamma \geq 1$, and let

$$k = 2^\gamma p_0^{-1} \prod_{(p,r)\in\mathcal{A}_{\max}} p^r.$$

Note that k is an integer with $v_2(k) = \gamma$ and $v_{p_0}(k) = r_0 - 1$. One has

$$\epsilon^k_{p_0,r_0} = r_0(k+1) - \min\{r_0, v_{p_0}(k)\} \equiv r_0 - (r_0 - 1) = 1 \mod 2.$$

If $r < r_0$, then $r \leq v_{p_0}(k)$, so $\epsilon^k_{p_0,r} = r(k-1) - r \equiv 0 \mod 2$. Finally if $p \neq p_0$, then $(p, r) \in \mathcal{A}$ implies $r \leq v_p(k)$ by our choice of k, so $\epsilon^k_{p,r} = r(k+1) - r \equiv 0 \mod 2$. Again, $\Lambda \equiv 1 \mod 2$, so $\xi_k(G, q_1) \neq \xi_k(G, q_2)$. □

Lemma 5.2. *Let b and b' be two nondegenerate symmetric bilinear forms on a finite abelian 2-group G. Let q and q' be quadratic forms such that $\partial q = b$ and $\partial q' = b'$. Let k be a positive integer such that $v_2(k) = 0$ or $v_2(k) > \max\{2, v_2(\exp(G))\}$. Then $\xi_k(G, q) = \xi_k(G, q')$.*

Proof. By the structure theorem of finite abelian groups and by Theorem 2.1, we can decompose G and (G, q) as

$$G \simeq \bigoplus_{r=1}^{\infty} (\mathbb{Z}/2^r\mathbb{Z})^{N_r} \quad \text{and} \quad (G, q) \simeq (H_1, \mu_1) \perp \cdots \perp (H_m, \mu_m),$$

respectively, where each $H_i \simeq \mathbb{Z}/2^{r_i}\mathbb{Z}$ or $H_i \simeq (\mathbb{Z}/2^{r_i}\mathbb{Z})^2$ and μ_i is an irreducible nondegenerate quadratic form on H_i.

Suppose k is odd. By Lemmas 3.2(b) and 3.3, if $(H_i, \mu_i) \cong (\mathbb{Z}/2^{r_i}\mathbb{Z}, \alpha x^2/2^{r_i+1})$, then

$$\xi_k(H_i, \mu_i) = (-1)^{kr_i(\alpha^2-1)/8} \boldsymbol{e}(\alpha/8)^k (-1)^{r_i(k^2\alpha^2-1)/8} \boldsymbol{e}(-k\alpha/8).$$

Using (11), this simplifies to

$$\xi_k(H_i, \mu_i) = (-1)^{r_i(k^2-1)/8}.$$

By Lemma 3.2, if $(H_i, \mu_i) \cong ((\mathbb{Z}/2^{r_i}\mathbb{Z})^2, (\alpha x_1^2 + x_1x_2 + \alpha x_2^2)/2^{r_i})$ with $\alpha \in \{0, 1\}$, then

$$\xi_k(H_i, \mu_i) = (-1)^{\alpha^2 r_i k}(-1)^{(-k\alpha)^2 r_i} = (-1)^{\alpha r_i k + \alpha r_i k^2} = 1.$$

We summarize both cases with the equation

$$\xi_k(H_i,\mu_i) = (-1)^{\mathrm{rk}(H_i) r_i (k^2-1)/8}.$$

Summing over all i such that $r_i = r$ yields $\sum_i \mathrm{rk}(H_i) r_i = \sum_r r N_r$. So

$$\xi_k(G,q) = (-1)^{\sum_r r N_r (k^2-1)/8}.$$

The expression for $\xi_k(G,q)$ does not depend on q, so we get $\xi_k(G,q) = \xi_k(G,q')$ for k odd.

Now suppose that $k = 2^n\beta$ with β odd and $n > \max\{2, v_2(\exp(G))\}$. Then $\max\{r-n, 0\} = 0$ for all r such that $N_r > 0$. Since $n > v_2(\exp(G))$, the quadratic forms $2^{n-1}b(x,x)$ and $2^{n-1}b'(x,x)$ are identically equal to 0, so Lemma 3.6 implies that $\varsigma_n(b) = \varsigma_n(b') = 1$. From Lemma 3.8, we get

$$\xi_{2^n\beta}(G,q) = |G[2^n]|^{1/2} \varsigma_n(b)^{(2^n-1)\beta} = |G|^{1/2}.$$

Thus, $\xi_{2^n\beta}(G,q)$ does not depend on q and we get $\xi_{2^n\beta}(G,q) = \xi_{2^n\beta}(G,q')$. □

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. Write $\mathcal{C}_1 = \mathrm{TY}(G_1, b_1, \tau_1)$ and $\mathcal{C}_2 = \mathrm{TY}(G_2, b_2, \tau_2)$. Let $m_1 = m_{\mathcal{C}_1}$ and $m_2 = m_{\mathcal{C}_2}$. We have $\mathrm{pdim}(x) = 1$ for $x \in G_j$ and $\mathrm{pdim}(m_j) = \sqrt{|G_j|}$. So the hypothesis in the theorem yields

$$(\sqrt{|G_1|} - 1)\nu_k(m_1) = (\sqrt{|G_2|} - 1)\nu_k(m_2) \quad \text{for all } k \geq 1. \tag{14}$$

Lemma 4.1 implies that, if k is a multiple of $8|G_1||G_2|$, then $\nu_k(m_j) = \sqrt{|G_j|}$ for $j = 1, 2$. It follows that $(\sqrt{|G_1|} - 1)\sqrt{|G_1|} = (\sqrt{|G_2|} - 1)\sqrt{|G_2|}$ and hence $|G_1| = |G_2|$.

First consider the trivial case: $|G_1| = |G_2| = 1$. Then the bilinear forms b_1 and b_2 are trivial. So there are only two such TY-categories, and they are only distinguished by the value of $\tau \in \{\pm 1\}$. We know $\sum_{x \in G_j} \nu_k(x) = |G_j[k]|$ and $\mathrm{sign}(\tau_j) = \nu_2(m_{\mathcal{C}_j})$. (See Theorem 3.2 of [Shimizu 2011] and the remark following the proof of Theorem 3.4 of [Shimizu 2011]. Or else, see Lemma 4.1.) It follows that $1 + \mathrm{sign}(\tau_1) = \sum_{V \in \mathrm{Irr}\,\mathcal{C}_1} \nu_2(V) = \sum_{V \in \mathrm{Irr}\,\mathcal{C}_2} \nu_2(V) = 1 + \mathrm{sign}(\tau_2)$. So $\mathrm{sign}(\tau_1) = \mathrm{sign}(\tau_2)$, and the theorem holds in the trivial case.

We may now assume that $|G_1| = |G_2| > 1$. Equation (14) implies $\nu_k(m_1) = \nu_k(m_2)$ and hence $\sum_{x \in G_1} \nu_k(x) = \sum_{x \in G_2} \nu_k(x)$ for all $k \geq 1$. It follows that $|G_1[k]| = |G_2[k]|$ for each $k \geq 1$. This forces $G_1 \simeq G_2$, and so we may assume without loss of generality that $G_1 = G_2 = G$. By [Shimizu 2011], $\mathrm{sign}(\tau_j) = \nu_2(m_{\mathcal{C}_j})$, and so it follows that $\tau_1 = \tau_2$. Assume that b_1 and b_2 are nonisomorphic.

Write $G = G_e \oplus G_o$ where G_e is the 2-Sylow subgroup of G and $G_o = \bigoplus_{p \neq 2} G_{(p)}$ is the "odd part". Then $(G, b_j) = (G_o, b_j^o) \perp (G_e, b_j^e)$. Choose quadratic forms q_j^o and q_j^e such that $b_j^o = \partial q_j^o$ and $b_j^e = \partial q_j^e$. Then $q_j = q_j^o \perp q_j^e$ is a quadratic form such that $\partial q_j = b_j$. By Lemma 4.1, it is enough to show that $\xi_k(G, q_1) \neq \xi_k(G, q_2)$ for some k. Since ξ_k is multiplicative for $j \in \{1, 2\}$, we have

$$\xi_k(G, q_j) = \xi_k(G_o, q_j^o)\xi_k(G_e, q_j^e).$$

We split the argument into two cases.

Case 1 ($b_1^o \ncong b_2^o$). Then Lemma 5.1 implies that there is an integer $k > 1$ that is either odd or $v_2(k) > \max\{2, v_2(\exp(G_e))\}$ such that $\xi_k(G_o, q_1^o) \neq \xi_k(G_o, q_2^o)$ and Lemma 5.2 implies that $\xi_k(G_e, q_1^e) = \xi_k(G_e, q_2^e)$. So $\nu_{2k}(m_1) \neq \nu_{2k}(m_2)$ if $b_1^o \ncong b_2^o$.

Case 2 ($b_1^o \cong b_2^o$). In this case, we must have $b_1^e \ncong b_2^e$. From Theorem 3.5, there exists some $n \geq 1$ such that $\sigma_n(b_1^e) \neq \sigma_n(b_2^e)$, which implies $\varsigma_n(b_1^e) \neq \varsigma_n(b_2^e)$. Now Lemma 3.8 implies that

$$\xi_{2^n}(G_e, q_j^e) = (-1)^{\Gamma_{G_e,1,n}} |G_e[2^n]|^{1/2} \varsigma_n(b_j^e)^{2^n - 1}$$

where $\Gamma_{G_e,1,n}$ is an integer dependent on G_e and n but independent of q_j^e. It follows that $\xi_{2^n}(G_e, q_1^e) \neq \xi_{2^n}(G_e, q_2^e)$. On the other hand, since $(G_o, b_1^o) \cong (G_o, b_2^o)$, we have $\xi_{2^n}(G_o, q_1^o) = \xi_{2^n}(G_o, q_2^o)$. So $\nu_{2^{n+1}}(m_1) \neq \nu_{2^{n+1}}(m_2)$. □

6. Tambara–Yamagami categories associated to groups with an odd factor are determined by the state-sum invariants

Let G be a finite abelian group, χ be a nondegenerate symmetric bicharacter on G and τ be a square root of $|G|^{-1}$. Let $\mathcal{C} = \mathrm{TY}(G, \chi, \tau)$ denote the associated Tambara–Yamagami category. If M is a closed compact 3-manifold, we denote by $|M|_{\mathcal{C}}$ the state-sum invariant of M defined using the category $\mathcal{C}$, as in [Turaev and Vainerman 2012]. Let $L_{m,n}$ denote the lens spaces.

Lemma 6.1. *For all $k \geq 1$, one has $|L_{k,1}|_{\mathcal{C}} = (|G[k]| + |G|^{1/2}\nu_k(m_{\mathcal{C}}))/(2|G|)$.*

This lemma follows directly from Theorem 0.3 of [Turaev and Vainerman 2012] as well as Lemma 4.1. The former expresses $|L_{2k,1}|_{\mathcal{C}}$ in terms of a quantity $\zeta_k(\chi)$ that is essentially the right-hand side of the equation in Lemma 4.1.

Corollary 6.2. *For all $k \geq 1$, $|L_{k,1}|_{\mathcal{C}} = (\mathrm{pdim}(\mathcal{C}))^{-1} \sum_{V \in \mathrm{Irr}(\mathcal{C})} \nu_k(V)\,\mathrm{pdim}(V)$.*

The corollary follows from Theorem 3.2 of [Shimizu 2011], which implies $\sum_{x \in G} \nu_k(x) = |G[k]|$.

Theorem 6.3. *Let $\mathcal{C} = \mathrm{TY}(G, \chi, \tau)$ and $\mathcal{C}' = \mathrm{TY}(G', \chi', \tau')$ be any two* TY-*categories. Suppose $|G|$ is not a power of* 2. *If $|L_{k,1}|_{\mathcal{C}} = |L_{k,1}|_{\mathcal{C}'}$ for all $k \geq 1$, then $\mathcal{C} \simeq \mathcal{C}'$.*

Proof. Let G_e and G_e' be the 2-Sylow subgroups of G and G', respectively. Let G_o and G_o' be the sums of the p-Sylow subgroups for all odd p. From Theorem 0.1 of [Turaev and Vainerman 2012], we already know that $|G| = |G'|$ and that the p-Sylow subgroups of G and G' are isomorphic for all odd p. It follows that $|G_e| = |G'_e|$. We claim that $G_e \simeq G'_e$ as well. The claim implies $G \simeq G'$, and then Lemma 6.1 tells us $\nu_k(m_{\mathcal{C}}) = \nu_k(m_{\mathcal{C}'})$ for all k, which forces $\chi \simeq \chi'$ by Theorem 1.1. Thus, to complete the proof, we need to show $G_e \simeq G'_e$. For this, it suffices to show that $|G[2^n]| = |G'[2^n]|$ for all $n \geq 0$. Suppose this is false. Since $|G[2^0]| = |G'[2^0]| = 1$, we may pick the smallest $n \geq 0$ such that $|G[2^{n+1}]| > |G'[2^{n+1}]|$ (without loss of generality) and $|G[2^m]| = |G'[2^m]|$ for all $m \leq n$.

Let $a = |G_o| = |G'_o|$. Let $n \geq 0$. Then $G[2^n a] = G_o \oplus G[2^n]$. By Lemma 4.2, we can write $\nu_{2^{n+1}a}(m_{\mathcal{C}}) = |G[2^n a]|^{1/2}\psi_n$, where $\psi_n \in \mu_8 \cup \{0\}$. Define ψ'_n similarly for $\mathcal{C}'$. We have

$$\begin{aligned} 2|G||L_{2^{n+1}a,1}|_{\mathcal{C}} &= |G[2^{n+1}a]| + |G|^{1/2}\nu_{2^{n+1}a}(m_{\mathcal{C}}) \\ &= |G_o|(|G[2^{n+1}]| + |G_e|^{1/2}|G[2^n]|^{1/2}\psi_n). \end{aligned}$$

So $|L_{2^{n+1}a,1}|_{\mathcal{C}} = |L_{2^{n+1}a,1}|_{\mathcal{C}'}$ implies

$$|G[2^{n+1}]| + |G_e|^{1/2}|G[2^n]|^{1/2}\psi_n = |G'[2^{n+1}]| + |G'_e|^{1/2}|G'[2^n]|^{1/2}\psi'_n.$$

If $\psi_n = \psi'_n = 0$, then the above equation would imply $|G[2^{n+1}]| = |G'[2^{n+1}]|$. So $\psi_n \neq 0$ or $\psi'_n \neq 0$. Rearranging the above equation and remembering that $|G_e| = |G'_e|$, we get

$$|G[2^{n+1}]| - |G'[2^{n+1}]| = |G_e|^{1/2}|G[2^n]|^{1/2}(\psi'_n - \psi_n). \tag{15}$$

Each side of (15) belong to $\mathbb{Z}[e^{2\pi i/8}]$. Consider the absolute norm of each side. If $\psi \in \mu_8 \cup \{0\}$, one verifies that the absolute norm of $(\psi - 1)$ is a power of 2 or zero. For example, if ψ is a primitive 8-th root of unity, then $N_{\mathbb{Q}}^{\mathbb{Q}[\psi]}(\psi - 1) = \prod_{j=0}^{3}(\boldsymbol{e}((2j+1)/8) - 1) = 2$. If $\psi_n \neq 0$ or $\psi'_n \neq 0$, then writing $(\psi'_n - \psi_n) = \psi_n(\psi'_n/\psi_n - 1)$ or $(\psi'_n - \psi_n) = \psi'_n(1 - \psi_n/\psi'_n)$, respectively, we find that the norm of $(\psi'_n - \psi_n)$ is a power of 2 or zero. So the norm of the right-hand side of (15) is also a power of 2. However, note that the left-hand side is already an integer, so it must also be a power of 2. The only way this is possible is if $|G[2^{n+1}]| = 2|G'[2^{n+1}]|$. Write $\nu_{2^{n+1}}(m_{\mathcal{C}}) = |G[2^n]|^{1/2}\lambda_n$ and $\nu_{2^{n+1}}(m_{\mathcal{C}'}) = |G'[2^n]|^{1/2}\lambda'_n$ for some $\lambda_n, \lambda'_n \in \mu_8 \cup \{0\}$. Now the equality $|L_{2^{n+1},1}|_{\mathcal{C}} = |L_{2^{n+1},1}|_{\mathcal{C}'}$ yields

$$|G'[2^{n+1}]| = |G[2^{n+1}]| - |G'[2^{n+1}]| = |G|^{1/2}|G[2^n]|^{1/2}(\lambda'_n - \lambda_n).$$

Now the left-hand side is a power of 2, so the norm of the right-hand side must also be a power of 2. Since $N(\lambda'_n - \lambda_n)$ is a power of 2, it follows that $|G|$ is also a power of 2, which contradicts our assumption. It follows that $(G, \chi) \simeq (G', \chi')$. Now since $\nu_2(m_{\mathcal{C}}) = \operatorname{sgn}(\tau)$, the equality $|L_{2,1}|_{\mathcal{C}} = |L_{2,1}|_{\mathcal{C}'}$ implies $\tau = \tau'$. $\square$

Example. We exhibit two Tambara–Yamagami categories that have the same state-sum invariant for all lens spaces $L_{k,1}$. Recall that A_{2^n} denotes the metric group $((\mathbb{Z}/2^n\mathbb{Z}), x^2/2^{n+1})$. For $k \in \mathbb{Z}$, we shall denote the premetric group $((\mathbb{Z}/2^n\mathbb{Z}), kx^2/2^{n+1})$ by $(k \cdot A_{2^n})$. Let $(G_1, b_1) = (A_2)^4 \perp A_4$ and $(G_2, b_2) = (A_2)^2 \perp (A_4)^2$. Let $\mathcal{C}_1 = \mathrm{TY}(G_1, b_1, -\frac{1}{8})$ and $\mathcal{C}_2 = \mathrm{TY}(G_2, b_2, \frac{1}{8})$. Then we claim that $|L_{n,1}|_{\mathcal{C}_1} = |L_{n,1}|_{\mathcal{C}_2}$ for all positive integers n.

Proof of claim. Let q_i be a quadratic form such that $\partial q_i = b_i$ for $i \in \{1, 2\}$. We will break the proof into cases according to possible 2-valuations of n. The trivial case is that $|L_{n,1}|_{\mathcal{C}_1} = \frac{1}{128} = |L_{n,1}|_{\mathcal{C}_2}$ if n is odd. By Lemmas 6.1 and 4.1, to prove $|L_{2k,1}|_{\mathcal{C}_1} = |L_{2k,1}|_{\mathcal{C}_2}$, it is enough to show that

$$|G_1[2k]| + (-1)^k 8\xi_k(G, q_1) = |G_2[2k]| + 8\xi_k(G, q_2).$$

Since ξ_k is multiplicative,

$$\xi_k(G, q_1) = \xi_k(A_2)^4 \xi_k(A_4) \quad \text{and} \quad \xi_k(G, q_2) = \xi_k(A_2)^2 \xi_k(A_4)^2.$$

From Lemma 3.2, we have $\xi_k(A_{2^r}) = \Theta(A_{2^r})^k \Theta(-k \cdot A_{2^r}) = e(k/8)\Theta(-k \cdot A_{2^r})$. The values of $\Theta(-k \cdot A_{2^r})$ were computed in Lemma 3.3. This lets us compute the invariants. We shall consider three cases.

Case 1. Suppose k is odd. Then we have $\Theta(-k \cdot A_2) = (-1)^{(k^2-1)/8}\boldsymbol{e}(-k/8)$, so $\xi_k(A_2) = (-1)^{(k^2-1)/8}$. We have $\Theta(-k \cdot A_4) = (-1)^{2(k^2-1)/8}\boldsymbol{e}(-k/8) = \boldsymbol{e}(-k/8)$, so $\xi_k(A_4) = 1$. It follows that $\xi_k(G, q_1) = 1 = \xi_k(G, q_2)$. Since $|G_1[2k]| = 32$ and $|G_2[2k]| = 16$, we get $|L_{2k,1}|_{\mathcal{C}_1} = |L_{2k,1}|_{\mathcal{C}_2}$ in this case.

Case 2. Suppose $v_2(k) = 1$ or 2. Then $\Theta(-k \cdot A_2) = 0$ or $\Theta(-k \cdot A_4) = 0$, so $\xi_k(A_2) = 0$ or $\xi_k(A_4) = 0$. Since both (G_1, b_1) and (G_2, b_2) have components of type A_2 and A_4 and since ξ_k is multiplicative, it follows that $\xi_k(G, q_1) = \xi_k(G, q_2) = 0$. Since $|G_i[2k]| = 64$, we get $|L_{2k,1}|_{\mathcal{C}_1} = |L_{2k,1}|_{\mathcal{C}_2}$ in this case.

Case 3. Finally suppose $v_2(k) \geq 3$. Let $r = 1$ or $r = 2$. Then $\Theta(A_{2^r})^k = e(k/8) = 1$. The quadratic form $-k \cdot A_{2^r}$ is identically equal to 1, so $\xi_k(A_{2^r}) = \Theta(-k \cdot A_{2^r}) = 2^{r/2}$. It follows that $\xi_k(G, q_j) = |G|^{1/2} = 8$ for $j = 1, 2$. Since $|G_i[2k]| = 64$ and $(-1)^k = 1$, we get $|L_{2k,1}|_{\mathcal{C}_1} = |L_{2k,1}|_{\mathcal{C}_2}$ in this case too. □

Appendix: Diagonalization of bilinear and quadratic forms

In this appendix, we discuss the problem of decomposing quadratic and bilinear forms on finite abelian groups into irreducible components.

Notation. If R is an abelian group, we let $M_n(R)$ be the set of all $n \times n$ matrices with entries in R. If R is a commutative ring and S is an R-module, then S^n is a (left) $M_n(R)$-module and $M_n(S)$ is an $M_n(R)$-bimodule. The action of $M_n(R)$ on S^n is obtained by writing elements of S^n as column vectors and multiplying by the matrix on the left. The two actions of $M_n(R)$ on $M_n(S)$ are by left and right multiplication.

Recall from Section 2 that, if x is an element in a p-group of finite order, then we write $v_p(x) = -\log_p(\text{order}(x))$ and $v_p(0) = \infty$. The lemma below is elementary. We leave the proof as an easy exercise.

Lemma A.1. *Let p be a prime. Let G be an abelian p-group.*

(a) *Let $x \in G$ and $r \in \mathbb{Z}$. Then $rx = 0$ if and only if $v_p(r) + v_p(x) \geq 0$.*

(b) *If $x \in G$ and $r \in \mathbb{Z}$ such that $rx \neq 0$, then $v_p(r) + v_p(x) = v_p(rx)$.*

(c) *Let $x_1, x_2 \in G$. Then $v_p(x_1 + x_2) \geq \min\{v_p(x_1), v_p(x_2)\}$, and equality holds if $\langle x_1\rangle \cap \langle x_2\rangle = 0$ or $v_p(x_1) \neq v_p(x_2)$. (Here and later, $\langle x\rangle$ denotes the cyclic subgroup generated by x.)*

(d) *Let b be a symmetric bilinear form on a finite abelian p-group G. If $g \in G$, then $v_p(g) \leq v_p(b(g, h))$ for all $h \in G$. Further, if b is nondegenerate, then $v_p(g) = \min\{v_p(b(g, h)) : h \in G\}$.*

Decomposing symmetric bilinear forms into irreducible components is almost equivalent to diagonalizing matrices by row and column operations. We introduce these operations next.

Definitions. Let E_{ij} be the $n \times n$ matrix whose (i, j)-th entry is 1 and all other entries are 0. Let I_n denote the $n \times n$ identity matrix. Let R be a commutative ring. Let A be an $n\times n$ matrix with entries in some R-module M. The operations $\text{Flip}_{ij}(A)$, $\text{Add}_i^{r,j}(A)$, and $\text{Scale}_i^r(A)$ defined below are called *row-column operations* on A.

- Let $\text{Flip}_{ij}(A) = S^{\text{tr}}AS$ where $S = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$. This operation interchanges the i-th and j-th rows of A and then interchanges the i-th and j-th columns of A.
- Let $\text{Add}_i^{r,j}(A) = S^{\text{tr}}AS$, where $S = I_n + rE_{ji}$ for some $r \in R$ and $i \neq j$. This operation adds r times the j-th row of A to the i-th row of A and then adds r times the j-th column of A to the i-th column of A.
- Let $\text{Scale}_i^r(A) = S^{\text{tr}}AS$ where $S = I_n + (r - 1)E_{ii}$ for some $r \in R$. This operation multiplies the i-th row of A by r and then multiplies the i-th column by r.

Let (G, b) be a discriminant form and $(e_1, \dots, e_n) \in G^n$. For each $i \neq j$, the operation Flip_{ij} converts $\text{Gram}_b(e_1, \dots, e_n)$ to $\text{Gram}_b(f_1, \dots, f_n)$ where $f_j = e_i$, $f_i = e_j$, and $f_k = e_k$ for $k \notin \{i, j\}$. The operation $\text{Add}_i^{r,j}$ converts $\text{Gram}_b(e_1, \dots, e_n)$ to $\text{Gram}_b(f_1, \dots, f_n)$ where $f_i = e_i + re_j$ and $f_k = e_k$ for $k \neq i$. The operation Scale_i^r converts $\text{Gram}_b(e_1, \dots, e_n)$ to $\text{Gram}_b(f_1, \dots, f_n)$ where $f_i = re_i$ and $f_k = e_k$ for $k \neq i$. We shall say that a row-column operation on $\text{Gram}_b(e_1, \dots, e_n)$ is *valid* if $G = \bigoplus_k \langle e_k \rangle$ implies $G = \bigoplus_k \langle f_k \rangle$. Clearly, Flip_{ij} is always valid. The operation Scale_i^r is valid if r is relatively prime to the exponent of G. Lemma A.2 lets us decide when $\mathrm{Add}_j^{r;i}$ is valid.

Lemma A.2. *Let G be a finite abelian group and $e_1, \dots, e_n \in G$ such that $G = \bigoplus_k \langle e_k \rangle$. Let $f_1, \dots, f_n \in G$ such that $\mathrm{ord}(f_k) = \mathrm{ord}(e_k)$ for all k and $f_1, \dots, f_n$ generate G. Then there exists $\phi \in \mathrm{Aut}(G)$ such that $\phi(e_k) = f_k$. In particular, $G = \bigoplus_k \langle f_k \rangle$.*

Proof. Let $n_k = \mathrm{ord}(e_k) = \mathrm{ord}(f_k)$. Since $\langle e_k \rangle$ is a cyclic group of order n_k and f_k is an element of order n_k in G, there exists a homomorphism $\phi_k : \langle e_k \rangle \to G$ given by $\phi_k(e_k) = f_k$. By the universal property of the direct sum, there exists a homomorphism $\phi : G \to G$ such that $\phi(e_k) = f_k$ for all k. Since the f_k generate G, the map ϕ is onto. Since G is a finite group, ϕ must be injective as well. □

Let $A \in M_n(\mathbb{Q}_{(p)}/\mathbb{Z})$. The proofs of Lemmas A.3 and A.4 are based on the algorithm to reduce A to a diagonal matrix (or a block-diagonal matrix with blocks of size at most 2 when $p = 2$) by conjugation or equivalently using the elementary row-column operations introduced above. This paves the way to proving Theorem 2.1 of [Wall 1963]. Let $\mathrm{diag}(a_1, \dots, a_n)$ denote the diagonal $n \times n$ matrix with diagonal entries $a_1, \dots, a_n$.

Lemma A.3. *Let p be an odd prime. Let u_p be a quadratic nonresidue modulo p. Let $A \neq 0$ be a symmetric matrix in $M_n(\mathbb{Q}_{(p)}/\mathbb{Z})$. Let r_1 be the smallest number such that $p^{r_1} A = 0$.*

(a) *Then there exists a matrix $S \in \mathrm{GL}_n(\mathbb{Z})$ such that $S \bmod p \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ and*

$$S^{\mathrm{tr}} A S = \mathrm{diag}(p^{-r_1}\epsilon_1, \dots, p^{-r_n}\epsilon_n) \quad \text{with } r_1 \geq r_2 \geq \cdots \geq r_n \geq 0,\ \epsilon_j \in \{1, u_p, 0\}, \text{ and } \epsilon_1 \neq 0.$$

(b) *Let (G, b) be a nondegenerate discriminant form where G is a p-group. Let $G = \bigoplus_{j=1}^n \langle e_j \rangle$. Then there exists $f_1, \dots, f_n \in G$ such that $G = \bigoplus_{j=1}^n \langle f_j \rangle$ and $\mathrm{Gram}_b(f_1, \dots, f_n) = \mathrm{diag}(p^{-r_1}\epsilon_1, \dots, p^{-r_n}\epsilon_n)$ with $r_1 \geq r_2 \geq \cdots \geq r_n > 0$ and $\epsilon_j \in \{1, u_p\}$.*

Proof. (a) One proceeds by finding a pivot with the smallest p-valuation and then using this pivot to sweep out the rows and columns. Let $A = ((a_{ij})) \in M_n(\mathbb{Q}_{(p)}/\mathbb{Z})$ be a symmetric nonzero matrix. Let $r_1 > 0$ be the smallest integer such that $p^{r_1} A = 0$. By induction on n, it suffices to show that there is a sequence of row-column operations that converts A to a matrix of the form $\begin{pmatrix} d_1 & 0 \\ 0 & A' \end{pmatrix}$ where $d_1 = p^{-r_1}$ or $d_1 = u_p p^{-r_1}$ and $A' \in M_{n-1}(\mathbb{Q}_{(p)}/\mathbb{Z})$ is a symmetric matrix such that $p^{r_1} A' = 0$.

Claim (finding a pivot). *After changing A by row-column operations, we may assume that $a_{11} = p^{-r_1}$ or $a_{11} = u_p p^{-r_1}$.*

Proof of claim. If there is a diagonal entry a_{ii} such that $v_p(a_{ii}) = -r_1$, then apply Flip_{1i} to A to get $v_p(a_{11}) = -r_1$. Otherwise, there exists $i \neq j$ such that $v_p(a_{ij}) = -r_1$ and $v_p(a_{ii}) > -r_1$ and $v_p(a_{jj}) > -r_1$. In this case, apply $\mathrm{Add}_i^{1,j}$ to A. This changes the (i,i)-th entry of the matrix from a_{ii} to $(a_{ii} + 2a_{ij} + a_{jj})$, whose p-valuation is $-r_1$.[1] Now we apply Flip_{1i}. Either way, we get $v_p(a_{11}) = -r_1$. Using the operation Scale_i^r, we can change a_{11} to $r^2 a_{11}$. By choosing r appropriately, we can make $a_{11} = p^{-r_1}$ or $a_{11} = u_p p^{-r_1}$. This proves the claim.

Sweeping out. Now $a_{11} = \epsilon_1 p^{-r_1}$ with $\epsilon_1 = 1$ or u_p. Since ϵ_1 is relatively prime to p, we can pick $\epsilon' \in \mathbb{Z}$ such that $\epsilon'\epsilon_1 \equiv 1 \bmod p^{r_1}$. We can represent a_{1i} in the form $\beta_i p^{-r_1}$ with $\beta_i \in \mathbb{Z}$. We add $(-\beta_i\epsilon')$ times the first row to the i-th row and then add $(-\beta_i\epsilon')$ times the first column to the i-th column to make $a_{1i} = 0$ and $a_{i1} = 0$. Performing this operation for $i = 2, 3, \dots, n$ converts A to a matrix of the form $\left(\begin{smallmatrix} \epsilon_1 p^{-r_1} & 0 \\ 0 & A' \end{smallmatrix}\right)$. Finally note that the entries of A' are $\mathbb{Z}$-linear combinations of entries of A, so $p^{r_1}A = 0$ implies $p^{r_1}A' = 0$. The row-column operations above correspond to conjugating A by certain matrices that are always invertible modulo p. Now part (a) follows by induction.

(b) Assume the setup of part (b). Let $A = \mathrm{Gram}_b(e_1, \dots, e_n)$. Part (a) shows that the matrix A can be diagonalized by a sequence of row-column operations. Performing a row-column operation on $\mathrm{Gram}_b(e_1, \dots, e_n)$ converts it to $\mathrm{Gram}_b(f_1, \dots, f_n)$ where the f_j are given in the definition preceding Lemma A.2. We need to verify that all the row-column operation used in the proof of part (a) are valid (see the definition preceding Lemma A.2). While finding the pivot, we may perform $\mathrm{Add}_i^{1,j}$ to a matrix $\mathrm{Gram}_b(e_1, \dots, e_n)$ if a nondiagonal entry of the matrix, say a_{ij}, has the highest power of p in the denominator. Since $a_{ij} = a_{ji}$, Lemma A.1(d) implies that $\mathrm{order}(e_i) = \mathrm{order}(e_j)$. Since $\langle e_i\rangle \cap \langle e_j\rangle = 0$, Lemma A.1 implies that $\mathrm{ord}(e_i + e_j) = \mathrm{ord}(e_i)$. Now Lemma A.2 implies that $\mathrm{Add}_j^{1,j}$ is valid.

While sweeping out, we perform the row-column operation $\mathrm{Add}_i^{-\beta_i\epsilon',1}$ where $a_{1i} = \beta_i p^{-r_1}$. This operation changes $\mathrm{Gram}_b(e_1, \dots, e_n)$ to $\mathrm{Gram}_b(f_1, \dots, f_n)$ where $f_i = e_i - \beta_i\epsilon' e_1$ and $f_k = e_k$ for $k \neq i$. Assume $G = \bigoplus_k \langle e_k\rangle$. Since the discriminant form on G is nondegenerate, we have $v_p(e_1) = -r_1$ and hence $v_p(-\beta_i\epsilon' e_1) = v_p(\beta_i) - r_1$. Also, $v_p(e_i) \le v_p(a_{1i}) = v_p(\beta_i) - r_1$. Since $\langle e_i\rangle \cap \langle -\beta_i\epsilon' e_1\rangle = \{0\}$, we have $v_p(f_i) = \min\{v_p(e_i), v_p(-\beta_i\epsilon' e_1)\} = v_p(e_i)$. Lemma A.2 implies that the row-column operations performed while sweeping out are valid.

It follows that there exist $f_1, \dots, f_n \in G$ such that $G = \bigoplus\langle f_j\rangle$ and that $\mathrm{Gram}_b(f_1, \dots, f_n) = \mathrm{diag}(p^{-r_1}\epsilon_1, \dots, p^{-r_n}\epsilon_n)$ with $r_1 \ge r_2 \ge \cdots \ge r_n \ge 0$ and $\epsilon_j \in \{1, u_p, 0\}$. Since (G, b) is nondegenerate, it follows that we must have $\epsilon_j \neq 0$ and $\mathrm{order}(f_j) = p^{r_j}$ for all j. □

[1] This is the step in the argument that fails for $p = 2$.

The next lemma handles the case of the prime $p = 2$. This proof is similar to the proof of Lemma A.3 but somewhat more complicated. We only elaborate on the necessary modifications.

Lemma A.4. (a) *Let $A \neq 0$ be a symmetric matrix in $M_n(\mathbb{Q}_{(2)}/\mathbb{Z})$. Let m be the smallest number such that $2^m A = 0$. Then there exists a matrix $S \in \mathrm{GL}_n(\mathbb{Z})$ such that $(S \bmod 2) \in \mathrm{GL}_n(\mathbb{Z}/2\mathbb{Z})$ and $S^{\mathrm{tr}} A S$ is block-diagonal with blocks of size* 1 *or* 2. *Each block is of the form*

$$(2^{-r}\delta) \quad or \quad 2^{-r}\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \tag{16}$$

where r is some nonnegative integer, a, b, and c are integers with b odd, and $\delta \in \{0, \pm 1, \pm 5\}$. The largest r that occurs is equal to m.

(b) *Let (G, b) be a nondegenerate discriminant form where G is a 2-group. Let $G = \bigoplus_{j=1}^{n} \langle e_j \rangle$. Then there exists $f_1, \dots, f_n \in G$ such that $G = \bigoplus_{j=1}^{n} \langle f_j \rangle$ and $\mathrm{Gram}_b(f_1, \dots, f_n)$ is a block-diagonal matrix with blocks of size* 1 *or* 2. *Each block is of the form given in* (16) *where r is some positive integer, a, b, and c are integers with b odd, and $\delta \in \{\pm 1, \pm 5\}$.*

Proof. (a) As above, we try to get a diagonal entry of A to have minimum 2-valuation. If this succeeds, then we can proceed with the sweep out as before and split off a 1×1 block from A. This procedure fails only in the situation when there exists $i \neq j$ such that $\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix} = 2^{-m}\begin{pmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{pmatrix}$ where $\alpha, \beta, \gamma \in \mathbb{Z}$, β is odd, and all the diagonal entries of A have 2-valuation strictly larger than $-m$. In this case, we can use row-column flips to move this 2×2 submatrix to the upper-left corner of A so that $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = 2^{-m}\begin{pmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{pmatrix}$ and then use this 2×2 block to sweep out the first two rows and first two columns simultaneously.

This is how it is done. Suppose the first two entries of the i-th row are $2^{-m}(u, v)$ for $u, v \in \mathbb{Z}$ where $i > 2$. We want to find r_1 and r_2 such that

$$(r_1, r_2) 2^{-m}\begin{pmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{pmatrix} = 2^{-m}(u, v) \bmod \mathbb{Z}.$$

This system can always be solved since the determinant $(4\alpha\gamma - \beta^2)$ of the coefficient matrix is odd. Solving the equation yields

$$(r_1, r_2) = d(2\gamma u - \beta v, 2\alpha v - \beta u)$$

where d is an inverse of $(4\alpha\gamma - \beta^2)$ modulo 2^m. Now we add to the i-th row $-r_1$ times the first row and $-r_2$ times the second row and then perform the corresponding column operations to the i-th column. Verify that after these operations the first two entries of the i-th row and i-th column become zero. Part (a) follows.

(b) Let $A = \mathrm{Gram}_b(e_1, \dots, e_n)$. The sweep-out operation above corresponds to replacing $\mathrm{Gram}_b(e_1, \dots, e_n)$ by $\mathrm{Gram}_b(f_1, \dots, f_n)$ where $f_i = e_i + r_1 e_1 + r_2 e_2$ and $f_j = e_j$ for all $j \neq i$. The extra work needed in part (b) is to check that this operation is valid. Note that, since 2^m is the maximum denominator in A, $\mathrm{order}(e_1) = \mathrm{order}(e_2) = 2^m$. Suppose $\mathrm{order}(e_i) = 2^k$. Then u and v must be divisible by 2^{m-k} because the entries of the i-th row can have denominator at most 2^k. From the formula for r_1 and r_2, we see that 2^{m-k} divides r_1 and r_2. It follows that $2^k f_i = 0$. On the other hand, since $\langle e_i \rangle \cap \langle e_1, e_2 \rangle = 0$, we have $\mathrm{order}(f_i) \geq 2^k$. So $\mathrm{order}(f_i) = \mathrm{order}(e_i)$ and Lemma A.2 implies the sweep-out operations using 2×2 blocks described above are valid. □

For p-groups with p odd, Wall's Theorem 2.1(a) follows from Lemma A.3. For $p = 2$, we need Lemma A.4 and we also need Lemmas 2.2 and A.7, which describe the irreducible nondegenerate quadratic and bilinear forms on $(\mathbb{Z}/2^r\mathbb{Z})^2$. Proving Lemmas 2.2 and A.7 depends on solving a system of congruence equations modulo 2^n for all n. This can be done by a standard application of Hensel's lemma, which we now state in the necessary form.

Lemma A.5 (Hensel's lemma). *Let p be a prime. Let $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ and $f = (f_1, \dots, f_m)$. Let $Df = ((\partial f_i/\partial x_j))$ be the Jacobian of f. Let $t_1 \in \mathbb{Z}^n$ such that $f(t_1) \equiv 0 \bmod p$ and the $m \times n$ matrix $(Df(t_1) \bmod p)$ has rank m over $\mathbb{F}_p$. Then, for all $k \geq 1$, there exists $t_k \in \mathbb{Z}^n$ such that $t_{k+1} \equiv t_k \bmod p^k$ and $f(t_k) \equiv 0 \bmod p^k$.*

The proof is omitted.

Lemma A.6. (a) *Let $s = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$ be a 2×2 matrix of indeterminates. Let*

$$(A(s), B(s), C(s)) \\ = (s_{11}^2 + s_{11}s_{12} + s_{12}^2, 2s_{11}s_{21} + s_{11}s_{22} + s_{21}s_{12} + 2s_{12}s_{22}, s_{21}^2 + s_{21}s_{22} + s_{22}^2).$$

Let A, B, and C be odd integers. Let $n \geq 1$. Then the equation

$$(A(s), B(s), C(s)) \equiv (A, B, C) \bmod 2^n \tag{17}$$

has a solution $S \in M_2(\mathbb{Z})$ such that $S \equiv I \bmod 2$ (here I denotes the 2×2 identity matrix).

(b) *Let $s = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$ be a 2×2 matrix of indeterminates. Let*

$$(A(s), B(s), C(s)) = (s_{11}s_{12}, s_{11}s_{22} + s_{21}s_{12}, s_{21}s_{22}).$$

Let A, B, and C be integers such that B is odd and AC is even. Let $n \geq 1$. Then the equation

$$(A(s), B(s), C(s)) \equiv (A, B, C) \bmod 2^n \tag{18}$$

has a solution $S \in M_2(\mathbb{Z})$ such that $S \equiv \begin{pmatrix} A & 1 \\ 1 & C \end{pmatrix} \bmod 2$.

Proof. (a) Apply Hensel's lemma to $f = (f_1, f_2, f_3)$ for $f_1(s) = s_{11}^2 + s_{11}s_{12} + s_{12}^2 - A$, $f_2(s) = 2s_{11}s_{21} + s_{11}s_{22} + s_{21}s_{12} + 2s_{12}s_{22} - B$, and $f_3(s) = s_{21}^2 + s_{21}s_{22} + s_{22}^2 - C$. Since A, B, and C are odd, $s = I$ is a solution to $f(s) \equiv 0 \bmod 2$. One computes

$$Df = \begin{pmatrix} 2s_{11}+s_{12} & 0 & s_{11}+2s_{12} & 0 \\ 2s_{21}+s_{22} & 2s_{11}+s_{12} & s_{21}+2s_{22} & s_{11}+2s_{12} \\ 0 & 2s_{21}+s_{22} & 0 & s_{21}+2s_{22} \end{pmatrix},$$

$$\text{so} \quad Df(I) \equiv \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \bmod 2,$$

which has rank 3. For part (b), let $f_1(s) = s_{11}s_{12} - A$, $f_2(s) = s_{11}s_{22} + s_{21}s_{12} - B$, and $f_3(s) = s_{21}s_{22} - C$. Since B is odd and AC is even, $s_* = \left(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\right)$ satisfies $f(s_*) \equiv 0 \bmod 2$. One computes

$$Df = \begin{pmatrix} s_{12} & 0 & s_{11} & 0 \\ s_{22} & s_{12} & s_{21} & s_{11} \\ 0 & s_{22} & 0 & s_{21} \end{pmatrix}, \quad \text{so} \quad Df(s_*) \equiv \begin{pmatrix} 1 & 0 & A & 0 \\ C & 1 & 1 & A \\ 0 & C & 0 & 1 \end{pmatrix} \bmod 2.$$

Since A or C is even, either the second or the third column of the above matrix is equal to $(0, 1, 0)^{\mathrm{tr}}$. So the matrix $(Df(s_*) \bmod 2)$ has rank 3. ☐

Proof of Lemma 2.2. (a) Note that $2q(x) = \partial q(x, x) \in 2^{-r}\mathbb{Z}/\mathbb{Z}$. So $q(x)$ takes values in $2^{-r-1}\mathbb{Z}/\mathbb{Z}$, and

$$q(x_1, x_2) = 2^{-r-1}(\alpha x_1^2 + 2Bx_1x_2 + \gamma x_2^2)$$

where $q(1, 0) = 2^{-r-1}\alpha$, $q(0, 1) = 2^{-r-1}\gamma$, and $\partial q((1, 0), (0, 1)) = 2^{-r}B$. Suppose α is odd. Let $\bar{\alpha}$ be an inverse of α modulo 2^{r+1}. Then we can complete squares to write

$$q(x_1, x_2) = 2^{-r-1}(\alpha(x_1 + B\bar{\alpha}x_2)^2 + (\gamma - B^2\bar{\alpha})x_2^2).$$

This contradicts the irreducibility of q, and thus, α has to be even. For the same reason, γ has to be even. So we can write

$$q(x_1, x_2) = 2^{-r}(Ax_1^2 + Bx_1x_2 + Cx_2^2).$$

If A, B, and C are all even, then ∂q takes values in $2^{-r+1}\mathbb{Z}/\mathbb{Z}$ and hence cannot be nondegenerate. If B is even, then A or C must be odd, and we can once again complete squares (as above) and decompose (G, q) into an orthogonal direct sum of two metric groups. So B must be odd.

First, suppose AC is odd. Let $F(x_1, x_2) = x_1^2 + x_1x_2 + x_2^2$. Let $s = \left(\begin{smallmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{smallmatrix}\right)$. Note that

$$F((x_1, x_2)s) = A(s)x_1^2 + B(s)x_1x_2 + C(s)x_2^2$$

where $(A(s), B(s), C(s))$ are the polynomials given in Lemma A.6(a). We want to show $q(x_1, x_2) \simeq 2^{-r} F(x_1, x_2)$. This is equivalent to finding a matrix $s \in M_2(\mathbb{Z})$ with odd determinant such that

$$F((x_1, x_2)s) \equiv (Ax_1^2 + Bx_1x_2 + Cx_2^2) \bmod 2^r$$

or equivalently $(A(s), B(s), C(s)) \equiv (A, B, C) \bmod 2^r$. The proof follows from Lemma A.6(a) if AC is odd. If AC is even, then the proof is identical, using $F(x_1, x_2) = x_1x_2$ and using part (b) of Lemma A.6 instead of part (a). □

Lemma A.7. (a) *Let A, B, and C be odd integers. Let $r \geq 1$. Then there exists a matrix $S \in M_2(\mathbb{Z})$ such that $S\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)S^{\mathrm{tr}} \equiv \left(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right) \bmod 2^r$ and $S \equiv I \bmod 2$.*

(b) *Let A, B, and C be integers such that AC is even and B is odd. Let $r \geq 1$. Then there exists a matrix $S \in M_2(\mathbb{Z})$ such that $S\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)S^{\mathrm{tr}} \equiv \left(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right) \bmod 2^r$ and $S \equiv \left(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\right) \bmod 2$.*

Proof. (a) The congruences in part (a) translate into $A(s) \equiv A \bmod 2^{r-1}$, $B(s) \equiv B \bmod 2^r$, and $C(s) = C \bmod 2^{r-1}$ where $A(s)$, $B(s)$, and $C(s)$ are as in Lemma A.6(a). Part (a) follows from Lemma A.6. Similarly part (b) follows from part (b) of Lemma A.6. □

Proof of Theorem 2.1. (a) Let (G, b) be a nondegenerate discriminant form. It suffices to decompose (G, b) into irreducibles when G is a p-group for some prime p. First suppose p is odd. From Lemma A.3, it follows that there exist $f_1, \ldots, f_n \in G$ such that $G = \bigoplus \langle f_j \rangle$ and $\mathrm{Gram}_b(f_1, \ldots, f_n) = \mathrm{diag}(p^{-r_1}\epsilon_1, \ldots, p^{-r_n}\epsilon_n)$ with $r_1 \geq r_2 \geq \cdots \geq r_n \geq 0$ and $\epsilon_j \in \{1, u_p\}$. Since (G, b) it nondegenerate, it follows that we must have $\mathrm{order}(f_j) = p^{r_j}$ for all j. Thus, (G, b) is an orthogonal direct sum of the rank-1 discriminant forms $(\langle f_j \rangle, b|_{\langle f_j \rangle})$ and each of these are of type A or B. This completes the argument for odd p.

Now we consider the case $p = 2$. From Lemma A.4, it follows that there exist $f_1, \ldots, f_n \in G$ such that $G = \bigoplus \langle f_j \rangle$ and $\mathrm{Gram}_b(f_1, \ldots, f_n)$ is block-diagonal with blocks of size 1 or 2 as given in Lemma A.4. Accordingly, (G, b) is an orthogonal direct sum of rank-1 or -2 discriminant forms spanned by one or two of the f_j. The rank-1 forms among these are clearly of type A, B, C, or D. The Gram matrix of a rank-2 piece has the form $2^{-r}\left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix}\right)$. Lemma A.7 shows that such a rank-2 piece is either of type E or F.

(b) Let (G, q) be a metric group. By part (a), $(G, \partial q)$ is an orthogonal direct sum of irreducible forms (G_j, b_j). Each G_j is a homogeneous p-group of rank 1 or 2. Further, G_j can have rank 2 only if $p = 2$. It follows that (G, q) is also an orthogonal direct sum of (G_j, q_j) where $q_j = q|_{G_j}$. The rank-1 forms are clearly of type A, B, C, or D. The rank-2 forms either decompose into two rank-1 forms or they are irreducible as metric groups. In the latter case, Lemma 2.2 shows that (G_j, q_j) is of type E or F. □

Acknowledgments

This work would not be possible without the guidance of Siu-Hung Ng during the inception of the project. We are grateful to him for suggesting the problem for this project. We would also like to thank him for his encouragement, for many useful conversations, and for pointing out many references. We would like to thank both of our referees for their thoughtful reviews. The referee's suggested revision of an earlier draft led to a simplification of our previous proof and a significant reduction in preparatory lemmas needed.

References

[Bantay 1997] P. Bantay, "The Frobenius–Schur indicator in conformal field theory", *Phys. Lett. B* **394**:1–2 (1997), 87–88. MR 98c:81195 Zbl 0925.81331

[Brown 1972] E. H. Brown, Jr., "Generalizations of the Kervaire invariant", *Ann. of Math.* (2) **95**:2 (1972), 368–383. MR 45 #2719 Zbl 0241.57014

[Conway and Sloane 1999] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd ed., Grundlehren math. Wiss. **290**, Springer, New York, 1999. MR 2000b:11077 Zbl 0915.52003

[Etingof 2002] P. Etingof, "On Vafa's theorem for tensor categories", *Math. Res. Lett.* **9**:5–6 (2002), 651–657. MR 2003i:18009 Zbl 1035.18004

[Etingof et al. 2005] P. Etingof, D. Nikshych, and V. Ostrik, "On fusion categories", *Ann. of Math.* (2) **162**:2 (2005), 581–642. MR 2006m:16051 Zbl 1125.16025

[Etingof et al. 2010] P. Etingof, D. Nikshych, and V. Ostrik, "Fusion categories and homotopy theory", *Quantum Topol.* **1**:3 (2010), 209–273. MR 2011h:18007 Zbl 1214.18007

[Fuchs and Schweigert 2003] J. Fuchs and C. Schweigert, "Category theory for conformal boundary conditions", pp. 25–70 in *Vertex operator algebras in mathematics and physics* (Toronto, 2000), edited by S. Berman et al., Fields Inst. Commun. **39**, Amer. Math. Soc., Providence, RI, 2003. MR 2005b:17056 Zbl 1084.17012

[Fuchs et al. 1999] J. Fuchs, A. C. Ganchev, K. Szlachányi, and P. Vecsernyés, "S_4 symmetry of $6j$ symbols and Frobenius–Schur indicators in rigid monoidal C^* categories", *J. Math. Phys.* **40**:1 (1999), 408–426. MR 99k:81111 Zbl 0986.81044

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Coll. Pub. **53**, Amer. Math. Soc., Providence, RI, 2004. MR 2005h:11005 Zbl 1059.11001

[Kashina et al. 2006] Y. Kashina, Y. Sommerhäuser, and Y. Zhu, *On higher Frobenius–Schur indicators*, Mem. Amer. Math. Soc. **181**:855, 2006. MR 2007k:16071 Zbl 1163.16029

[Kashina et al. 2012] Y. Kashina, S. Montgomery, and S.-H. Ng, "On the trace of the antipode and higher indicators", *Israel J. Math.* **188** (2012), 57–89. MR 2897723 Zbl 1260.16027

[Kawauchi and Kojima 1980] A. Kawauchi and S. Kojima, "Algebraic classification of linking pairings on 3-manifolds", *Math. Ann.* **253**:1 (1980), 29–42. MR 82b:57007 Zbl 0427.57001

[Linchenko and Montgomery 2000] V. Linchenko and S. Montgomery, "A Frobenius–Schur theorem for Hopf algebras", *Algebr. Represent. Theory* **3**:4 (2000), 347–355. MR 2001k:16073 Zbl 0971.16018

[Mason and Ng 2005] G. Mason and S.-H. Ng, "Central invariants and Frobenius–Schur indicators for semisimple quasi-Hopf algebras", *Adv. Math.* **190**:1 (2005), 161–195. MR 2005h:16066 Zbl 1100.16033

[Miranda 1984] R. Miranda, "Nondegenerate symmetric bilinear forms on finite abelian 2-groups", *Trans. Amer. Math. Soc.* **284**:2 (1984), 535–542. MR 85m:20075 Zbl 0512.10014

[Ng and Schauenburg 2007a] S.-H. Ng and P. Schauenburg, "Frobenius–Schur indicators and exponents of spherical categories", *Adv. Math.* **211**:1 (2007), 34–71. MR 2008b:16067 Zbl 1138.16017

[Ng and Schauenburg 2007b] S.-H. Ng and P. Schauenburg, "Higher Frobenius–Schur indicators for pivotal categories", pp. 63–90 in *Hopf algebras and generalizations* (Evanston, IL, 2004), edited by L. H. Kauffman et al., Contemp. Math. **441**, Amer. Math. Soc., Providence, RI, 2007. MR 2008m:18015 Zbl 1153.18008

[Ng and Schauenburg 2008] S.-H. Ng and P. Schauenburg, "Central invariants and higher indicators for semisimple quasi-Hopf algebras", *Trans. Amer. Math. Soc.* **360**:4 (2008), 1839–1860. MR 2009d:16065 Zbl 1141.16028

[Ng and Schauenburg 2010] S.-H. Ng and P. Schauenburg, "Congruence subgroups and generalized Frobenius–Schur indicators", *Comm. Math. Phys.* **300**:1 (2010), 1–46. MR 2012g:81193 Zbl 1206.18007

[Nikulin 1979] V. V. Nikulin, "Integral symmetric bilinear forms and some of their applications", *Izv. Akad. Nauk SSSR Ser. Mat.* **43**:1 (1979), 111–177. In Russian; translated in *Math. USSR-Izv.* **14**:1 (1980), 103–167. MR 80j:10031 Zbl 0408.10011

[Shimizu 2011] K. Shimizu, "Frobenius–Schur indicators in Tambara–Yamagami categories", *J. Algebra* **332** (2011), 543–564. MR 2012b:18014 Zbl 1236.18012

[Tambara and Yamagami 1998] D. Tambara and S. Yamagami, "Tensor categories with fusion rules of self-duality for finite abelian groups", *J. Algebra* **209**:2 (1998), 692–707. MR 2000b:18013 Zbl 0923.46052

[Turaev and Vainerman 2012] V. Turaev and L. Vainerman, "The Tambara–Yamagami categories and 3-manifold invariants", *Enseign. Math.* (2) **58**:1–2 (2012), 131–146. MR 2985013 Zbl 06187660

[Turaev and Virelizier 2013] V. Turaev and A. Virelizier, "On two approaches to 3-dimensional TQFTs", preprint, 2013. arXiv 1006.3501v5

[Wall 1963] C. T. C. Wall, "Quadratic forms on finite groups, and related topics", *Topology* **2**:4 (1963), 281–298. MR 28 #133 Zbl 0215.39903

Communicated by Susan Montgomery
Received 2014-07-24 Revised 2015-06-18 Accepted 2015-07-25

tathagat@iastate.edu *Department of Mathematics, Iowa State University, Ames, IA 50011, United States*

johnsor@grace.edu *Department of Mathematics, Grace College, Winona Lake, IN 46590, United States*

ALGEBRA AND NUMBER THEORY 9:8 (2015)
dx.doi.org/10.2140/ant.2015.9.1825

The number of nonzero coefficients of modular forms (mod p)

Joël Bellaïche and Kannan Soundararajan

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a modular form modulo a prime p, and let $\pi(f, x)$ be the number of nonzero coefficients a_n for $n < x$. We give an asymptotic formula for $\pi(f, x)$; namely, if f is not constant, then

$$\pi(f,x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log\log x)^{h(f)},$$

where $\alpha(f)$ is a rational number such that $0 < \alpha(f) \leq 3/4$, $h(f)$ is a nonnegative integer and $c(f)$ is a positive real number. We also discuss the equidistribution of the nonzero values of the coefficients a_n.

1. Introduction

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a holomorphic modular form of integral weight $k \geq 0$ and some level $\Gamma_1(N)$ such that the coefficients a_n are integers. Let p be a prime number. Serre [1976] has shown that the sequence $a_n \pmod p$ is *lacunary*. That is, the natural density of the set of integers n such that $p \nmid a_n$ is 0. More precisely, Serre gave the asymptotic upper bound

$$|\{n < x,\ a_n \not\equiv 0 \pmod p\}| \ll \frac{x}{(\log x)^{\beta}}, \tag{1}$$

where β is a positive constant depending on f. Later, Ahlgren [1999, Lemma 2.1] established the following asymptotic lower bound: assume that p is odd and that there exists an integer $n \geq 2$ divisible by at least one prime ℓ not dividing Np such that $p \nmid a_n$. Then

$$|\{n < x,\ a_n \not\equiv 0 \pmod p\}| \gg \frac{x}{(\log x)}. \tag{2}$$

Joël Bellaïche was supported by NSF grant DMS 1101615. Kannan Soundararajan was partially supported by NSF grant DMS 1001068 and a Simons Investigator grant from the Simons Foundation.
MSC2010: primary 11F33; secondary 11F25, 11N25, 11N37.
Keywords: modular forms modulo p, Hecke operators, Selberg–Delange's method.

Under the same hypothesis, this lower bound was recently improved by Chen [2012]: for every $K \geq 0$,

$$|\{n < x,\ a_n \not\equiv 0 \pmod{p}\}| \gg \frac{x}{(\log x)}(\log\log x)^K, \tag{3}$$

where the implicit constant depends on K.

We improve on results (1), (2) and (3) by giving an asymptotic formula for $|\{n < x,\ a_n \not\equiv 0 \pmod{p}\}|$. To describe our results, we slightly change our setting by working directly with modular forms over a finite field, which allows for more generality and more flexibility.

Let p be an odd prime[1] and $N \geq 1$ an integer. We define the space of modular forms of level $\Gamma_1(N)$ with coefficients in $\mathbb{F}_p$, denoted by $M(N, \mathbb{F}_p)$, as the subspace of $\mathbb{F}_p[\![q]\!]$ generated by the reductions modulo p of the q-expansions at ∞ of all holomorphic modular forms of level $\Gamma_1(N)$ and some integral weight $k \geq 0$ with coefficients in $\mathbb{Z}$. For $\mathbb{F}$ a finite extension of $\mathbb{F}_p$, we define $M(N, \mathbb{F})$ as $M(N, \mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}$. Given f in $M(N, \mathbb{F})$, let

$$\pi(f, x) = |\{n < x : a_n \neq 0\}|.$$

Theorem 1. *Let $f = \sum_{n=0}^{\infty} a_n q^n \in M(N, \mathbb{F})$, and assume that f is not constant; that is, assume $a_n \neq 0$ for some $n \geq 1$. Then there exists a rational number $\alpha(f)$ with $0 < \alpha(f) \leq 3/4$, an integer $h(f) \geq 0$, and a positive real constant $c(f) > 0$ such that*

$$\pi(f, x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log\log x)^{h(f)}.$$

This theorem was established by Serre [1976] for the case when f is an *eigenform* for all Hecke operators T_m (that is, $T_m f = \lambda_m f,\ \lambda_m \in \mathbb{F}$), and in this case one has $h(f) = 0$. However, the case of eigenforms is special because, as shown by Atkin, Serre, Tate and Jochnowitz in the 1970s, there are only finitely many normalized eigenforms in the infinite-dimensional space $M(N, \mathbb{F})$. One can decompose every $f \in M(N, \mathbb{F})$ as a finite sum $\sum_i f_i$ of *generalized eigenforms*[2] f_i but this fact does not seem to be of immediate use, for two reasons. The methods for treating genuine eigenforms do not seem to apply readily to generalized eigenforms, and moreover it is not clear how to obtain an asymptotic formula for $\pi(f, x)$ from asymptotics for $\pi(f_i, x)$. For f an eigenform, the main tool in Serre's study is the Galois representation over a finite field attached to f by Deligne's construction, $\bar{\rho}_f : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F})$. To deal with a general modular form f we replace ρ_f by a two-dimensional Galois *pseudorepresentation*, t_f,

[1] When $p = 2$, similar but slightly different results may be obtained, see [Bellaïche and Nicolas 2015].

[2] We call a form $f \in M(N, \mathbb{F})$ a *generalized eigenform* if, for every ℓ not dividing Np, there exist $\lambda_\ell \in \mathbb{F}$ and $n_l \in \mathbb{N}$ such that $(T_\ell - \lambda_\ell)^{n_\ell} f = 0$.

of $G_{\mathbb{Q},Np}$ over a *finite ring* A_f. The ring A_f is obtained as the quotient of A by the annihilator of f, where A is the Hecke algebra acting on the space of modular forms $M(N, \mathbb{F})$. The ring A_f is not in general a field. In fact, it is a field precisely when f is an eigenform for the Hecke operators T_ℓ ($\ell \nmid Np$). The Hecke algebra A (at least in the case of $\Gamma_0(N)$) was introduced and studied in the wake of Swinnerton-Dyer's work on congruences between modular forms by Serre, Tate, Mazur, Jochnowitz and others. More recent progress on understanding its structure may be found in [Nicolas and Serre 2012a; 2012b; Bellaïche and Khare 2015]. In Section 3, we recall the definitions of the Hecke algebra A, its quotient A_f, and the pseudorepresentation t_f and gather the results we need pertaining to them.

To prove Theorem 1, we introduce the notion of a *pure form*. A form f is *pure* if every Hecke operator T_ℓ (with $\ell \nmid Np$) in A_f is either invertible or nilpotent. Generalized eigenforms are pure since the finite ring A_f is local in this case, but there are pure forms that are not generalized eigenforms. For pure forms we can give a reasonable description of the set of integers n with $(n, Np) = 1$ and such that $a_n \neq 0$, and using this and a refinement of the Selberg–Delange method (see Section 2) we deduce (in Section 4A) an asymptotic formula for the number of $n \leq x$ with $a_n \neq 0$ and $(n, Np) = 1$. For a general f, we show in Section 4B that if $f = \sum_i f_i$ is a minimal decomposition of f into pure forms, then $\pi(f, x)$ is asymptotically $\sum_i \pi(f_i, x)$. To complete the proof of Theorem 1, it remains to handle coefficients a_n with $(n, Np) > 1$, and this is treated in Section 4C.

Theorem 1 gives an asymptotic formula for the number of $n < x$ such that $a_n \neq 0$ but says nothing about the number of $n < x$ such that $a_n = a$, where a is a specific fixed value in $\mathbb{F}^*$. Some partial results are given during the course of the proof of Theorem 1 in Section 4A. We say that f has the *equidistribution property* if the number of $n < x$ such that $a_n = a$ is asymptotically the same for every $a \in \mathbb{F}^*$. In Section 5 we give sufficient conditions and, in some cases, necessary conditions for the equidistribution property.

In Section 6 we consider a variant of the main theorem, where one counts only the nonzero coefficients at square-free integers of a modular form.

Let us finally mention that the constants $\alpha(f)$, $h(f)$ and $c(f)$ of Theorem 1 can be effectively computed from our proof. This is done in some cases in Section 7. However, we do not have a satisfactory understanding of how $h(f)$ and $c(f)$ behave as f varies. Such an understanding would require a more detailed study of the structure of the Hecke algebra A and of the space $M(N, \mathbb{F})$ as a Hecke-module than is currently available (except in the case $p = 2,\ N = 1$ [Nicolas and Serre 2012b; Bellaïche and Nicolas 2015] and partially in the case $p = 3,\ N = 1$ [Medvedovki 2015]).

2. Applications of the Landau–Selberg–Delange method

2A. ***Frobenian and multifrobenian sets.*** If Σ is a finite set of primes and L is a finite Galois extension of $\mathbb{Q}$ unramified outside Σ and ∞, then for any prime $\ell \notin \Sigma$ we denote by $\mathrm{Frob}_\ell \in \mathrm{Gal}(L/\mathbb{Q})$ an element of Frobenius attached to ℓ. We recall that Frob_ℓ is only well-defined up to conjugation in $\mathrm{Gal}(L/\mathbb{Q})$.

Definition 2. Let h be a nonnegative integer and Σ a finite set of primes. We say that a set $\mathcal{M}$ of positive integers is Σ-*multifrobenian* of height h if there exists a finite Galois extension L of $\mathbb{Q}$ with Galois group G, unramified outside Σ and ∞, and a subset D of G^h, invariant under conjugation and under permutations of the coordinates, such that $m \in \mathcal{M}$ if and only if $m = \ell_1 \cdots \ell_h$ where the ℓ_i are distinct primes not in Σ, and $(\mathrm{Frob}_{\ell_1}, \dots, \mathrm{Frob}_{\ell_h}) \in D$. For such a Σ-multifrobenian set $\mathcal{M}$ we define its density $\delta(\mathcal{M})$ to be

$$\delta(\mathcal{M}) = \frac{\#D}{h!(\#G)^h}.$$

Observe that the condition $(\mathrm{Frob}_{\ell_1}, \dots, \mathrm{Frob}_{\ell_h}) \in D$ depends only on the product $\ell_1 \cdots \ell_h$, since replacing each Frob_{ℓ_i} by a conjugate in G amounts to replacing $(\mathrm{Frob}_{\ell_1}, \dots, \mathrm{Frob}_{\ell_h})$ by a conjugate in G^h and D is invariant by conjugacy in G^h, and since changing the order of the prime factors $\ell_1, \dots, \ell_h$ permutes the components of $(\mathrm{Frob}_{\ell_1}, \dots, \mathrm{Frob}_{\ell_h})$ and D is invariant by permutations. Thus the notion of a multifrobenian set is well-defined.

There is only one Σ-multifrobenian set of height $h = 0$, namely $\{1\}$. Note that a Σ-multifrobenian set of height 1 is just a Σ-frobenian set of prime numbers in the usual sense (see [Serre 2012, §3.3.1]). In what follows we will say that a set is *multifrobenian* if it is Σ-multifrobenian for some finite set of primes Σ and *frobenian* if it is multifrobenian of height 1. We observe that this definition of frobenian is slightly more restrictive than the one used by Serre (cf. [2012, §3.3.2]) for whom a set of primes is frobenian if it is frobenian in our sense up to a finite set of primes. The more restrictive definition of frobenian that we adopt here will be sufficient for our purposes, and we hope that its use will cause no confusion to the reader.

Lemma 3. *Let $\mathcal{M}$ be a multifrobenian set of height h and density $\delta(\mathcal{M})$. Then*

$$\sum_{\substack{m \in \mathcal{M} \\ m \le x}} \frac{1}{m} \sim \delta(\mathcal{M})(\log \log x)^h.$$

Proof. This follows from the Chebotarev density theorem. □

Note in particular that $\delta(\mathcal{M})$ depends only on the set $\mathcal{M}$ and not on the choice of L, G and D.

Remark 4. Using the Chebotarev density theorem, one may show that if $\mathcal{M}$ is a multifrobenian set of height h, then

$$|\{n \le x : n \in \mathcal{M}\}| \sim h\delta(\mathcal{M}) \frac{x}{\log x} (\log\log x)^{h-1}.$$

This formula clearly implies Lemma 3 by partial summation, but the weaker Mertens-type estimate of Lemma 3 suffices for our purposes.

2B. ***Square-free integers with prime factors in a frobenian set and random walks.*** We begin with a general result of the Landau–Selberg–Delange type, which follows by the method discussed in Chapter II.5 of Tenenbaum's book [1995], or as in Théorème 2.8 of Serre's paper [1976].

Proposition 5. *Let $a(n)$ be a sequence of complex numbers with $|a(n)| \le d_k(n)$ for some natural number k, where $d_k(n)$ denotes the k-divisor function defined by $\zeta(s)^k = \sum_{n=1}^{\infty} d_k(n) n^{-s}$. Suppose that in the region* $\mathrm{Re}(s) > 1$ *the function $A(s) = \sum_{n=1}^{\infty} a(n) n^{-s}$ can be written, for some real number α, as*

$$A(s) = \zeta(s)^{\alpha} B(s),$$

where $B(s)$ extends analytically to the region $\mathrm{Re}(s) > 1 - c/\log(2 + |t|)$ *for some positive constant c and is bounded in that region by $|B(s)| \le C(1 + |t|)$ for some constant C. Then, for all $x \ge 3$ and any $J \ge 0$, there is an asymptotic expansion*

$$\sum_{n \le x} a(n) = \sum_{j=0}^{J} \frac{A_j x}{(\log x)^{1+j-\alpha}} + O\left(\frac{Cx}{(\log x)^{J+2-\alpha}}\right),$$

where the A_j are constants, with

$$A_0 = \frac{B(1)}{\Gamma(\alpha)},$$

and the implied constant in the remainder term depends only on c, k, and J.

Proof. As mentioned above, this is a straightforward application of the Landau–Selberg–Delange method, and so we content ourselves with sketching the argument briefly. The constant c can be replaced by a possibly smaller constant so that $\zeta(s)$ has no zeros in the region $\mathrm{Re}(s) > 1 - c/\log(2+|t|)$, and moreover in this region we have the classical bounds $|\zeta(s)^{\alpha}| \ll (\log(|s|+2))^{A|\alpha|}$ for some constant A provided we stay away from $s = 1$ (see for example II.3 of [Tenenbaum 1995]). Next, by applying a quantitative version of Perron's formula we see that, for $x \ge 3$ and with $x^{1/(10k)} \ge T \ge 1$,

$$\sum_{n \le x} a(n) = \frac{1}{2\pi i} \int_{1+1/\log x - iT}^{1+1/\log x + iT} A(s) \frac{x^s}{s}\, ds + O\left(\frac{x}{T} (\log x)^k\right).$$

Now we deform the line of integration as follows. First make a slit along the real line segment from $1 - c/\log(T+2)$ to 1. Then from $1 + 1/\log x + iT$ we proceed in a straight line to $1 - c/\log(T+2) + iT$ and from there to $1 - c/\log(T+2) + i0^{+}$ (on the upper part of the slit) and from there to 1. We then circle around to the lower part of the slit until $1 - c/\log(T+2) + i0^{-}$ and from there to $1 - c/\log(T+2) - iT$ and thence to $1 + 1/\log x - iT$. The integrand has a logarithmic singularity at 1, and the change in the argument above and below the slit leads to the main terms in the asymptotic expansion (by "Hankel's formula"; see [Tenenbaum 1995, §II.5.2]). The remaining integrals are estimated using the bounds for $|\zeta(s)^{\alpha}|$ in the zero-free region, together with our assumed bound for $|B(s)|$. The resulting error terms are bounded by $O(x^{1-c/\log(T+2)}(T+2)\log(T+2))$. Choosing $T = \exp(c_1\sqrt{\log x})$ for a suitably small positive constant c_1, we obtain the proposition. □

Now suppose we are given a frobenian set of primes $\mathcal{U}$ of density $\beta = \delta(\mathcal{U}) > 0$, a finite abelian group Γ, and a frobenian map[3] $\tau_0 : \mathcal{U} \to \Gamma$ such that the image $\tau_0(\mathcal{U})$ generates Γ. Using multiplicativity, extend τ_0 to a map τ from the set of square-free numbers composed of prime factors in $\mathcal{U}$ to Γ.

Theorem 6. *Let g be any given element of Γ, and let r be a positive integer. Then, for $x \geq 3$ and uniformly in r, we have*

$$\#\{n \leq x : n \text{ square-free}, \ p \mid n \Longrightarrow p \in \mathcal{U}, \ \tau(n) = g, \ (n,r) = 1\} \\ = C(\mathcal{U}, r)\frac{1}{|\Gamma|}\frac{x}{(\log x)^{1-\beta}} + O\biggl(\frac{x d(r)}{(\log x)^{1-\beta+\delta}}\biggr),$$

where $C(\mathcal{U}, r) = (1/\Gamma(\beta))\prod_p w_p$ with $w_p = (1+1/p)(1-1/p)^{\beta}$ if $p \in \mathcal{U}$ with $p \nmid r$, and $w_p = (1-1/p)^{\beta}$ otherwise. In the remainder term above, $d(r)$ denotes the number of divisors of r, and δ is a fixed positive number (depending only on the group Γ).

Proof. We use the orthogonality of the characters of the group Γ, which we write multiplicatively even though it is abelian. Thus the quantity we want is

$$\frac{1}{|\Gamma|}\sum_{\chi \in \widehat{\Gamma}} \overline{\chi(g)} \sum_{\substack{n \leq x \\ (n,r)=1}} \chi(\tau(n)),$$

where we set $\chi(\tau(n)) = 0$ if n is divisible by some prime not in $\mathcal{U}$ or if n is not square-free.

We will use Proposition 5 to evaluate the sum over n above. Since the map τ is frobenian, by the usual proof of the Chebotarev density theorem (that is, by expressing frobenian sets in terms of Hecke L-functions and using the zero-free

[3] A map from a frobenian set of primes to a finite set is called *frobenian* if its fibers are frobenian.

region for Hecke L-functions) we may write

$$\sum_{\substack{n=1\\(n,r)=1}}^{\infty} \frac{\chi(\tau(n))}{n^s} = \zeta(s)^{\beta(\chi)} B_{\chi,r}(s), \quad \text{where } \beta(\chi) = \sum_{g\in\Gamma} \chi(g)\delta(\tau_0^{-1}(g)),$$

and $B_{\chi,r}(s)$ extends analytically to the region $\mathrm{Re}(s) > 1 - c/(\log(2+|t|))$ for some $1/10 \geq c > 0$ and in that region satisfies the bound $|B_{\chi,r}(s)| \leq Cd(r)(1+|t|)$ for some constant C. The constants c and C depend only on $\mathcal{U}$ and Γ but not on r.

First suppose that χ equals the trivial character χ_0. Note that $\beta(\chi)$ then equals β and that

$$B_{\chi_0,r}(s) = \prod_{\substack{p\in\mathcal{U}\\ p\nmid r}} \left(1 - \frac{1}{p^s}\right)^{\beta} \left(1 + \frac{1}{p^s}\right) \prod_{\substack{p\notin\mathcal{U}\\ \text{or } p|r}} \left(1 - \frac{1}{p^s}\right)^{\beta}.$$

Therefore, appealing to Proposition 5, we obtain the main term of the theorem.

Now suppose that χ is not the trivial character. Then $\mathrm{Re}(\beta(\chi)) \leq \beta - \delta$ for some fixed $\delta > 0$, since there is a g in the image of τ_0 such that $\chi(g) \neq 1$ (since $\tau(\mathcal{U})$ generates Γ), and the frobenian set $\tau_0^{-1}(g)$ is nonempty and hence of positive density $\delta(\tau_0^{-1}(g))$. Therefore, by Proposition 5, we see that the contribution of the nontrivial characters is

$$O\left(\frac{xd(r)}{(\log x)^{1-\beta+\delta}}\right). \qquad \square$$

2C. *A density result.* We keep the notation and hypotheses of the preceding section: $\mathcal{U}$ is a frobenian set with $\beta = \delta(\mathcal{U}) > 0$, Γ is a finite abelian group, and $\tau_0 : \mathcal{U} \to \Gamma$ is a frobenian map whose image generates Γ. In addition, let $\mathcal{M}$ be a multifrobenian set of height $h \geq 0$, such that every element in $\mathcal{M}$ is coprime to the primes in $\mathcal{U}$. Let $\mathcal{S}$ be a given nonempty set of square-full numbers (we permit 1 to be treated as a square-full number).

Define $\mathcal{Z} = \mathcal{Z}(\mathcal{U}, \mathcal{M}, \mathcal{S})$ to be the set of positive integers $n \geq 1$ that can be written as

(2.1) $n = mm'm''$ with m, m', m'' positive integers such that

(2.1.1) m is square-free and all its prime factors are in $\mathcal{U}$;

(2.1.2) $m' \in \mathcal{M}$;

(2.1.3) $m'' \in \mathcal{S}$ and m'' is relatively prime to mm'.

These conditions imply that m, m' and m'' are pairwise relatively prime, and for $n \in \mathcal{Z}$ such a decomposition $n = mm'm''$ is unique. Extend τ to a map $\mathcal{Z} \to \Gamma$ by setting $\tau(n) = \tau(m)$ for n as in (2.1). Let Δ be any nonempty subset of Γ.

Theorem 7. *With notation as above, we have*

$$\#\{n \leq x : n \in \mathcal{Z},\ \tau(n) \in \Delta\} \sim C\delta(\mathcal{M}) \frac{|\Delta|}{|\Gamma|} \frac{x}{(\log x)^{1-\beta}} (\log\log x)^h,$$

where (*with* $C(\mathcal{U}, s)$ *as in Theorem 6*)

$$C = \sum_{s \in \mathcal{S}} \frac{C(\mathcal{U}, s)}{s}.$$

Proof. Set $R = (\log x)^2$ and $z = x^{1/\log\log x}$. We want to count $n = mm'm''$ for $m'' \in \mathcal{S}$, $m' \in \mathcal{M}$, with $(m', m'') = 1$, and for m composed of primes in $\mathcal{U}$, with $(m, m'') = 1$ and $\tau(m) = g$. We now group these terms according to whether (i) $m'' \le R$ and $m' \le z$, or (ii) $m'' \le R$ but $m' > z$, or (iii) $m'' > R$. We shall show that the first case gives the main term in the asymptotics, and the other two cases are negligible.

First consider case (i). This case contributes

$$\sum_{\substack{m'' \in \mathcal{S} \\ m'' \le R}} \sum_{\substack{m' \in \mathcal{M} \\ m' \le z \\ (m', m'')=1}} \sum_{g \in \Delta} \left| \left\{ m \le \frac{x}{m'm''} : \tau(m) = g,\ (m, m'') = 1 \right\} \right|.$$

Now we use Theorem 6, so that the above equals

$$\sum_{\substack{m'' \in \mathcal{S} \\ m'' \le R}} \sum_{\substack{m' \in \mathcal{M} \\ m' \le z \\ (m', m'')=1}} \left(C(\mathcal{U}, m'') \frac{|\Delta|}{|\Gamma|} \frac{x}{m'm''(\log(x/m'm''))^{1-\beta}} + O\left(\frac{x d(m'')}{m'm''(\log x)^{1-\beta+\delta}} \right) \right).$$

Using Lemma 3, and since $\sum_{m'' \in \mathcal{S}} d(m'')/m''$ converges, we see that the error term above is $O(x/(\log x)^{1-\beta+\delta-\epsilon})$, which is negligible. Since $\log(x/m'm'') \sim \log x$, the main term above is (again using Lemma 3)

$$\sim \frac{|\Delta|}{|\Gamma|} \frac{x}{(\log x)^{1-\beta}} (\delta(\mathcal{M})(\log\log x)^h) \sum_{\substack{m'' \in \mathcal{S} \\ m'' \le R}} \frac{C(\mathcal{U}, m'')}{m''},$$

which equals the main term of the theorem.

Now consider case (ii). Since all the terms involved are positive, we see that they contribute (with $\omega(u)$ denoting the number of distinct prime factors of u)

$$\ll \sum_{\substack{m'' \in \mathcal{S} \\ m'' \le R}} \sum_{\substack{z \le u \le x/m'' \\ \omega(u)=h}} \sum_{\substack{m \le x/(um'') \\ p|m \Rightarrow p \in \mathcal{U}}} 1. \tag{4}$$

Now in the sums above either $u \le \sqrt{x}$ or $m \le \sqrt{x}$. In the first case, note that the largest prime factor of u lies in $[z^{1/h}, \sqrt{x}]$ and the others are all below $\sqrt{x}$. Moreover, using Proposition 5, the inner sum over m in (4) is $\ll x/(um''(\log x)^{1-\beta})$.

Thus we see that the first-case contribution to (4) is bounded by

$$\ll \sum_{\substack{m''\in\mathcal{S}\\ m''\le R}} \sum_{\substack{z<u\le\sqrt{x}\\ \omega(u)=h}} \frac{x}{um''(\log x)^{1-\beta}} \ll \frac{x}{(\log x)^{1-\beta}} \Bigg(\sum_{\substack{p\ge z^{1/h}\\ p\le\sqrt{x}}} \frac{1}{p}\Bigg)\Bigg(\sum_{p\le\sqrt{x}} \frac{1}{p}\Bigg)^{h-1}$$
$$\ll \frac{x}{(\log x)^{1-\beta}} (\log\log x)^{h-1} \log\log\log x.$$

For the second case, note that for $m \le \sqrt{x}$ (and $m'' \le R = (\log x)^2$) we have (by standard estimates for the number of integers with h distinct prime factors)

$$\sum_{\substack{u\le x/(mm'')\\ \omega(u)=h}} 1 \ll \frac{x}{mm''} \frac{(\log\log x)^{h-1}}{\log x},$$

and so we obtain that the second-case contribution to (4) is bounded by

$$\ll \frac{x}{\log x} (\log\log x)^{h-1} \sum_{\substack{m\le\sqrt{x}\\ m\in\mathcal{U}}} \frac{1}{m} \ll \frac{x}{\log x} (\log\log x)^{h-1} \prod_{\substack{p\le\sqrt{x}\\ p\in\mathcal{U}}} \Big(1+\frac{1}{p}\Big)$$
$$\ll \frac{x}{(\log x)^{1-\beta}} (\log\log x)^{h-1}.$$

Putting both cases together, we see that the contribution of the terms in case (ii) is

$$\ll \frac{x}{(\log x)^{1-\beta}} (\log\log x)^{h-1} \log\log\log x,$$

which is small compared to the contribution from case (i).

Finally, since the number of $mm' \le x/m''$ is trivially at most x/m'', the contribution in case (iii) is

$$\ll \sum_{\substack{m''\in\mathcal{S}\\ m''>R}} \frac{x}{m''} \ll \frac{x}{\sqrt{R}} = \frac{x}{\log x},$$

which is negligible. This completes our proof. □

3. Modular forms modulo p

3A. ***The algebra of modular forms $M(N, \mathbb{F})$.*** As in the introduction, we fix an odd prime p and a level $N \ge 1$. Let $k \ge 0$ be an integer. The space $M_k(N, \mathbb{Z})$ denotes the space of all holomorphic modular forms of weight k and level $\Gamma_1(N)$ and with q-expansion at infinity in $\mathbb{Z}[[q]]$. For any commutative ring A we define

$$M_k(N, A) = M_k(N, \mathbb{Z}) \otimes A.$$

The natural q-expansion map $M_k(N, A) \to A[\![q]\!]$ is injective for any ring A (this is the q-expansion principle; see [Diamond and Im 1995, Theorem 12.3.4]), and so we may view below $M_k(N, A)$ as a subspace of $A[\![q]\!]$. Finally we define

$$M(N, A) = \sum_{k=0}^{\infty} M_k(N, A) \subset A[\![q]\!].$$

Note that if A is a subring of $\mathbb{C}$, then $M(N, A)$ is the *direct* sum of the spaces $M_k(N, A)$ (see [Miyake 2006, Lemma 2.1.1]). However, the situation is different for general rings A and, in particular, when A is a finite field. For instance, the constant modular form 1 of weight 0 in $M_0(N, \mathbb{F}_p)$ and the Eisenstein series E_{p-1} in $M_{p-1}(N, \mathbb{F}_p)$ both have the same q-expansion 1, showing that the subspaces $M_0(N, \mathbb{F}_p)$ and $M_{p-1}(N, \mathbb{F}_p)$ are not in direct sum in $\mathbb{F}_p[\![q]\!]$. For the same reason it is not true that $M(N, A) \otimes_A A' = M(N, A')$ in general (though this is true if A' is flat over A); rather $M(N, A')$ is the image of $M(N, A) \otimes_A A'$ in $A'[\![q]\!]$.

3B. ***Hecke operators on $M_k(N, A)$.*** For any $k \geq 0$, the space of modular forms $M_k(N, \mathbb{C})$ is endowed with the action of the Hecke operators T_n for positive integers n. If n is a positive integer coprime to N, define the operator S_n as $n^{k-2}\langle n \rangle$, where $\langle n \rangle$ is the diamond operator. Recall that these operators satisfy the following properties.

(3.1) All the operators T_n and S_m commute.

(3.2) We have $S_1 = 1$ and $S_{mn} = S_m S_n$ for all m, n coprime to N.

(3.3) The Hecke relations $T_1 = 1$, $T_{mn} = T_m T_n$ if $(m, n) = 1$ hold. If $\ell \nmid N$ is prime, then $T_{\ell^{n+1}} = T_{\ell^n} T_\ell - \ell S_\ell T_{\ell^{n-1}}$. If $\ell \mid N$ is prime then $T_{\ell^n} = (T_\ell)^n$.

As is customary, we shall also use below the notation U_ℓ for the operators T_ℓ when $\ell \mid N$. From the above relations one sees that the operators T_ℓ and S_ℓ for ℓ prime determine all the others. Recall that the action of the Hecke operators on q-expansions is given as follows.

(3.4) If $\ell \mid N$ then $a_n(U_\ell f) = a_{\ell n}(f)$.

(3.5) If $\ell \nmid N$ is prime, then $a_n(T_\ell f) = a_{\ell n}(f) + \ell a_{n/\ell}(S_\ell f)$, with the understanding that $a_{n/\ell}$ means 0 if $\ell \nmid n$.

It follows that

(3.6) if $(n, m) = 1$ then $a_n(T_m f) = a_{nm}(f)$; in particular, $a_1(T_m f) = a_m(f)$ for every $m \geq 1$.

Lastly, we recall the following important fact, which follows from the geometric interpretation due to Katz [1973] of the elements of $M_k(N, A)$ as the sections of a coherent sheaf on the modular curve $Y_1(N)_{/A}$ over A, and of the Hecke operators as correspondences on $Y_1(N)$. A convenient reference is [Diamond and Im 1995, Chapter 12].

(3.7) Let A be a subring of $\mathbb{C}$. All the operators T_n and S_n leave stable the subspace $M_k(N, A)$ of $M_k(N, \mathbb{C})$.

This fact allows us to define unambiguously the operators T_n and S_n over $M_k(N, A) = M_k(N, \mathbb{Z}) \otimes_{\mathbb{Z}} A$ by extending the scalars from $\mathbb{Z}$ to A for the linear operators T_n and S_n on $M_k(N, \mathbb{Z})$.

3C. *Hecke operators on $M(N, \mathbb{F})$.* From now on, $\mathbb{F}$ is a finite field of characteristic p. First we recall a result due to Serre and Katz, which allows us to assume that the level N is prime to p; for a proof, see [Gouvêa 1988, pages 21–22].

(3.8) Let $\mathbb{F}$ be a finite field of characteristic p. Write $N = N_0 p^\nu$ with $(N_0, p) = 1$. Then as subspaces of $\mathbb{F}[[q]]$ one has $M(N, \mathbb{F}_p) = M(N_0, \mathbb{F}_p)$.

Henceforth, we assume that $(N, p) = 1$.

(3.9) There are unique operators T_n (for any $n \geq 1$) and S_n (for $n \geq 1$ with $(n, N) = 1$) on $M(N, \mathbb{F})$ such that, for any $k \geq 0$, the inclusion $M_k(N, \mathbb{F}) \hookrightarrow M(N, \mathbb{F})$ is compatible with the operators T_n and S_n defined on the source and target.

Since the sum of the $M_k(N, A)$ for $k = 0, 1, 2, \ldots$ is $M(N, A)$ by definition, the uniqueness claimed in (3.9) follows. The existence relies on the interpretation of the elements of $M(N, A)$ as algebraic functions on the open Igusa curve (an étale cover of degree $p - 1$ of the ordinary locus of $Y_1(N)_{/\mathbb{F}_p}$) which is due to Katz (see [1973; 1975, Theorem 2.2]) and based on earlier work of Igusa. For a more recent reference for (3.9), see [Gross 1990, Propositions 5.5 and 5.9].

It is clear that the operators T_n and S_n still satisfy properties (3.1) to (3.6). We record one more easy consequence of (3.9).

(3.10) The actions of the Hecke operators T_n and S_n on $M(N, \mathbb{F})$ are locally finite. That is, any form $f \in M(N, \mathbb{F})$ is contained in a finite-dimensional subspace of $M(N, \mathbb{F})$ stable under all these operators.

We shall use the notation U_p instead of T_p when acting on the space $M(N, \mathbb{F})$. More generally, if m is an integer all of whose prime factors divide Np we shall use the notation U_m instead of T_m.

Finally, we note that the space $M(N, \mathbb{F})$ enjoys an additional Hecke operator (see [Jochnowitz 1982, §1]).

(3.11) The subspace $M(N, \mathbb{F})$ of $\mathbb{F}[[q]]$ is stable under the operator V_p defined by $V_p\left(\sum a_n q^n\right) = \sum a_n q^{pn}$.

3D. ***The subspace $\mathcal{F}(N, \mathbb{F})$ of $M(N, \mathbb{F})$.*** Using the same notation as in [Nicolas and Serre 2012a; 2012b], let us define $\mathcal{F}(N, \mathbb{F})$ as the subspace $\bigcap_{\ell | Np} \ker U_\ell$ of $M(N, \mathbb{F})$. In other words,

(3.12) $\mathcal{F}(N, \mathbb{F}) = \{f = \sum_{n=0}^{\infty} a_n q^n \in M(N, \mathbb{F}),\ a_n \neq 0 \Rightarrow (n, Np) = 1\}$.

Since the Hecke operators commute, T_ℓ and S_ℓ for $\ell \nmid Np$ stabilize $\mathcal{F}(N, \mathbb{F})$.

3E. ***The residual Galois representations $\bar\rho$ and the invariant $\alpha(\bar\rho)$.*** We denote by $G_{\mathbb{Q},Np}$ the Galois group of the maximal algebraic extension of $\mathbb{Q}$ unramified outside Np. We denote by c a complex conjugation in $G_{\mathbb{Q},Np}$. If ℓ is a prime not dividing Np, we denote by Frob_ℓ an element of Frobenius associated to ℓ in $G_{\mathbb{Q},Np}$. We fix an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$.

We shall denote by $R = R(N, p)$ the set of equivalence classes of continuous odd[4] semisimple two-dimensional representations $\bar\rho$ of the Galois group $G_{\mathbb{Q},Np}$ over $\overline{\mathbb{F}_p}$ that are attached to eigenforms in $M(N, \overline{\mathbb{F}_p})$. Here we say that $\bar\rho$ is *attached to an eigenform* in $M(N, \overline{\mathbb{F}_p})$ if there exists a nonzero eigenform $f \in M(N, \overline{\mathbb{F}_p})$ for the Hecke operators T_ℓ and S_ℓ for $\ell \nmid Np$, with eigenvalues λ_ℓ and σ_ℓ, such that

(3.13) the characteristic polynomial of $\bar\rho(\mathrm{Frob}_\ell)$ is $X^2 - \lambda_\ell X + \ell\sigma_\ell$.

Although we do not need this fact, we remark that Khare and Wintenberger have shown Serre's conjecture that every odd semisimple two-dimensional representation of Serre's conductor N is attached to an eigenform in $M(N, \overline{\mathbb{F}_p})$.

A result of Atkin, Serre and Tate in the case $N = 1$ [Serre 1973], and of Jochnowitz in the general case [1982, Theorem 2.2], states that the number of systems of eigenvalues for the T_ℓ and S_ℓ appearing in $M(N, \overline{\mathbb{F}_p})$ is finite. Hence $R(N, p)$ is a finite set. If $\bar\rho : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is a representation, it is defined over some finite extension $\mathbb{F}$ of $\mathbb{F}_p$ inside $\overline{\mathbb{F}_p}$ (for absolutely irreducible $\bar\rho$, this amounts to saying that $\operatorname{tr} \bar\rho(G_{\mathbb{Q},Np}) \subset \mathbb{F}$, since finite fields have trivial Brauer groups). Therefore, there exists a finite extension $\mathbb{F}$ of $\mathbb{F}_p$ such that all representations in $R(N, p)$ are defined over $\mathbb{F}$.

For $\bar\rho \in R(N, p)$, we shall denote by $U_{\bar\rho}$ the open and closed subset of $G_{\mathbb{Q},Np}$ of elements g such that $\operatorname{tr} \bar\rho(g) \neq 0$, and by $N_{\bar\rho}$ its complement, the set of elements g such that $\operatorname{tr} \bar\rho(g) = 0$. We set $\alpha(\bar\rho) = \mu_{G_{\mathbb{Q},Np}}(N_{\bar\rho})$, where $\mu_{G_{\mathbb{Q},Np}}$ is the Haar measure on the compact group $G_{\mathbb{Q},Np}$.

Proposition 8. *For all representations $\bar\rho$ we have $\alpha(\bar\rho) \in \mathbb{Q}$ with $0 < \alpha(\bar\rho) \leq 3/4$. If $\bar\rho$ is reducible, we have $\alpha(\bar\rho) \leq 1/2$.*

Proof. By definition, $\alpha(\bar\rho)$ is the proportion of elements of trace zero in the finite subgroup $G = \bar\rho(G_{\mathbb{Q},Np})$ of $\mathrm{GL}_2(\overline{\mathbb{F}_p})$. Thus $\alpha(\bar\rho)$ is rational and is at most one. Since $\bar\rho(c)$ has trace zero, we have $\alpha(\bar\rho) > 0$. It remains now to obtain the upper

[4] That is, such that $\operatorname{tr} \bar\rho(c) = 0$.

bounds claimed for $\alpha(\bar\rho)$. Let G' be the image of G in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. Then $\alpha(\bar\rho)$ is also the proportion of elements of trace zero in G' (it makes sense to say that an element of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ has "trace zero", even though the trace of such an element is of course not well-defined). Also, observe that an element g' in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ has trace 0 if and only if it has order exactly 2. Indeed, let g be a lift of g' in $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$. If g is diagonalizable and x, y are its eigenvalues, then g' having order exactly 2 means that $x \neq y$, but $x^2 = y^2$; thus $x = -y$, and $\operatorname{tr} g = 0$. If g is not diagonalizable, then the order of g' is a power of p, hence not 2, and it has a double eigenvalue $x \neq 0$ so its trace $2x$ is not 0. Hence $\alpha(\bar\rho)$ is also the proportion of elements of order 2 in G'.

If $\bar\rho$ is reducible, then, since $\bar\rho$ is assumed semisimple, G is conjugate to a subgroup of the diagonal subgroup $D = \overline{\mathbb{F}}_p^* \times \overline{\mathbb{F}}_p^*$, and G' may thus be assumed to be a subgroup of the image D' of D in PGL_2. The group D' is isomorphic to $\overline{\mathbb{F}}_p^*$, by the isomorphism sending $x \in \overline{\mathbb{F}}_p^*$ to the image of $\left(\begin{smallmatrix}1&0\\0&x\end{smallmatrix}\right)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$, and via this identification the only element of trace zero of D' is -1, which is always in G' because G contains $\bar\rho(c)$. Thus one has $\alpha(\bar\rho) = 1/|G'|$. Therefore, $\alpha(\bar\rho) \leq 1/2$ since G' is not the trivial group because $\bar\rho(c)$ is not trivial in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$.

Now assume that $\bar\rho$ is irreducible. We shall use the classification of subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ for which a convenient modern reference is [Faber 2012]. According to Theorems B and C of [Faber 2012], if G' is any finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$, we are in one of the 9 situations described there and labeled B(1) to B(4) and C(1) to C(5). The case B(3) does not arise since we assume $p > 2$, and neither do cases B(2) and C(1) which contradict the assumed irreducibility of $\bar\rho$ (for B(2) because G' cyclic implies G abelian, and for C(1) by Remark 2.1 of [Faber 2012]). In the other situations, we argue as follows.

- C(2) G' is isomorphic to a dihedral group D_{2n} of order $2n$ (for $n \geq 2$ an integer) which is a semidirect product of a cyclic group C_n by a subgroup of order 2. In this case, the elements of order 2 are the elements not in C_n and, if n is even, the unique element of order 2 in C_n. Thus
$$\alpha(\bar\rho) = \begin{cases} \frac{1}{2} & \text{if } n \text{ is odd,} \\ \frac{1}{2} + \frac{1}{2n} & \text{if } n \text{ is even.} \end{cases}$$
Note that if $n = 2$, then $\alpha(\bar\rho) = 3/4$, and in all other cases $\alpha(\bar\rho) \leq 5/8$.
- C(3) $G' \simeq A_4$, so $\alpha(\bar\rho) = 1/4$ since A_4 has order 12, and has 3 elements of order 2.
- C(4) $G' \simeq S_4$, so $\alpha(\bar\rho) = 3/8$ since S_4 has order 24 and 9 elements of order 2 (6 transpositions and 3 products of two disjoint transpositions).
- C(5), B(4) $G' \simeq A_5$, so $\alpha(\bar\rho) = 1/4$ since A_5 has order 60 and has 15 elements of order 2 (the products of two disjoint transpositions).

B(1) The subgroup G' of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is conjugate to $\mathrm{PGL}_2(\mathbb{F}_q)$, where q is some power of p. In this case, the number of matrices of trace 0 in G' is q^2, while $|G'| = q(q-1)(q+1)$, so

$$\alpha(\bar{\rho}) = \frac{q}{(q-1)(q+1)}.$$

Thus in this case we have $\alpha(\bar{\rho}) \le 3/8$, and this bound is attained for $q = 3$.

B(1) again The subgroup G' of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is conjugate to $\mathrm{PSL}_2(\mathbb{F}_q)$. The number of matrices of trace 0 in $\mathrm{SL}_2(\mathbb{F}_q)$ is $q^2 - q$ if -1 is not a square in $\mathbb{F}_q$ and $q^2 + q$ if -1 is a square. Since $|\mathrm{SL}_2(\mathbb{F}_q)| = q(q-1)(q+1)$ one has

$$\alpha(\bar{\rho}) = \begin{cases} \frac{1}{q+1} & \text{if } -1 \text{ is not a square in } \mathbb{F}_q, \\ \frac{1}{q-1} & \text{if } -1 \text{ is a square in } \mathbb{F}_q. \end{cases}$$

Thus in this case we have $\alpha(\bar{\rho}) \le 1/4$, and this value is attained for $q = 3$ and $q = 5$. □

3F. *The Hecke algebra A.* From now on, we assume that $\mathbb{F}$ is a finite field contained in $\overline{\mathbb{F}}_p$ and large enough to contain the fields of definition of all the representations $\bar{\rho} \in R(N, p)$.

Let $A = A(N, \mathbb{F})$ be the closed subalgebra of $\mathrm{End}_{\mathbb{F}}(M(N, \mathbb{F}))$ generated by the Hecke operators T_ℓ and S_ℓ for ℓ prime not dividing Np. Equivalently, by (3.3), A is the closed subalgebra of $\mathrm{End}_{\mathbb{F}}(M(N, \mathbb{F}))$ generated by the T_m for all m relatively prime to Np. Here we give $M(N, \mathbb{F})$ its discrete topology and $\mathrm{End}_{\mathbb{F}}(M(N, \mathbb{F}))$ its compact-open topology. Then $M = M(N, \mathbb{F})$ and $\mathcal{F} = \mathcal{F}(N, \mathbb{F})$ are topological A-modules. Note that if $f \in M$ (or if $f \in \mathcal{F}$) the submodule Af of M (respectively of $\mathcal{F}$) generated by f is finite-dimensional over $\mathbb{F}$ by (3.10), and hence is finite as a set.

By construction, the maximal ideals of $A(N, \mathbb{F})$ correspond to the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F})$-conjugacy classes of systems of eigenvalues (for the T_ℓ and S_ℓ, $\ell \nmid Np$) appearing in $M(N, \overline{\mathbb{F}}_p)$. As recalled earlier, the set of such systems is finite and in natural bijection (determined by the Eichler–Shimura relation (3.13)) with the set $R(N, p)$. Further, by our choice of $\mathbb{F}$, all those eigenvalues are in $\mathbb{F}$. It follows that A is a semilocal ring; more precisely, we have a natural decomposition

$$A = \prod_{\bar{\rho} \in R(N,p)} A_{\bar{\rho}},$$

where $A_{\bar{\rho}}$ is the localization of A at the maximal ideal corresponding to the system of eigenvalues corresponding to $\bar{\rho}$. The quotient $A_{\bar{\rho}}$ of A is a complete local $\mathbb{F}$-algebra of residue field $\mathbb{F}$, and if one denotes by $T_{\bar{\rho}}$ the image of an element $T \in A$

in $A_{\bar\rho}$, then $A_{\bar\rho}$ is characterized among the local components of A by the following property.

(3.14) For every $\ell \nmid Np$, the elements $T_{\ell,\bar\rho} - \operatorname{tr}\bar\rho(\mathrm{Frob}_\ell)$ and $\ell S_\ell - \det\bar\rho(\mathrm{Frob}_\ell)$ belong to the maximal ideal $\mathfrak{m}_{\bar\rho}$ of $A_{\bar\rho}$ (or, equivalently, are topologically nilpotent in $A_{\bar\rho}$).

The decomposition of A as $\prod A_{\bar\rho}$ gives rise to corresponding decompositions of $M = M(N, \mathbb{F})$ and $\mathcal{F} = \mathcal{F}(N, \mathbb{F})$:

$$M = \bigoplus_{\bar\rho\in R(N,p)} M_{\bar\rho}, \quad \mathcal{F} = \bigoplus_{\bar\rho\in R(N,p)} \mathcal{F}_{\bar\rho},$$

such that $A_{\bar\rho}M_{\bar\rho} = M_{\bar\rho}$ and $A_{\bar\rho}M_{\bar\rho'} = 0$ if $\bar\rho \neq \bar\rho'$, and similarly for $\mathcal{F}$. In other words, $M_{\bar\rho}$ (or $\mathcal{F}_{\bar\rho}$) is the common generalized eigenspace in M (respectively $\mathcal{F}$) for all the operators T_ℓ and ℓS_ℓ ($\ell \nmid Np$) with generalized eigenvalues $\operatorname{tr}\bar\rho(\mathrm{Frob}_\ell)$ and $\det\bar\rho(\mathrm{Frob}_\ell)$.

Let $\bar\rho \in R$. Since A acts faithfully on M, the algebra $A_{\bar\rho}$ acts faithfully on $M_{\bar\rho}$. In particular $M_{\bar\rho}$ is nonzero. It is easy to deduce that $M_{\bar\rho}$ contains a nonzero eigenform for all the Hecke operators T_ℓ and S_ℓ, $\ell \nmid Np$. We shall need on one occasion the following slightly more precise result, due to Ghitza [2006].

(3.15) Let $\bar\rho \in R$. There exists a form $f = \sum_{n=1}^{\infty} a_n q^n$ in $M_{\bar\rho}$, with $a_0 = 0$, $a_1 = 1$, that is an eigenform for all the Hecke operators T_ℓ and S_ℓ, $\ell \nmid Np$.

Indeed, according to [Ghitza 2006, Theorem 1], there exists an eigenform $h \in M_{\bar\rho}$ which is cuspidal, that is, such that $a_0(h) = 0$. Let $m \in \mathbb{N}$ with $a_m(h) \neq 0$. Then $f = (1/a_m(h))U_m h$ is an eigenform and satisfies $a_0(f) = 0$, $a_1(f) = 1$.

3G. ***The Hecke modules Af and the Hecke algebra A_f.*** For $f \in M(N, \mathbb{F})$, recall that we defined Af to be the submodule of M (over A) generated by f, which by (3.10) is a finite-dimensional vector space over $\mathbb{F}$. We shall denote by A_f the image of A under the restriction map $\mathrm{End}_{\mathbb{F}}(M) \to \mathrm{End}_{\mathbb{F}}(Af)$. Thus A_f is a finite-dimensional quotient of A. We continue to denote by T_ℓ and S_ℓ the images of T_ℓ and S_ℓ in A_f.

3H. ***The support $R(f)$ of a modular form.*** For $f \in M$, we define the support of f to be the subset of R consisting of those representations $\bar\rho$ such that the component $f_{\bar\rho}$ of f in $M_{\bar\rho}$ is nonzero. We will denote the support of f by $R(f)$. Thus $R(f) = \varnothing$ if and only if $f = 0$, and $R(f)$ is a singleton $\{\bar\rho\}$ if and only if f is a generalized eigenform for all the operators T_ℓ and S_ℓ (with $\ell \nmid Np$). Equivalently, $R(f)$ is the smallest subset of R such that the natural surjection $A = \prod_{\bar\rho\in R} A_{\bar\rho} \to A_f$ factors through $\prod_{\bar\rho\in R(f)} A_{\bar\rho}$. In view of (3.14), we have the following lemma.

Lemma 9. *Let $\ell \nmid Np$. The action of the operator T_ℓ on the finite-dimensional space Af is nilpotent if and only if* $\mathrm{Frob}_\ell \in N_{\bar\rho}$ *for every $\bar\rho \in R(f)$. Similarly, the action of R_ℓ on Af is invertible if and only if* $\mathrm{Frob}_\ell \in U_{\bar\rho}$ *for every $\bar\rho \in R(f)$.*

3I. ***Pure modular forms and the invariants $\alpha(f)$ and $h(f)$.***

Definition 10. We say that $f \in M$ is *pure* if, for every $\bar\rho, \bar\rho' \in R(f)$, one has $N_{\bar\rho} = N_{\bar\rho'}$, or equivalently $U_{\bar\rho} = U_{\bar\rho'}$. If f is pure and nonzero, we denote by N_f and U_f the common sets $N_{\bar\rho}$ and $U_{\bar\rho}$ for $\bar\rho \in R(f)$. Further, we let $\mathcal{N}_f$ and $\mathcal{U}_f$ denote the sets of primes $\ell \nmid Np$ with $\mathrm{Frob}_\ell \in N_f$ and $\mathrm{Frob}_\ell \in U_f$ respectively.

Note that generalized eigenforms are pure, but that the converse is false in general. Also note that, by Lemma 9, if f is nonzero and pure and $\ell \nmid Np$, then T_ℓ is nilpotent on Af if $\ell \in \mathcal{N}_f$, and T_ℓ is invertible on Af if $\ell \in \mathcal{U}_f$.

Definition 11. Let f be a pure, nonzero, modular form. Define $\alpha(f) = \mu_{G_{\mathbb{Q},Np}}(N_f)$ such that $\alpha(f) = \alpha(\bar\rho)$ for any $\bar\rho \in R(f)$. Define the *strict order of nilpotence* of f, denoted by $h(f)$, as the largest integer h such that there exist (not necessarily distinct) prime numbers $\ell_1, \dots, \ell_h \nmid Np$ in $\mathcal{N}_f$ with $T_{\ell_1} \cdots T_{\ell_h} f \neq 0$.

Note that, in the definition of the strict order of nilpotence, the largest integer h exists and is no more than the dimension of Af, since the T_{ℓ_i} act nilpotently on Af for $\ell_i \in \mathcal{N}_f$.

(3.16) Given a general nonzero form f, partition the finite set $R(f)$ into equivalence classes $R_i(f)$ based on the equivalence relation $\bar\rho \sim \bar\rho'$ if and only if $N_{\bar\rho} = N'_{\bar\rho}$. Thus we may write

$$f = \sum_i f_i, \quad f_i = \sum_{\bar\rho \in R_i(f)} f_{\bar\rho},$$

so that the f_i are pure. We call this decomposition the *canonical decomposition of f into pure forms*.

We now extend the definitions of $\alpha(f)$ and $h(f)$ to forms that are not necessarily pure.

Definition 12. If $f = \sum_i f_i$ is the canonical decomposition of f into pure forms, we set $\alpha(f) = \min_i \alpha(f_i)$ and $h(f) = \max_{i, \alpha(f_i) = \alpha(f)} h(f_i)$.

3J. ***Existence of a pseudorepresentation and consequences.***

Proposition 13. *There exist continuous maps $t : G_{\mathbb{Q},Np} \to A$ and $d : G_{\mathbb{Q},Np} \to A$ such that*

(i) *d is a morphism of groups $G_{\mathbb{Q},Np} \to A^*$,*

(ii) *t is central (i.e., $t(gh) = t(hg)$),*

(iii) $t(1) = 2$,

(iv) $t(gh) + t(gh^{-1})d(h) = t(g)t(h)$ *for all* $g, h \in G_{\mathbb{Q},Np}$,

(v) $t(\mathrm{Frob}_\ell) = T_\ell$ *for all* $\ell \nmid Np$,

(vi) $d(\mathrm{Frob}_\ell) = \ell S_\ell$ *for all* $\ell \nmid Np$.

The uniqueness of such a pair (t, d) is clear: the function t is characterized uniquely by (ii) and (v) alone using the Chebotarev density theorem, and d is characterized by (i) and (vi) (or else by (iv); see (5) below). The existence of t and d is proved by "glueing" the traces and determinants of the representations attached by Deligne to eigenforms in characteristic zero and then reducing modulo p. For details, see [Bellaïche and Khare 2015].

Remark 14. The properties (i) to (iv) express the fact that (t, d) is a pseudorepresentation of dimension 2. The map t is called the trace, and the map d is called the determinant of the representation (t, d) (see [Chenevier 2014]). It is easy to check that the trace and determinant of any continuous two-dimensional representation (of a topological group over any topological commutative ring) satisfy properties (i) to (iv). Since $p > 2$, one can recover d from t by the formula

$$d(g) = (t(g)^2 - t(g^2))/2, \tag{5}$$

which follows upon taking $g = h$ in (iv) and using (iii).

We prove for later use the following lemma.

Lemma 15. *For every* $g \in G_{\mathbb{Q},Np}$ *one has* $t(g^p) = t(g)^p$.

Proof. Let $m \in \mathrm{GL}_2(A)$ be the matrix $\left(\begin{smallmatrix} 0 & -1 \\ d(g) & t(g) \end{smallmatrix}\right)$ with $\mathrm{tr}(m) = t(g)$ and $\det(m) = d(g)$. Since tr and det on the multiplicative subgroup generated by m satisfy properties (i) to (iv) above, one sees easily by induction on n that $\mathrm{tr}(m^n) = t(g^n)$ for all n. Thus it suffices to prove that $\mathrm{tr}(m^p) = \mathrm{tr}(m)^p$.

Let $f : \mathbb{F}_p[D, T] \to A$ be the morphism of rings sending D to $d(g)$ and T to $t(g)$, where D and T are two indeterminates. Let $M \in \mathrm{GL}_2(\mathbb{F}_p[D, T])$ be the matrix $\left(\begin{smallmatrix} 0 & -1 \\ D & T \end{smallmatrix}\right)$. Since $f(M) = m$, it clearly suffices to prove that $\mathrm{tr}(M^p) = \mathrm{tr}(M)^p$. Since $\mathbb{F}_p[D, T]$ can be embedded in an algebraic field k of characteristic p, it suffices to prove that, for all $M \in M_2(k)$, one has $\mathrm{tr}(M^p) = \mathrm{tr}(M)^p$. Replacing M by a conjugate matrix if necessary, we may assume that M is triangular, in which case the formula is obvious. □

Let $f \in M(N, \mathbb{F})$ be a modular form. Let $t_f : G \to A_f$ and $d_f : G \to A_f$ be the composition of t and d with the natural morphism of algebras $A \to A_f$. Note that (t_f, d_f) satisfies the same properties (i) to (vi), and so (t_f, d_f) is a pseudorepresentation of G on A_f. In particular, (v) reads

$$t_f(\mathrm{Frob}_\ell) f = T_\ell f. \tag{6}$$

We now deduce certain consequences of the existence of the pseudorepresentation (t, d) for the algebra A and for modular forms $f \in M$.

Proposition 16. *The Hecke algebra A is topologically generated by the T_ℓ for $\ell \nmid Np$ alone (that is, without the S_ℓ).*

Proof. Let A' be the closed subalgebra of A generated by the T_ℓ. Since the elements Frob_ℓ for $\ell \nmid Np$ are dense in $G_{\mathbb{Q},Np}$ and $t(\mathrm{Frob}_\ell) = T_\ell \in A'$, one sees that $t(G_{\mathbb{Q},Np}) \subset A'$. In particular, for ℓ not dividing Np, we have $t(\mathrm{Frob}_\ell^2) \in A'$, hence we also have $(t(\mathrm{Frob}_\ell^2) - t(\mathrm{Frob}_\ell)^2)/2$. But this element is just $d(\mathrm{Frob}_\ell) = \ell S_\ell$. Hence $S_\ell \in A'$ and $A' = A$. □

Lemma 17. *There exists a finite quotient G_f of $G_{\mathbb{Q},Np}$ such that, for $\ell \nmid Np$, the action of T_ℓ on Af depends only on the image of* Frob_ℓ *in G_f.*

Proof. Let H denote the subset of $G_{\mathbb{Q},Np}$ consisting of elements h such that $t_f(gh) = t_f(g)$ for every $g \in G$. Since t is central (property (ii) above), it follows that H is a normal subgroup of G. We call H the *kernel* of the pseudorepresentation (t_f, d_f). By (5) and (iii) one has $d_f(h) = 1$ for $h \in H$. Let $G_f = G_{\mathbb{Q},Np}/H$. The maps $t_f, d_f : G_{\mathbb{Q},Np} \to A_f$ factor through G_f to give maps $G_f \to A_f$, which we shall also denote by t_f and d_f. Note that, by construction, there is no $h \neq 1$ in G_f such that $t_f(gh) = t_f(g)$ for every $g \in G_f$. Since A_f is finite, it follows easily that G_f is a finite group. Finally, by (6), $T_\ell f$ depends only on $t_f(\mathrm{Frob}_\ell)$, which only depends on the image of Frob_ℓ in G_f. Therefore, if $g \in Af$, then $g = Tf$ for some $T \in A$, and $T_\ell g = T_\ell T f = T T_\ell f$ depends only on the image of Frob_ℓ in G_f. □

We draw three consequences of this lemma.

Proposition 18. *Let $f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{F} = \mathcal{F}(N, \mathbb{F})$. If $f \neq 0$, then there exists a square-free integer n such that $a_n \neq 0$.*

Proof. Since f is nonzero, $a_n \neq 0$ for some $n \in \mathbb{N}$, and since $f \in \mathcal{F}$, one has $(n, Np) = 1$. Thus $a_1(T_n f) \neq 0$. By Proposition 16, T_n is a limit of linear combinations of terms of the form $T_{\ell_1} \cdots T_{\ell_s}$ with $\ell_1, \dots, \ell_s$ being (not necessarily distinct) primes all not dividing Np. Since $T \mapsto a_1(Tf)$ is continuous and linear, we deduce that $a_1(T_{\ell_1} \cdots T_{\ell_s} f) \neq 0$ for some primes $\ell_1, \dots, \ell_s$ not dividing Np (again not necessarily distinct). Since the action of T_{ℓ_i} on Af depends only on Frob_{ℓ_i} in the finite Galois group G_f, one can replace ℓ_i by any other prime whose Frobenius has the same image without affecting the action of T_{ℓ_i}. In this manner, we may find distinct primes ℓ'_i such that $T_{\ell_1} \cdots T_{\ell_s} = T_{\ell'_1} \cdots T_{\ell'_s}$, and then with $m = \ell'_1 \cdots \ell'_s$ it follows that $a_m(f) = a_1(T_m f) = a_1(T_{\ell'_1} \cdots T_{\ell'_s} f) = a_1(T_{\ell_1} \cdots T_{\ell_s} f) \neq 0$. □

Proposition 19. *Let $f \in M(N, \mathbb{F})$ be a pure form, and let f' be any element of $M(N, \mathbb{F})$. Let h be a nonnegative integer, and let $\mathcal{M}$ denote the set of square-free integers m having exactly h prime factors, all from the set $\mathcal{N}_f$, and such that $T_m f = f'$. Then $\mathcal{M}$ is multifrobenian.*

Proof. Let G_f be as in Lemma 17 and let $D_{f,f'} \subset G_f^h$ denote the set of h-tuples $(g_1, \dots, g_h)$ such that $t_f(g_1) \cdots t_f(g_h) f = f'$, where $g_i \in N_f$ for $i = 1, \dots, h$. Then $D_{f,f'}$ is invariant under conjugation and symmetric under permutations, and hence by definition $\mathcal{M}$ is the multifrobenian set of weight h attached to $D_{f,f'}$ and G_f. □

Proposition 20. *Let f be a pure modular form. Then there exist $h(f)$ distinct primes $\ell_1, \dots, \ell_{h(f)}$ in $\mathcal{N}_f$ such that $T_{\ell_1} \cdots T_{\ell_{h(f)}} f \neq 0$.*

Proof. The fact that we can find $h(f)$ primes $\ell_1, \dots, \ell_{h(f)}$ in $\mathcal{N}_f$ such that $f' := T_{\ell_1} \cdots T_{\ell_{h(f)}} f \neq 0$ simply follows from the definition of $h(f)$. In the notation of the previous proposition we see that $D_{f,f'}$ is not empty as it contains $(\mathrm{Frob}_{\ell_1}, \dots, \mathrm{Frob}_{\ell_{h(f)}})$. Hence the multifrobenian set $\mathcal{M}$ of that proposition is not empty, and there exist distinct primes $\ell'_1, \dots, \ell'_{h(f)}$ in $\mathcal{N}_f$ such that $T_{\ell'_1} \cdots T_{\ell'_{h(f)}} f = f' \neq 0$. □

4. Asymptotics: proof of Theorem 1

Let $f = \sum a_n q^n \in M = M(N, \mathbb{F})$. We assume below that f is not constant. We set

$$Z(f) = \{n \in \mathbb{N},\ a_n \neq 0\} \quad \text{and} \quad \pi(f, x) = |\{n < x,\ a_n \neq 0\}|,$$

and our goal is to establish an asymptotic formula for $\pi(f, x)$. For a given $a \in \mathbb{F}^*$ it will also be convenient to define

$$Z(f, a) = \{n \in \mathbb{N},\ a_n = a\} \quad \text{and} \quad \pi(f, a, x) = |\{n < x,\ a_n = a\}|.$$

By (3.8), we may assume without loss of generality that $(N, p) = 1$, so all the results of Section 3 apply.

4A. ***Proof of Theorem 1 when $f \in \mathcal{F}(N, \mathbb{F})$ and f is pure.*** We assume in this section that f is a pure form in $\mathcal{F}(N, \mathbb{F})$. From Section 3I recall that the set of primes ℓ not dividing Np may be partitioned into two sets, $\mathcal{U}_f$ and $\mathcal{N}_f$, such that $\ell \in \mathcal{U}_f$ if T_ℓ acts invertibly on Af and $\ell \in \mathcal{N}_f$ if T_ℓ acts nilpotently on Af.

Given $a \in \mathbb{F}^*$ we wish to prove an asymptotic formula for $\pi(f, a, x)$. If n is an integer with $a_n(f) = a$ (and since $f \in \mathcal{F}$ we must have $(n, Np) = 1$) then we may write $n = mm'm''$ with m square-free and containing all prime factors from $\mathcal{U}_f$, with m' square-free and containing $h \leq h(f)$ prime factors all from $\mathcal{N}_f$, and with m'' square-full and coprime to mm'. Such a decomposition of the number n is unique, and if we write $f'' = T_{m''} f$ and $f' = T_{m'} f''$ then f' and f'' are forms in $Af - \{0\}$ with $a_m(f') = a$. Thus integers n with $a_n(f) = a$ uniquely define triples (f', f'', h) and we may decompose

$$Z(f, a) = \coprod_{f', f'', h} Z(f, a;\ f', f'', h), \tag{7}$$

where the disjoint union is taken over forms f', f'' in $Af - \{0\}$ and integers $0 \le h \le h(f)$. Here the set $Z(f, a;\, f', f'', h)$ is defined as the set of integers $n = mm'm''$ with $(n, Np) = 1$ such that

(4.1) m is square-free and all its prime factors are in $\mathcal{U}_f$;

(4.2) m' is square-free, has exactly h prime factors, and all its prime factors are in $\mathcal{N}_f$, and moreover $f' = T_{m'} f''$;

(4.3) m'' is square-full, relatively prime to mm', and $f'' = T_{m''} f$;

(4.4) $a_m(f') = a$.

Next we evaluate the number of elements up to x in the set $Z(f, a;\, f', f'', h)$ using Theorem 7. Write $\mathcal{S}_{f,f''}$ for the set of square-full integers m'' such that $T_{m''} f = f''$, and write $\mathcal{M}_{f',f''}$ for the set of integers m' that are the product of h distinct primes in $\mathcal{N}_f$ and such that $f' = T_{m'} f''$. By Proposition 19, $\mathcal{M}_{f',f''}$ is a multifrobenian set of height h. Observe that conditions (4.1), (4.2), (4.3) are the same as conditions (2.1.1), (2.1.2), (2.1.3) defining the set $\mathcal{Z}(\mathcal{U}_f, \mathcal{M}_{f',f''}, \mathcal{S}_{f,f''})$. Now, define a map $\tau_f : \mathcal{U}_f \to A_f^*$ sending ℓ to $t_f(\mathrm{Frob}_\ell) = T_\ell$ and extend it by multiplicativity to the set of all square-free integers composed only of primes from $\mathcal{U}_f$. Let Γ_f be the image of τ_f, which is a finite abelian subgroup of the finite group A_f^*, and let $\Delta_{f',a}$ denote the set of $\gamma \in \Gamma_f$ such that $a_1(\gamma f') = a$. For $n = mm'm'' \in Z(f, a;\, f', f'', h)$ set $\tau_f(n) = \tau_f(m)$ so that condition (4.4) is the same as $\tau_f(n) \in \Delta_{f',a}$. Thus we are in a position to apply Theorem 7, which yields, assuming that the sets $\mathcal{M}_{f',f''}$, $\mathcal{S}_{f,f''}$ and $\Delta_{f',a}$ are all not empty,

$$
\begin{aligned}
&|\{n < x : n \in Z(f, a;\, f', f'', h)\}| \\
&\qquad = |\{n < x : n \in \mathcal{Z}(\mathcal{U}_f, \mathcal{M}_{f',f''}, \mathcal{S}_{f,f''}),\ \tau(n) \in \Delta_{f',a}\}| \\
&\qquad\qquad \sim c\, \delta(\mathcal{M}_{f',f''}) \frac{|\Delta_{f',a}|}{|\Gamma_f|} \frac{x}{(\log x)^{\alpha(f)}} (\log\log x)^h, \qquad (8)
\end{aligned}
$$

where $c = c(f, f'') > 0$ is a constant depending only on $\mathcal{U}_f$ and $\mathcal{S}_{f,f''}$ (thus only on f and f''), and $\alpha(f) = 1 - \delta(\mathcal{U}_f) = \delta(\mathcal{N}_f)$ as defined in Section 3I. If at least one of the sets $\mathcal{M}_{f',f''}$, $\mathcal{S}_{f,f''}$ or $\Delta_{f',a}$ is empty, then so is $Z(f, a;\, f', f'', h)$.

Using (7), one deduces that either all the $Z(f, a, f', f'', h)$ are empty for all permissible choices of (f', f'', h), in which case $\pi(f, a, x) = 0$ for all x, or

$$
\pi(f, a, x) \sim c(f, a) \frac{x}{(\log x)^{\alpha(f)}} (\log\log x)^{h(f,a)}, \qquad (9)
$$

where $h(f, a) \le h(f)$ is the largest integer $h \le h(f)$ for which there exist forms $f', f'' \in Af - \{0\}$ such that $Z(f, a;\, f', f'', h)$ is not empty, and where

$$
c(f, a) = \sum_{(f', f'', h(f,a))} c(f, f'') \delta(\mathcal{M}_{f',f''}) \frac{\#\Delta_{f',a}}{\#\Gamma_f}, \qquad (10)
$$

the sum being over those $f', f'' \in Af - \{0\}$ such that $Z(f, a; f', f'', h(f, a))$ is not empty.

We claim that the set $Z(f, a; f', f'', h(f))$ is not empty for some choice of $(f', f'') \in (Af - \{0\})^2$ and some $a \in \mathbb{F}^*$. To see this, take $m'' = 1$ and $f'' = f = T_{m''} f$. By Proposition 20, there exists an integer m' with $h(f)$ distinct prime factors in $\mathcal{N}_f$ such that $T_{m'} f \neq 0$. Fix one such m' and let $f' = T_{m'} f$. Proposition 18 tells us that there exists a square-free integer m such that $a_m(f') \neq 0$. Note that $h(f') = 0$, hence m has all its prime factors in $\mathcal{U}_f$. Define $a = a_m(f') \in \mathbb{F}^*$. Then the set $Z(f, a; f', f'', h(f))$ contains $n = mm'm''$ and is therefore not empty, which proves the claim.

Since $\pi(f, x) = \sum_{a \in \mathbb{F}^*} \pi(f, a, x)$, it follows from (9) and the above claim that

$$\pi(f, x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}, \quad \text{with } c(f) = \sum_{\substack{a \in \mathbb{F}^* \\ h(f,a) = h(f)}} c(f, a). \qquad \square$$

4B. *Proof of Theorem 1 when $f \in \mathcal{F}(N, \mathbb{F})$ but f is not necessarily pure.* Let $f = \sum_i f_i$ be the canonical decomposition (see (3.16)) of f into pure forms. By the preceding section, one has

$$\pi(f_i, x) \sim c(f_i) \frac{x}{(\log x)^{\alpha(f_i)}} (\log \log x)^{h(f_i)}.$$

Consider the indices i such that $\alpha(f_i)$ is minimal (and by definition $\alpha(f_i) = \alpha(f)$); among those, select the indices with $h(f_i)$ maximal (and by definition $h(f_i) = h(f)$). Let I denote the set of such indices. We claim that

$$\pi(f, x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}, \quad \text{with } c(f) = \sum_{i \in I} c(f_i).$$

To prove the claim, first note that we can forget those f_i with $i \notin I$, because they have a negligible contribution compared to the asserted asymptotics (either the power of $\log \log x$ is smaller, or the power of $\log x$ is larger). It remains to prove that, for $i, j \in I$, $i \neq j$, one has

$$\pi(f_i, f_j, x) = o\left(\frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)} \right), \tag{11}$$

where $\pi(f_1, f_j, x) = |\{n \leq x,\ a_n(f_i) \neq 0,\ a_n(f_j) \neq 0\}|$. But if n is such that $a_n(f_i) \neq 0$ and $a_n(f_j) \neq 0$, it has at most $h(f_i) + h(f_j) = 2h(f)$ prime factors ℓ such that $\mathrm{Frob}_\ell \in N_{f_i} \cup N_{f_j}$. Moreover, the two open sets N_{f_i} and N_{f_j} of $G_{\mathbb{Q},Np}$ are not equal by definition of the decomposition into pure forms (3.16). Therefore the measure α' of the open set $N_{f_i} \cup N_{f_j}$ is strictly greater than the common measure

$\alpha(f) = \alpha(f_i) = \alpha(f_j)$ of N_{f_i} and N_{f_j}. Hence an application of Theorem 7 gives

$$\pi(f_1, f_j, x) = O\left(\frac{x}{(\log x)^{\alpha'}}(\log\log x)^{2h(f)}\right),$$

which implies (11) since $\alpha' > \alpha(f)$. □

4C. *Proof of Theorem 1: general case.* Let $\mathcal{B}$ be the set of integers $m \geq 1$ all of whose prime factors divide Np. Note that the series $\sum_{m\in\mathcal{B}} 1/m$ converges. For $m \in \mathcal{B}$, we consider the following operators on $\mathbb{F}[\![q]\!]$:

$$U_m\left(\sum a_n q^n\right) = \sum a_{mn} q^n \quad \text{and} \quad V_m\left(\sum a_n q^n\right) = \sum a_n q^{mn}.$$

We also consider the operator W defined by

$$W\left(\sum a_n q^n\right) = \sum_{(n,Np)=1} a_n q^n.$$

The operators U_m stabilize the space $M(N, \mathbb{F})$ (see Section 3C). The operator V_m however does not stabilize $M(N, \mathbb{F})$ (except for $m = p$; see (3.11)), but it sends $M(N, \mathbb{F})$ into $M(Nm, \mathbb{F})$ since it is the reduction modulo p of the action on q-expansions of the operator on modular forms $f(z) \mapsto f(mz)$. As for the operator W, it is easily seen from the definitions to satisfy

$$W = \sum_{m\in\mathcal{B}} \mu(m) V_m U_m,$$

where $\mu(m)$ is the Möbius function. Since μ vanishes on integers that are not square-free, the sum is in fact finite, and it follows that W sends $M(N, \mathbb{F})$ into $M(N^2, \mathbb{F})$ and, more precisely, into $\mathcal{F}(N^2, \mathbb{F})$.

Let $f = \sum a_n q^n \in M(N, \mathbb{F})$ be a modular form. For any integer $m \in \mathcal{B}$, define

$$f_m = \sum_{\substack{n=mm' \\ (m',Np)=1}} a_n q^n,$$

so that $f = a_0 + \sum_{m\in\mathcal{B}} f_m$. This sum may genuinely be infinite, but it obviously converges in $\mathbb{F}[\![q]\!]$. Clearly

$$\pi(f, x) = \sum_{m\in\mathcal{B}} \pi(f_m, x) + O(1),$$

where the error term $O(1)$ is just 0 if $a_0 = 0$ and 1 otherwise. One sees from the definitions that $f_m = V_m W U_m f$, so that

$$\pi(f_m, x) = \pi(W U_m f, x/m).$$

Since $\pi(f_m, x)$ is clearly at most x/m, and since $\sum_{m\in\mathcal{B}, m>(\log x)^2} 1/m \ll 1/\log x$, we conclude that

$$\pi(f, x) = \sum_{\substack{m\in\mathcal{B}\\ m\le(\log x)^2}} \pi(WU_m f, x/m) + O\left(\frac{x}{\log x}\right). \tag{12}$$

Now $WU_m f \in \mathcal{F}(N^2, \mathbb{F})$, and we can apply the results of Section 4B and thus estimate $\pi(WU_m f, x/m)$. Thus, if $WU_m f \neq 0$ and $m \le (\log x)^2$ (so that $\log(x/m) \sim \log x$), then

$$\pi(WU_m f, x/m) \sim c(WU_m f)\frac{x}{m(\log x)^{\alpha(WU_m f)}}(\log\log x)^{h(WU_m f)}. \tag{13}$$

Note that, since f is not a constant, $WU_m f \neq 0$ for at least one $m \in \mathcal{B}$. Further, note that, while $\mathcal{B}$ is infinite, the set of forms $WU_m f$ for $m \in \mathcal{B}$ is finite since $U_m f$ belongs to the Hecke-module generated by f which is finite-dimensional over $\mathbb{F}$ (see (3.10)). Thus the asymptotic formula (13) holds uniformly for all $m \le (\log x)^2$ with $m \in \mathcal{B}$ and as $x \to \infty$. Finally, since the Hecke operators T_ℓ for ℓ prime to Np commute with the operators U_m, V_m and W, it follows that

$$\alpha(f) = \min_{\substack{m\in\mathcal{B}\\ WU_m f\neq 0}} \alpha(WU_m f) \quad \text{and} \quad h(f) = \max_{\substack{m\in\mathcal{B}\\ WU_m f\neq 0\\ \alpha(WU_m f)=\alpha(f)}} h(WU_m f).$$

Thus, setting $c_m = c(WU_m f)$ when $WU_m f \neq 0$ (which happens for at least one $m \in \mathcal{B}$) and setting $c_m = 0$ otherwise, we may recast (13) as

$$\pi(WU_m f, x/m) = (c_m + \epsilon_m(x))\frac{x}{m(\log x)^{\alpha(f)}}(\log\log x)^{h(f)}, \tag{14}$$

where $\epsilon_m(x) \to 0$ as $x \to \infty$, uniformly for all $m \in \mathcal{B}$ with $m \le (\log x)^2$.

From (12) and (14) we obtain

$$\pi(f, x) \sim \sum_{\substack{m\in\mathcal{B}\\ m<(\log x)^2}} \frac{c_m}{m}\frac{x}{(\log x)^{\alpha(f)}}(\log\log x)^{h(f)} \sim c\frac{x}{(\log x)^{\alpha(f)}}(\log\log x)^{h(f)},$$

with

$$c = \sum_{m\in\mathcal{B}} \frac{c_m}{m}, \tag{15}$$

noting that this series converges because c_m takes only finitely many values (and hence is bounded). This finishes the proof of Theorem 1. □

5. Equidistribution

Definition 21. We say that a form $f \in M(\Gamma_1(N), \mathbb{F})$ has the *equidistribution property* if, for any two $a, b \in \mathbb{F}^*$, we have $\pi(f, a, x) \sim \pi(f, b, x)$. We say that a subspace $V \subset M(\Gamma_1(N), \mathbb{F})$ has the *equidistribution property* if every nonconstant form $f \in V$ has the equidistribution property.

In view of Theorem 1, f having the equidistribution property is equivalent to

$$\pi(f, a, x) \sim \frac{c(f)}{|\mathbb{F}| - 1} \frac{x}{\log(x)^{\alpha(f)}} (\log\log x)^{h(f)},$$

where $c(f)$ is the constant of Theorem 1.

We now give a sufficient condition for equidistribution for generalized eigenforms, which generalizes a similar criterion for true eigenforms due to Serre [1976, Exercise 6.10].

Proposition 22. *Let $\bar\rho : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F})$ be a representation in $R(N, p)$. If the set $\operatorname{tr}\bar\rho(G_{\mathbb{Q},Np}) - \{0\}$ generates $\mathbb{F}^*$ multiplicatively, then the generalized eigenspace $M(N, \mathbb{F})_{\bar\rho}$ has the equidistribution property.*

Proof. First assume that $f \in \mathcal{F}(N, \mathbb{F})_{\bar\rho}$. Since f is pure, the asymptotic formula (9) holds for $\pi(f, a, x)$, and to obtain equidistribution it remains to show that the constant $c(f, a)$ appearing there is independent of $a \in \mathbb{F}^*$. By formula (10), which gives the values of $c(f, a)$, it suffices to prove that the cardinalities of the subsets $\Delta_{f',a}$ of Γ_f are independent of $a \in \mathbb{F}^*$, for any given form $f' \in Af - \{0\}$. Recall that Γ_f is the subgroup of A_f^* generated by the elements $T_\ell = t_f(\mathrm{Frob}_\ell)$ for $\ell \in \mathcal{U}_f = \mathcal{U}_{\bar\rho}$ and hence, by Chebotarev and the definition of $\mathcal{U}_f$, the subgroup of A_f^* generated by $t_f(G_{\mathbb{Q},Np}) \cap A_f^*$. Recall also that $\Delta_{f',a}$ is the set of elements $\gamma \in \Gamma_f$ such that $a_1(\gamma f') = a$. To prove that $|\Delta_{f',a}|$ is independent of a, it therefore suffices to prove that Γ_f contains the subgroup $\mathbb{F}^*$ of A_f^*, in which case multiplication by ba^{-1} will induce a bijection between $\Delta_{f',a}$ and $\Delta_{f',b}$ for any $b \in \mathbb{F}^*$. Since by hypothesis $\operatorname{tr}\bar\rho(G_{\mathbb{Q},Np}) - \{0\}$ generates $\mathbb{F}^*$, it suffices to show that $\operatorname{tr}\bar\rho(G_{\mathbb{Q},Np}) - \{0\} \subset \Gamma_f$. For this, let $g \in G_{\mathbb{Q},Np}$, and assume that $\operatorname{tr}\bar\rho(g) \neq 0$. By (3.14), one has $t_f(g) \equiv \operatorname{tr}\bar\rho(g) \pmod{\mathfrak{m}_{A_f}}$ where $\mathfrak{m}_{A_f}$ is the maximal ideal of the finite local algebra A_f. Let n be an integer such that $\mathfrak{m}_{A_f}^n = 0$, and let q be the cardinality of $\mathbb{F}$. Then, by Lemma 15,

$$t_f(g^{q^n}) = t_f(g)^{q^n} \equiv (\operatorname{tr}\bar\rho(g))^{q^n} \pmod{\mathfrak{m}_{A_f}^n},$$

so that, since $x \mapsto x^q$ induces the identity on $\mathbb{F}$,

$$t_f(g^{q^n}) = \operatorname{tr}\bar\rho(g).$$

Hence $\operatorname{tr}\bar\rho(g) \in \Gamma_f$ and this completes the proof of the proposition for forms $f \in \mathcal{F}(N, \mathbb{F})_{\bar\rho}$.

Now consider a general nonconstant form $f \in \mathcal{M}(N, \mathbb{F})_{\bar\rho}$. Mimicking the proof in Section 4C, one has

$$\pi(f, a, x) = \sum_{\substack{m \in \mathcal{B} \\ m \le (\log x)^2}} \pi(WU_m f, a, x/m) + O\left(\frac{x}{\log x}\right)$$

and the asymptotic formula obtained for $\pi(WU_m f, a, x/m)$ is independent of $a \in \mathbb{F}^*$, since $WU_m f \in \mathcal{F}(N^2, \mathbb{F})_{\bar\rho}$ and by the result just established. □

Serre has given an example of an eigenform f mod p that does not have the equidistribution property: namely, the form Δ mod 7 (see [Serre 1976, Exercise 12]). Here is a generalization.

Proposition 23. *Suppose f is a nonconstant eigenform in $\mathcal{F}(N, \mathbb{F})_{\bar\rho}$. If the set* $\operatorname{tr}\bar\rho(G_{\mathbb{Q},Np}) - \{0\}$ *does not generate $\mathbb{F}^*$ multiplicatively, then f does not have the equidistribution property.*

Proof. Let $f = \sum_{n=1}^{\infty} a_n q^n$. Since f is an eigenform for the T_ℓ, $\ell \nmid Np$, and also is killed by the U_ℓ for $\ell \mid Np$ (because it is in $\mathcal{F}$), the sequence a_n is multiplicative and one has $a_\ell = 0$ for $\ell \mid Np$ and $a_\ell = \operatorname{tr}\bar\rho(\mathrm{Frob}_\ell)$ for all $\ell \nmid Np$. Also one has $a_1 \ne 0$ since f is nonconstant, and we may assume $a_1 = 1$.

Let B be the proper subgroup of $\mathbb{F}^*$ generated by $\operatorname{tr}\bar\rho(G_{\mathbb{Q},Np}) - \{0\}$. By multiplicativity, $a_n \in B \cup \{0\}$ for all square-free integers m. Since $a_n \ne 0$ for square-free n exactly when n is composed only of primes in $\mathcal{U}_f$, we see that

$$\sum_{\substack{n \le x \\ a_n \in B}} 1 \ge \sum_{\substack{n \le x \\ n \text{ square-free} \\ p \mid n \Rightarrow p \in \mathcal{U}_f}} 1 \sim c \frac{x}{(\log x)^{\alpha(f)}} \tag{16}$$

for a suitable positive constant c. Now if f has the equidistribution property, then, since $|B| \le |\mathbb{F}^* - B|$ for proper subgroups B of $\mathbb{F}^*$, we must have

$$\sum_{\substack{n \le x \\ a_n \in B}} 1 \le (1 + o(1)) \sum_{\substack{n \le x \\ a_n \in \mathbb{F}^* - B}} 1.$$

The right-hand side above is at most the number of integers of the form $mr \le x$ where $1 < m$ is square-full and $r \le x/m$ is square-free with $(r, m) = 1$ and $a_r \ne 0$. Ignoring the condition $(r, m) = 1$, the number of such integers is (arguing as in Section 4C)

$$\le \sum_{\substack{1 < m \le x \\ m \text{ square-full}}} \sum_{\substack{r \le x/m \\ r \text{ square-free} \\ p \mid r \Rightarrow p \in \mathcal{U}_f}} 1 \le \sum_{\substack{1 < m \le (\log x)^2 \\ m \text{ square-full}}} \frac{x}{m} \frac{c + o(1)}{(\log x)^{\alpha(f)}} + \sum_{\substack{m > (\log x)^2 \\ m \text{ square-full}}} \frac{x}{m},$$

which is at most

$$(c+o(1))\frac{x}{(\log x)^{\alpha(f)}}\sum_{\substack{1<m\\ m \text{ square-full}}}\frac{1}{m}=(c+o(1))\frac{x}{(\log x)^{\alpha(f)}}\left(\frac{\zeta(2)\zeta(3)}{\zeta(6)}-1\right)$$
$$=((0.9435\ldots)c+o(1))\frac{x}{(\log x)^{\alpha(f)}}.$$

But this contradicts the lower bound (16), completing our proof. □

We can use the above result to give a converse to Proposition 22 when the level N is equal to 1.

Proposition 24. *Let $\bar\rho \in R(1,\mathbb{F})$. The space $M(1,\mathbb{F})_{\bar\rho}$ has the equidistribution property if and only if the set* $\operatorname{tr}\bar\rho(G_{\mathbb{Q},p})-\{0\}$ *generates $\mathbb{F}^*$ multiplicatively.*

Proof. By (3.15), $M(1,\mathbb{F})_{\bar\rho}$ has an eigenform $f=\sum_{n=1}^{\infty}a_nq^n$ with $a_1=1$ for all the Hecke operators T_ℓ and S_ℓ, $\ell\neq p$. Replacing f by $f-V_pU_pf$ (see (3.11)), we may assume that f is an eigenform in $\mathcal{F}(1,\mathbb{F})_{\bar\rho}$. If $M(1,\mathbb{F})_{\bar\rho}$, hence f, has the equidistribution property, then by the preceding proposition $\operatorname{tr}\bar\rho(G_{\mathbb{Q},p})-\{0\}$ generates $\mathbb{F}^*$ multiplicatively. □

In the same spirit, but concerning forms that are not necessarily generalized eigenforms, one has the following partial result.

Proposition 25. *If 2 is a primitive root modulo p, then $M(N,\mathbb{F}_p)$ has the equidistribution property.*

Proof. One reduces to the case of an $f\in\mathcal{F}(N,p)$ pure exactly as in Section 4B. Then, arguing as in the proof of Proposition 22, it suffices to prove that the group Γ_f generated by $t_f(G_{\mathbb{Q},Np})$ contains $\mathbb{F}_p^*$. But Γ_f contains $t_f(1)=2$ which by hypothesis generates $\mathbb{F}_p^*$. □

Again, one has a partial converse to this proposition.

Proposition 26. *In the case $N=1$ and $p\equiv 3 \pmod 4$, $M(1,\mathbb{F}_p)$ has the equidistribution property if and only if 2 is a primitive root modulo p.*

Proof. Let $\omega_p : G_{\mathbb{Q},p}\to\mathbb{F}_p^*$ be the cyclotomic character modulo p, and define $\bar\rho=1\oplus\omega_p^{(p-1)/2}$. The hypothesis $p\equiv 3 \pmod 4$ means that $(p-1)/2$ is odd, and so $\bar\rho$ is odd and thus belongs to $R(1,p)$ ($\bar\rho$ is the representation attached to the Eisenstein series $E_k(z)$ where $k=1+(p-1)/2$ for $p>3$ and to $E_4(z)$ if $p=3$). Reasoning as in Proposition 24, there is an eigenform f in $\mathcal{F}(1,p)_{\bar\rho}$. If $M(1,p)$, hence f, has the equidistribution property, then $\bar\rho(G_{\mathbb{Q},p})-\{0\}$ generates $\mathbb{F}_p^*$ by Proposition 23. Since the image of $\bar\rho$ is $\{0,2\}$, this implies that 2 is a primitive root modulo p. □

6. A variant: counting square-free integers with nonzero coefficients

Given a modular form $f = \sum_{n=0}^{\infty} a_n q^n$ in $M(N, p)$, let

$$\pi_{\mathrm{sf}}(f, x) = |\{n < x,\ n \text{ square-free},\ a_n \neq 0\}|.$$

Our proof of Theorem 1 allows us to get asymptotics for $\pi_{\mathrm{sf}}(f, x)$, and indeed this is a little simpler than Theorem 1. We state this asymptotic result, and sketch the changes to our proof, omitting details.

Theorem 27. *If there exists a square-free integer n with $a_n \neq 0$, then there exists a positive real constant $c_{\mathrm{sf}}(f) > 0$ such that*

$$\pi_{\mathrm{sf}}(f, x) \sim c_{\mathrm{sf}}(f) \frac{x}{(\log x)^{\alpha(f)}} (\log\log x)^{h(f)}.$$

If $a_n = 0$ for all square-free integers n, then in fact $a_n \neq 0$ only for those integers n that are divisible by ℓ^2 for some prime ℓ dividing Np.

Suppose below that f has some coefficient $a_n \neq 0$ with n not divisible by the square of any prime dividing Np. We first prove Theorem 27 for a pure form $f \in \mathcal{F}(N, p)$, as in Section 4A. In this case, our hypothesis on f is equivalent to saying that f is nonconstant. Then the proof given in Section 4A works by replacing the sets $Z(f)$, $Z(f, a)$ by their intersection $Z_{\mathrm{sf}}(f)$, $Z_{\mathrm{sf}}(f, a)$ with the set of square-free integers. We have a decomposition, analogous to (7) but simpler:

$$Z_{\mathrm{sf}}(f, a) = \coprod_{f', h} Z_{\mathrm{sf}}(f, a;\ f', h), \tag{17}$$

where the disjoint union is taken over forms f' in $Af - \{0\}$ and over integers $0 \leq h \leq h(f)$. Here the set $Z_{\mathrm{sf}}(f, a;\ f', h)$ is defined as the set of integers $n = mm'$ with $(n, Np) = 1$ such that

(6.1) m is square-free and all its prime factors are in $\mathcal{U}_f$;

(6.2) m' is square-free, has exactly h prime factors, and all its prime factors are in $\mathcal{N}_f$, and moreover $f' = T_{m'} f$;

(6.3) $a_m(f') = a$.

The asymptotics for the number of integers less than x in $Z(f, a;\ f', h)$ is then exactly as in Section 4A, except that the set of square-full integers $\mathcal{S}_{f,f''}$ is now $\{1\}$. The desired asymptotics for $\pi_{\mathrm{sf}}(f)$ follows.

The case where f is in $\mathcal{F}(N, \mathbb{F})$ but not necessarily pure is reduced to the pure case exactly as in Section 4B.

Finally, in the general case where $f \in M(N, \mathbb{F})$, let $\mathcal{B}_{\mathrm{sf}}$ be the set of *square-free integers m* whose prime factors all divide Np. We observe that $\mathcal{B}_{\mathrm{sf}}$ is a finite subset of the infinite set $\mathcal{B}$ defined in Section 4C. For $m \in \mathcal{B}_{\text{sf}}$, we define as in Section 4C

$$f_m = \sum_{\substack{n=mm'\\(m',Np)=1}} a_n q^n,$$

and we have clearly

$$\pi_{\text{sf}}(f, x) = \sum_{m \in \mathcal{B}_{\text{sf}}} \pi_{\text{sf}}(f_m, x).$$

By the assumption made on f, at least one of the f_m for $m \in \mathcal{B}_{\text{sf}}$ is nonconstant. The rest of the proof is therefore exactly as in Section 4C.

7. Examples

7A. ***Examples in the case $N = 1$, $p = 3$.*** The simplest case where our theory applies is $N = 1$, $p = 3$. Let us denote by $\Delta = q + 2q^4 + q^7 + q^{13} + \cdots \in \mathbb{F}_3[\![q]\!]$ the reduction modulo 3 of the q-expansion of the usual Δ function. The space $M(1, \mathbb{F}_3)$ is the polynomial algebra in one variable $\mathbb{F}_3[\Delta]$ and $\mathcal{F}(1, \mathbb{F}_3)$ is the subspace of basis (Δ^k) where k runs among positive integers not divisible by 3. The set of Galois representations $R(1, \mathbb{F}_3)$ has only one element, $\bar{\rho} = 1 \oplus \omega_3$ where ω_3 is the cyclotomic character modulo 3. Therefore, every nonzero form $f \in M(1, \mathbb{F}_3)$ is a generalized eigenform, and hence pure. Thus the sets $\mathcal{U}_f$, $\mathcal{N}_f$ are independent of f and are respectively the sets $\mathcal{U}$, $\mathcal{N}$ of prime numbers ℓ congruent to 1, 2 modulo 3; the invariant $\alpha(f)$ is 1/2.

The invariant $h(f)$ is more subtle. Recall from Section 3I that $h(f)$ is the largest integer h such that there exist primes $\ell_1, \ldots, \ell_h$ in $\mathcal{N}_f$ (that is, congruent to 2 mod 3) such that $T_{\ell_1} \cdots T_{\ell_h} f \neq 0$. According to a result of Anna Medvedowski [2015] $h(f)$ is also the largest h such that $T_2^h f \neq 0$. Using this it is easy to compute the value of $h(\Delta^k)$ for small values of k, as shown below (we omit the values of k divisible by 3 since $h(\Delta^{3k}) = h(\Delta^k)$):

f	Δ	Δ^2	Δ^4	Δ^5	Δ^7	Δ^8	Δ^{10}	Δ^{11}	Δ^{13}	Δ^{14}	Δ^{16}	Δ^{17}	Δ^{19}
$h(f)$	0	1	2	3	4	5	4	5	4	5	4	5	6

In general Medvedowski [2015] has shown that $h(\Delta^k) < 4k^{\log 2/\log 3}$. Numerical experiments suggest that $h(\Delta^k)$ is of the order $\sqrt{k}$ for large k with $3 \nmid k$, so there is perhaps some room to improve this upper bound (note $\log 2/\log 3 \approx 0.63$).

Calculation of $\pi(\Delta^2, x)$. The invariant $c(f)$ is the most difficult to determine. We shall calculate $c(\Delta^2)$, illustrating the proof of our theorem in this simplest nontrivial case. To ease notation, set $f = \Delta^2$. The Hecke module Af is a two-dimensional vector space generated by $f = \Delta^2$ and Δ, and the Hecke algebra A_f can be identified with the algebra of dual numbers $\mathbb{F}_3[\epsilon]$, where $\epsilon\Delta^2 = \Delta$ and $\epsilon\Delta = 0$. The value of the operators T_ℓ and ℓS_ℓ in $A_f = \mathbb{F}_3[\epsilon]$ is given by the following table (see [Bellaïche and Khare 2015, §A.3.1]):

$\ell \pmod 9$	$1, 4, 7$	2	5	8
T_ℓ	2	ϵ	2ϵ	0
ℓS_ℓ	1	-1	-1	-1

From this, using (3.3), it is not difficult to compute T_{ℓ^n} for any n:

$\ell \pmod 9$	$1,4,7$			2				5				8	
$n \pmod 6$	$0,3$	$1,4$	$2,5$	$0,2,4$	1	3	5	$0,2,4$	1	3	5	$0,2,4$	$1,3,5$
T_{ℓ^n}	1	2	0	1	ϵ	2ϵ	0	1	2ϵ	ϵ	0	1	0

We are now ready to follow the proof of Theorem 1. Since $f \in \mathcal{F}(1, \mathbb{F}_3)$ and f is pure, only Section 4A is relevant. As in our analysis there, write $f = \sum_{n\geq 1} a_n q^n$ and, for $a = 1, 2 \pmod 3$, let $Z(f, a)$ be the set of integers n such that $a_n = a$. The set $Z(f, a)$ is the disjoint union of sets $Z(f, a;\, f', f'', h)$ as in (7), where f', f'' are in $Af - \{0\}$ and $h \leq h(f) = 1$ is a nonnegative integer. The subsets with $h = 0$ have negligible contribution in view of (8). When $h = 1$, for the set $Z(f, a;\, f', f'', 1)$ to be nonempty one must have $h(f'') = 1$ and $h(f') = 0$. Since f'' and f' must be the image of f by some Hecke operators, this implies, in view of the table above, that f'' is either $2\Delta^2$ or Δ^2 and that f' is either 2Δ or Δ, so we have 4 sets $Z(f, a;\, f', f'', 1)$ to consider for each value 1, 2 of a. As explained in Section 4A, to each permissible choice of f', f'' is attached a set $\mathcal{S}_{f,f''}$ of square-full integers, namely the set of square-full m'' such that $T_{m''} f = f''$, and a multifrobenian set of height 1, that is, a frobenian set, $\mathcal{M}_{f',f''}$, which is the set of primes ℓ in $\mathcal{N}_f$ such that $T_\ell f'' = f'$. For every choice of f'', f', one sees from the table above that $\mathcal{M}_{f',f''}$ is either the set of primes congruent to $2 \pmod 9$ or to $5 \pmod 9$, and in any case $\delta(\mathcal{M}_{f',f''}) = 1/6$. The sets $\mathcal{S}_{f,f''}$ may be easily determined using our table above. Thus $\mathcal{S}_{\Delta^2,\Delta^2}$ consists of square-full numbers where primes $\equiv 2 \pmod 3$ appear in an even exponent, an even number of primes $\equiv 1 \pmod 3$ appear in exponents that are at least 2 and $\equiv 1$ or $4 \pmod 6$, and other primes $\equiv 1 \pmod 3$ appear in exponents that are multiples of 3. The set $\mathcal{S}_{\Delta^2,2\Delta^2}$ consists of square-full numbers that are divisible by an odd number of primes $\equiv 1 \pmod 3$ appearing in exponents at least 2 and $\equiv 1$ or $4 \pmod 6$, other primes $\equiv 1 \pmod 3$ appearing in exponents that are multiples of 3, and primes $\equiv 2 \pmod 3$ appearing in even exponents.

According to Theorem 7, for $a = 1$ or 2, $f' = \Delta$ or 2Δ, and $f'' = \Delta^2$ or $2\Delta^2$, one has

$$|\{n < x : n \in Z(f, a;\, f', f'', 1)\}| \sim \Bigg(\sum_{s\in\mathcal{S}_{f,f''}} \frac{C(\mathcal{U}, s)}{s}\Bigg)\left(\frac{1}{6}\right)\left(\frac{1}{2}\right)\frac{x}{(\log x)^{\frac{1}{2}}} \log\log x, \tag{18}$$

where

$$C(\mathcal{U}, s) = C(\mathcal{U}) \prod_{\substack{\ell \mid s \\ \ell \equiv 1 \pmod 3}} \left(1 + \frac{1}{\ell}\right)^{-1}$$

and

$$\begin{aligned} C(\mathcal{U}) &= \frac{1}{\Gamma(\frac{1}{2})} \prod_{p \equiv 1 \pmod 3} \left(1 + \frac{1}{p}\right)\left(1 - \frac{1}{p}\right)^{\frac{1}{2}} \prod_{p \not\equiv 1 \pmod 3} \left(1 - \frac{1}{p}\right)^{\frac{1}{2}} \\ &= \frac{\sqrt[4]{3}}{\pi\sqrt{2}} \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}} = 0.2913\ldots. \end{aligned} \tag{19}$$

In (18), the factor $1/6$ is $\delta(\mathcal{M}_{f'', f'})$ and the factor $1/2$ is $|\Delta|/|\Gamma|$ (and this factor would disappear if we counted cases $a = 1$ and $a = 2$ together).

Adding up all the possibilities, using (7), we finally obtain that

$$\pi(\Delta^2, x) \sim c(\Delta^2) \frac{x}{(\log x)^{\frac{1}{2}}} \log\log x,$$

where

$$c(\Delta^2) = \frac{1}{3} \sum_{s \in \mathcal{S}_{f,f} \cup \mathcal{S}_{f,2f}} \frac{C(\mathcal{U}, s)}{s} = \frac{C(\mathcal{U})}{3} \prod_{\ell \equiv 1 \pmod 3} \left(1 - \frac{1}{\ell^3}\right)^{-1} \prod_{\ell \equiv 2 \pmod 3} \left(1 - \frac{1}{\ell^2}\right)^{-1}.$$

Calculation of $\pi_{\mathrm{sf}}(\Delta^k, x)$ *for* $k = 1, 2, 4, 5, 7, 10$. In these examples, we describe the calculation of $c_{\mathrm{sf}}(\Delta^k)$, which is simpler than evaluating $c(\Delta^k)$. For $h \ge 0$ an integer, let $\mathcal{M}_h$ be the set of integers that are the product of exactly h distinct primes, all congruent to 2 or 5 modulo 9. This is a multifrobenian set, attached to the cyclotomic extension $\mathbb{Q}(\mu_9)/\mathbb{Q}$ of the Galois group $G = (\mathbb{Z}/9\mathbb{Z})^*$, and one has $\delta(\mathcal{M}_h) = 2^h/(h!6^h) = 1/(h!3^h)$. One can show that, for $k = 1, 2, 4, 5, 7, 10$ and $h = h(\Delta^k) = 0, 1, 2, 3, 4, 4$ respectively, and for $m' \in \mathcal{M}_h$, one has (with $f = \Delta^k$) that $T_{m'} f \neq 0$, and in fact $T_{m'} f = \Delta$ or $T_{m'} f = 2\Delta$. Also note that for $f' = \Delta$ or $f' = 2\Delta$, one also has $T_m f' = \Delta$ or 2Δ for any square-free m with prime factors in $\mathcal{U}$, so that $a_m(f') \neq 0$.

Thus, the main contribution to $Z_{\mathrm{sf}}(\Delta^k)$ is the set we call $\mathcal{Z}(\mathcal{U}, \mathcal{M}_h, 1)$, namely the set of all square-free numbers mm', where m is any product of primes in $\mathcal{U}$ (i.e., congruent to $1 \pmod 3$) and $m' \in \mathcal{M}_h$. According to Theorem 6,

$$\pi_{\mathrm{sf}}(\Delta^k, x) \sim \frac{C(\mathcal{U})}{h!3^h} \frac{x}{(\log x)^{1/2}} (\log\log x)^h, \quad k = 1, 2, 4, 5, 7, 10,$$

where $h = h(k) = 0, 1, 2, 3, 4, 4$ respectively and $C(\mathcal{U})$ is the constant appearing in (19).

7B. ***Example of a nonpure form in the case $N = 1$, $p = 7$.*** Examples of powers of Δ that are not pure arise (mod 7). There one has $\Delta^2 = f + \Delta$, where $f = \Delta^2 - \Delta$ is an eigenform for all the Hecke operators T_ℓ (ℓ a prime number with $\ell \neq 7$), with eigenvalue $\ell^2 + \ell^3$. The Galois representation $\bar\rho_f$ corresponding to this system is $\omega_7^2 \oplus \omega_7^3$ where ω_7 is the cyclotomic character modulo 7. The set $\mathcal{N}_{\bar\rho_f}$ is the set of prime numbers ℓ that are congruent to -1 modulo 7, and $\mathcal{U}_{\bar\rho_f}$ is the set of prime numbers congruent to $1, 2, 3, 4, 5$ modulo 7. One has $\alpha(f) = \alpha(\bar\rho_f) = 1/6$.

The form Δ is also of course an eigenform, with system of eigenvalues $\ell + \ell^4$ for T_ℓ, corresponding to the Galois representation $\bar\rho_\Delta = \omega_7 \oplus \omega_7^4$ with $\alpha(\bar\rho_\Delta) = 1/2$.

The decomposition $\Delta^2 = f + \Delta$ is thus the canonical decomposition into pure forms, and the pure form Δ can be neglected because $\alpha(\Delta) > \alpha(f)$. One finds

$$\pi_{\mathrm{sf}}(\Delta^2, x) \sim \pi_{\mathrm{sf}}(f, x) \sim C(\mathcal{U}_{\bar\rho_f}) \frac{x}{(\log x)^{1/6}}$$

with

$$C(\mathcal{U}_{\bar\rho_f}) = \frac{1}{\Gamma(5/6)} \prod_{\ell \equiv 1,2,3,4,5 \pmod 7} \left(1 + \frac{1}{\ell}\right)\left(1 - \frac{1}{\ell}\right)^{\frac{5}{6}} \prod_{\ell \equiv -1,0 \pmod 7} \left(1 - \frac{1}{\ell}\right)^{\frac{5}{6}}$$

so that

$$\pi_{\mathrm{sf}}(\Delta^2, x) \sim c_{\mathrm{sf}}(\Delta^2) \frac{x}{(\log x)^{1/6}}, \quad c_{\mathrm{sf}}(\Delta^2) = C(\mathcal{U}_{\bar\rho_f}) = 0.5976\ldots.$$

Acknowledgement

We are grateful to the referee for a very careful reading of the paper.

References

[Ahlgren 1999] S. Ahlgren, "Non-vanishing of the partition function modulo odd primes l", *Mathematika* **46**:1 (1999), 185–192. MR 2001h:11133 Zbl 0993.11053

[Bellaïche and Khare 2015] J. Bellaïche and C. Khare, "Level 1 Hecke algebras of modular forms modulo p", *Compos. Math.* **151**:3 (2015), 397–415. MR 3320566 Zbl 06434557

[Bellaïche and Nicolas 2015] J. Bellaïche and J.-L. Nicolas, "Parité des coefficients de formes modulaires", *The Ramanujan Journal* (2015), 1–44.

[Chen 2012] S.-C. Chen, "Distribution of the coefficients of modular forms and the partition function", *Arch. Math.* (*Basel*) **98**:4 (2012), 307–315. MR 2914347 Zbl 1276.11168

[Chenevier 2014] G. Chenevier, "The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings", pp. 221–285 in *Automorphic Forms and Galois Representations* (Durham, NC, 2011), vol. 1, edited by F. Diamond et al., London Mathematical Society Lecture Note Series **414**, Cambridge Univ. Press, 2014.

[Diamond and Im 1995] F. Diamond and J. Im, "Modular forms and modular curves", pp. 39–133 in *Seminar on Fermat's Last Theorem* (Toronto, 1993–1994), edited by V. K. Murty, CMS Conf. Proc. **17**, Amer. Math. Soc., Providence, RI, 1995. MR 97g:11044 Zbl 0853.11032

[Faber 2012] X. Faber, "Finite p-irregular subgroups of $\mathrm{PGL}_2(k)$", preprint, 2012. arXiv 1112.1999v2

[Ghitza 2006] A. Ghitza, "All Siegel Hecke eigensystems (mod p) are cuspidal", *Math. Res. Lett.* **13**:5-6 (2006), 813–823. MR 2008a:11053 Zbl 1185.11032

[Gouvêa 1988] F. Q. Gouvêa, *Arithmetic of p-adic modular forms*, Lecture Notes in Mathematics **1304**, Springer, Berlin, 1988. MR 91e:11056 Zbl 0641.10024

[Gross 1990] B. H. Gross, "A tameness criterion for Galois representations associated to modular forms (mod p)", *Duke Math. J.* **61**:2 (1990), 445–517. MR 91i:11060 Zbl 0743.11030

[Jochnowitz 1982] N. Jochnowitz, "Congruences between systems of eigenvalues of modular forms", *Trans. Amer. Math. Soc.* **270**:1 (1982), 269–285. MR 83e:10033b Zbl 0536.10022

[Katz 1973] N. M. Katz, "p-adic properties of modular schemes and modular forms", pp. 69–190. Lecture Notes in Mathematics, Vol. 350 in *Modular functions of one variable, III* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), edited by W. Kuyk and J.-P. Serre, Springer, Berlin, 1973. MR 56 #5434 Zbl 0271.10033

[Katz 1975] N. M. Katz, "Higher congruences between modular forms", *Ann. of Math.* (2) **101** (1975), 332–367. MR 54 #5120 Zbl 0356.10020

[Medvedovki 2015] A. Medvedovki, *Lower bounds on dimensions of mod-p Hecke algebras: the nilpotence method*, Ph.D. thesis, Brandeis University, 2015, http://people.brandeis.edu/~medved/Data/DissertationMedvedovsky.pdf.

[Miyake 2006] T. Miyake, *Modular forms*, 2nd ed., Springer, Berlin, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda. MR 2006g:11084 Zbl 1159.11014

[Nicolas and Serre 2012a] J.-L. Nicolas and J.-P. Serre, "Formes modulaires modulo 2: l'ordre de nilpotence des opérateurs de Hecke", *C. R. Math. Acad. Sci. Paris* **350**:7-8 (2012), 343–348. MR 2922080 Zbl 1275.11073

[Nicolas and Serre 2012b] J.-L. Nicolas and J.-P. Serre, "Formes modulaires modulo 2: structure de l'algèbre de Hecke", *C. R. Math. Acad. Sci. Paris* **350**:9-10 (2012), 449–454. MR 2929047 Zbl 1275.11074

[Serre 1973] J.-P. Serre, "Congruences et formes modulaires", *Séminaire Bourbaki* **14**:416 (1973), 319–338. Zbl 0276.14013

[Serre 1976] J.-P. Serre, "Divisibilité de certaines fonctions arithmétiques", *Enseignement Math.* (2) **22**:3-4 (1976), 227–260. MR 55 #7958 Zbl 0355.10021

[Serre 2012] J.-P. Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics **11**, CRC Press, Boca Raton, FL, 2012. MR 2920749 Zbl 1238.11001

[Tenenbaum 1995] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 2nd ed., Cours Spécialisés [Specialized Courses] **1**, Société Mathématique de France, Paris, 1995. MR 97e:11005a Zbl 0880.11001

Communicated by Barry Mazur
Received 2014-10-29 Revised 2015-07-05 Accepted 2015-08-03

jbellaic@brandeis.edu *Department of Mathematics, Brandeis University, 415 South Street, Waltham, MA 02453, United States*

ksound@math.stanford.edu *Department of Mathematics, Stanford University, 450 Serra Mall, Building 380, Stanford, CA 94305-2125, United States*

ALGEBRA AND NUMBER THEORY 9:8 (2015)
dx.doi.org/10.2140/ant.2015.9.1857

Noetherianity for infinite-dimensional toric varieties

Jan Draisma, Rob Eggermont, Robert Krone and Anton Leykin

We consider a large class of monomial maps respecting an action of the infinite symmetric group, and prove that the toric ideals arising as their kernels are finitely generated up to symmetry. Our class includes many important examples where Noetherianity was recently proved or conjectured. In particular, our results imply Hillar–Sullivant's independent set theorem and settle several finiteness conjectures due to Aschenbrenner, Martín del Campo, Hillar, and Sullivant.

We introduce a *matching monoid* and show that its monoid ring is Noetherian up to symmetry. Our approach is then to factorize a more general equivariant monomial map into two parts going through this monoid. The kernels of both parts are finitely generated up to symmetry: recent work by Yamaguchi–Ogawa–Takemura on the (generalized) Birkhoff model provides an explicit degree bound for the kernel of the first part, while for the second part the finiteness follows from the Noetherianity of the matching monoid ring.

1. Introduction and main result

Families of algebraic varieties parameterized by combinatorial data arise in various areas of mathematics, such as statistics (e.g., phylogenetic models parameterized by trees [Allman and Rhodes 2008; Draisma and Kuttler 2009; Draisma and Eggermont 2015; Pachter and Sturmfels 2005] or the relations among path probabilities in Markov chains parameterized by path length [Haws et al. 2014; Norén 2015]), commutative algebra (e.g., Segre powers of a fixed vector space parameterized by the exponent [Snowden 2013] or Laurent lattice ideals [Hillar and Martín del Campo 2013]), and combinatorics (e.g., algebraic matroids arising from determinantal ideals parameterized by matrix sizes [Kiraly and Rosen 2013] or edge ideals of hypergraphs parameterized by the number of vertices [Gross and Petrović 2013]).

Draisma and Eggermont are supported by a Vidi grant from the Netherlands Organisation for Scientific Research (NWO) .
Krone and Leykin are supported in part by the NSF under grant DMS 1151297.
MSC2010: primary 13E05; secondary 13P10, 14M25.
Keywords: Noetherianity up to symmetry, binomial ideals.

A natural question is whether such families *stabilize* as some of the combinatorial data tend to infinity. A recently established technique for proving such stabilization is passing to an infinite-dimensional limit of the family, giving some equations for that limit, and showing that those equations cut out a suitably Noetherian space. This then implies that the limit itself is given by finitely many further equations, and that the family stabilizes. This technique is applied, for instance, in the proof of the independent set theorem [Hillar and Sullivant 2012], and in the first author's work on the Gaussian k-factor model, chirality varieties, and tensors of bounded rank [Draisma 2010; Draisma and Kuttler 2014].

In the present paper, we follow a similar approach, utilizing the new concept of a *matching monoid* to prove that stabilization happens for a large class of toric varieties. Our main theorem provides one-step proofs for several existing results that were established in a rather less general context; and it settles conjectures and questions from [Aschenbrenner and Hillar 2007; Hillar and Sullivant 2012; Hillar and Martín del Campo 2013]. There is a list of three such consequences at the end of this Introduction. Moreover, we show Noetherianity in a constructive manner by complementing the main theorem with an algorithm that produces a finite set of equations whose orbits define the infinite-dimensional toric variety under consideration.

Instead of working with inverse systems of affine varieties, we work directly with direct limits of their coordinate rings. In fact, we formulate our main theorem directly in the infinite-dimensional setting, as going back to families of finite-dimensional coordinate rings of toric varieties is fairly straightforward. Throughout, $\mathbb{N}$ denotes $\{0, 1, 2, 3, \ldots\}$, and for $k \in \mathbb{N}$ we write $[k] := \{0, \ldots, k-1\}$. We write $\mathrm{Sym}(\mathbb{N})$ for the group of all bijections $\mathbb{N} \to \mathbb{N}$, and $\mathrm{Inc}(\mathbb{N})$ for the monoid of all strictly increasing maps $\mathbb{N} \to \mathbb{N}$. Let Y be a set equipped with an action of $\mathrm{Sym}(\mathbb{N})$. We require that the action has the following property: for each $y \in Y$ there exists a $k_y \in \mathbb{N}$ such that y is fixed by all of $\mathrm{Sym}(\mathbb{N} \setminus [k_y])$, i.e., by all elements of $\mathrm{Sym}(\mathbb{N})$ that fix $[k_y]$ elementwise. In this setting, $\mathrm{Inc}(\mathbb{N})$ also acts on Y, as follows: for $\pi \in \mathrm{Inc}(\mathbb{N})$ and $y \in Y$, choose a $\pi' \in \mathrm{Sym}(\mathbb{N})$ that agrees with π on $[k_y]$, set $\pi y := \pi' y$, and observe that this does not depend on the choice of π'. Observe that for each $y \in Y$ the $\mathrm{Inc}(\mathbb{N})$-orbit $\mathrm{Inc}(\mathbb{N})y$ is contained in $\mathrm{Sym}(\mathbb{N})y$, and that the latter is in fact equal to the orbit of y under the countable subgroup of $\mathrm{Sym}(\mathbb{N})$ consisting of permutations fixing all but finitely many natural numbers. See also [Hillar and Sullivant 2012, Section 5].

Let R be a Noetherian ring (commutative, with 1), and let $R[Y]$ be the commutative R-algebra of polynomials in which the elements of Y are the variables and the coefficients come from R. The group $\mathrm{Sym}(\mathbb{N})$ acts by R-algebra automorphisms on $R[Y]$ by permuting the variables. Furthermore, let k be a natural number, and let $Z = \{z_{ij} \mid i \in [k], j \in \mathbb{N}\}$ be a second set of variables, with a $\mathrm{Sym}(\mathbb{N})$-action given by $\pi z_{ij} = z_{i\pi(j)}$. Extend this action to an action by R-algebra automorphisms of $R[Z]$. Note that the $\mathrm{Sym}(\mathbb{N})$-actions on $R[Y]$, Z, and $R[Z]$ all have the property required of the action on Y. Hence they also yield $\mathrm{Inc}(\mathbb{N})$-actions, by means of injective R-algebra endomorphisms in the case of $R[Y]$ and $R[Z]$. In general, when a monoid Π acts on a ring S by means of endomorphisms, S is called Π-*Noetherian* if every Π-stable ideal in S is generated by the union of finitely many Π-orbits of elements, i.e., if S is Noetherian as a module under the *skew monoid ring* $S * \Pi$; see [Hillar and Sullivant 2012].

Theorem 1.1 (main theorem). *Assume that* $\mathrm{Sym}(\mathbb{N})$ *has only finitely many orbits on* Y. *Let* $\varphi : R[Y] \to R[Z]$ *be a* $\mathrm{Sym}(\mathbb{N})$*-equivariant homomorphism that maps each* $y \in Y$ *to a* monomial *in the* z_{ij}. *Then* $\ker \varphi$ *is generated by finitely many* $\mathrm{Inc}(\mathbb{N})$*-orbits of binomials*, *and* $\mathrm{im}\, \varphi \cong R[Y]/\ker \varphi$ *is an* $\mathrm{Inc}(\mathbb{N})$*-Noetherian ring.*

If an ideal is $\mathrm{Sym}(\mathbb{N})$-stable, then it is certainly $\mathrm{Inc}(\mathbb{N})$-stable, so the last statement implies that $R[Y]/\ker \varphi$ is $\mathrm{Sym}(\mathbb{N})$-Noetherian. The conditions in the theorem are sharp in the following senses.

(1) The ring $R[Y]$ itself is typically *not* $\mathrm{Sym}(\mathbb{N})$-Noetherian, let alone $\mathrm{Inc}(\mathbb{N})$-Noetherian. Take, for instance, $Y = \{y_{ij} \mid i, j \in \mathbb{N}\}$ with $\mathrm{Sym}(\mathbb{N})$ acting diagonally on both indices, and take any R with $1 \neq 0$. Then the $\mathrm{Sym}(\mathbb{N})$-orbits of the monomials

$$y_{12}y_{21},\ y_{12}y_{23}y_{31},\ y_{12}y_{23}y_{34}y_{41},\ \ldots$$

generate a $\mathrm{Sym}(\mathbb{N})$-stable ideal that is not generated by any finite union of orbits (see [Aschenbrenner and Hillar 2007, Proposition 5.2]).

(2) The R-algebra $R[Z]$ is $\mathrm{Sym}(\mathbb{N})$-Noetherian, and even $\mathrm{Inc}(\mathbb{N})$-Noetherian [Cohen 1987; Hillar and Sullivant 2012] — this is the special case of our theorem where $Y = Z$ and φ is the identity — but $\mathrm{Sym}(\mathbb{N})$-stable subalgebras of $R[Z]$ need not be, even when generated by finitely many $\mathrm{Sym}(\mathbb{N})$-orbits of polynomials. For instance, an (as yet) unpublished theorem due to Krasilnikov says that in characteristic 2, the ring generated by all 2×2-minors of a $2 \times \mathbb{N}$-matrix of variables is not $\mathrm{Sym}(\mathbb{N})$-Noetherian. Put differently, we do not know if the finite-generatedness of $\ker \varphi$ in the main theorem continues to hold if φ is an arbitrary $\mathrm{Sym}(\mathbb{N})$-equivariant homomorphism, but certainly the quotient is not, in general, $\mathrm{Sym}(\mathbb{N})$-Noetherian.

(3) Moreover, subalgebras of $R[Z]$ generated by finitely many $\mathrm{Inc}(\mathbb{N})$-orbits of *monomials* need not be $\mathrm{Inc}(\mathbb{N})$-Noetherian; see Krasilnikov's example in [Hillar and Sullivant 2012]. However, our main theorem implies that subalgebras of $R[Z]$ generated by finitely many $\mathrm{Sym}(\mathbb{N})$-orbits of monomials *are* $\mathrm{Inc}(\mathbb{N})$-Noetherian.

Our main theorem applies to many problems on Markov bases of families of point sets. In such applications, the following strengthening is sometimes useful.

Corollary 1.2. *Assume that* $\mathrm{Sym}(\mathbb{N})$ *has only finitely many orbits on* Y, *and let* S *be an* R*-algebra with trivial* $\mathrm{Sym}(\mathbb{N})$*-action. Let* $\varphi : R[Y] \to S[Z]$ *be a* $\mathrm{Sym}(\mathbb{N})$*-equivariant* R*-algebra homomorphism that maps each* $y \in Y$ *to an element of* S *times a monomial in the* z_{ij}. *Then* $\ker \varphi$ *is generated by finitely many* $\mathrm{Inc}(\mathbb{N})$*-orbits of binomials*, *and* $\operatorname{im} \varphi \cong R[Y]/\ker \varphi$ *is an* $\mathrm{Inc}(\mathbb{N})$*-Noetherian ring.*

Proof of the corollary given the main theorem. Let y_p, $p \in [N]$ be representatives of the $\mathrm{Sym}(\mathbb{N})$-orbits on Y. Then for all $p \in [N]$ and $\pi \in \mathrm{Sym}(\mathbb{N})$ we have $\varphi(\pi y_p) = s_p \pi u_p$ for some monomial u_p in the z_{ij} and some s_p in S. Apply the main theorem to $Y' := Y \times \mathbb{N}$ and $Z \cup Z'$ with $Z' := \{z'_{p,j} \mid p \in [N], j \in \mathbb{N}\}$ and φ' the map that sends the variable $(\pi y_p, j)$ to $z'_{p,j} \pi u_p$. Consider the commutative diagram

$$\begin{array}{ccc} R[Y'] & \xrightarrow{\ \varphi'\ } & R[Z \cup Z'] \\ \Big\downarrow{\scriptstyle \rho:(y,j)\mapsto y} & & \Big\downarrow{\scriptstyle \psi: z'_{pj} \mapsto s_p} \\ R[Y] & \xrightarrow{\ \varphi\ } & S[Z] \end{array}$$

of $\mathrm{Sym}(\mathbb{N})$-equivariant R-algebra homomorphisms. By the main theorem, $\operatorname{im} \varphi'$ is $\mathrm{Inc}(\mathbb{N})$-Noetherian, hence so is its image under ψ; and this image equals $\operatorname{im} \varphi$ because ρ is surjective. Similarly, $\ker(\psi \circ \varphi')$ is generated by finitely many $\mathrm{Inc}(\mathbb{N})$-orbits (because this is the case for both $\ker \varphi'$ and $\ker \psi|_{\operatorname{im} \varphi'}$), hence so is its image under ρ; and this image is $\ker \varphi$ because ρ is surjective. □

Here are some consequences of our main theorem.

(1) Our main theorem implies [Aschenbrenner and Hillar 2007, Conjecture 5.10], to the effect that chains of ideals arising as kernels of monomial maps of the form $y_{i_1,\dots,i_k} \mapsto z_{i_1}^{a_1} \cdots z_{i_k}^{a_k}$, where the indices $i_1, \dots, i_k$ are required to be distinct, stabilize. Aschenbrenner and Hillar proved this in the squarefree case, where the a_j are equal to 1. In the Laurent polynomial setting more is known [Hillar and Martín del Campo 2013].

(2) A consequence of [de Loera et al. 1995] is that for any $n \geq 4$ the vertex set $\{v_{ij} := e_i + e_j \mid i \neq j\} \subseteq \mathbb{R}^n$ of the $(n-1)$-dimensional second hypersimplex has a Markov basis corresponding to the relations $v_{ij} = v_{ji}$ and $v_{ij} + v_{kl} = v_{il} + v_{kj}$. Here is a qualitative generalization of this fact. Let m and k be fixed natural numbers. For every $n \in \mathbb{N}$ consider a finite set $P_n \subseteq \mathbb{Z}^m \times \mathbb{Z}^{k \times n}$. Let $\mathrm{Sym}(n)$ act trivially on $\mathbb{Z}^m$ and by permuting columns on $\mathbb{Z}^{k \times n}$. Assume that there exists an n_0 such that $\mathrm{Sym}(n) P_{n_0} = P_n$ for $n \geq n_0$; here we think of $\mathbb{Z}^{k \times n_0}$ as the subset of $\mathbb{Z}^{k \times n}$ where the last $n - n_0$ columns are zero. Then Corollary 1.2 implies that there exists an n_1 such that for any Markov basis M_{n_1} for the relations among the points in P_{n_1}, $\mathrm{Sym}(n) M_{n_1}$ is a Markov basis for P_n for all $n \geq n_1$. For the second hypersimplex, n_0 equals 2 and n_1 equals 4.

(3) A special case of the previous consequence is the independent set theorem of [Hillar and Sullivant 2012]. We briefly illustrate how to derive it directly from Corollary 1.2. Let m be a natural number and let $\mathcal{F}$ be a family of subsets of a finite set $[m]$. Let T be a subset of $[m]$ and assume that each $F \in \mathcal{F}$ contains at most one element of T. In other words, T is an independent set in the hypergraph determined by $\mathcal{F}$. For $t \in [m]\setminus T$ let r_t be a natural number. Set $Y := \{y_\alpha \mid \alpha \in \mathbb{N}^T \times \prod_{t\in[m]\setminus T}[r_t]\}$ and $Z := \{z_{F,\alpha} \mid F \in \mathcal{F}, \alpha \in \mathbb{N}^{F\cap T} \times \prod_{F\setminus T}[r_t]\}$, and let φ be the homomorphism $\mathbb{Z}[Y] \to \mathbb{Z}[Z]$ that maps y_α to $\prod_{F\in\mathcal{F}} z_{F,\alpha|_F}$, where $\alpha|_F$ is the restriction of α from $[m]$ to F. Then φ is equivariant with respect to the action of $\operatorname{Sym}(\mathbb{N})$ on the variables induced by the diagonal action of $\operatorname{Sym}(\mathbb{N})$ on $\mathbb{N}^T$, and (a strong form of) the independent set theorem boils down to the statement that $\ker\varphi$ is generated by finitely many $\operatorname{Sym}(\mathbb{N})$-orbits of binomials. By the condition that T is an independent set, each z-variable has at most one index running through all of $\mathbb{N}$. Setting S to be $\mathbb{Z}[z_{F,\alpha} \mid F \cap T = \varnothing]$, we find that Y, S, the remaining $z_{F,\alpha}$-variables, with $|F \cap T| = 1$, and the map φ satisfy the conditions of the corollary. The conclusion of the corollary now implies the independent set theorem.

The remainder of the paper is organized as follows: In Section 2 we reduce the main theorem to a particular class of maps φ related to *matching monoids* of complete bipartite graphs. For these maps, finite generation of the kernel follows from recent results on the Birkhoff model [Yamaguchi et al. 2014]; see Section 3, where we also describe the image of φ. In Section 4 we prove Noetherianity of $\operatorname{im}\varphi$, still for our special φ. As in [Cohen 1987; Hillar and Sullivant 2012], the strategy in Section 4 is to prove that a partial order on certain monoids is a well-partial-order. In our case, these are said to be matching monoids, and the proof that they are well-partially ordered is quite subtle. In Section 5 we establish that a finite $\operatorname{Inc}(\mathbb{N})$-generating set of $\ker\varphi$ is (at least theoretically) computable. The last section describes a simpler *procedure* that one can attempt in order to obtain a generating set; at the moment, we do not know if this procedure is guaranteed to terminate. We conclude the paper with a computational example for which termination does occur.

2. Reduction to matching monoids

In this section we reduce the main theorem to a special case to be treated in the next two sections. To formulate this special case, let $N \in \mathbb{N}$ and for each $p \in [N]$ let $k_p \in \mathbb{N}$. First, introduce a set Y' of variables $y'_{p,J}$ where $p \in [N]$ and $J = (j_l)_{l\in[k_p]} \in \mathbb{N}^{[k_p]}$ is a k_p-tuple of *distinct* natural numbers. The group $\operatorname{Sym}(\mathbb{N})$ acts on Y' by $\pi y'_{p,J} = y'_{p,\pi(J)}$ where $\pi(J) = (\pi(j_l))_{l\in[k_p]}$. This action has finitely many orbits and satisfies the condition preceding the main theorem.

Second, let X be a set of variables $x_{p,l,j}$ with $p \in [N], l \in [k_p], j \in \mathbb{N}$ and let $\mathrm{Sym}(\mathbb{N})$ act on X by its action on the last index.

Proposition 2.1. *Let $\varphi' : R[Y'] \to R[X]$ be the R-algebra homomorphism sending $y'_{p,J}$ to $\prod_{l\in[k_p]} x_{p,l,j_l}$. Then the main theorem implies that $\ker\varphi'$ is generated by finitely many $\mathrm{Inc}(\mathbb{N})$-orbits of binomials, and that $\mathrm{im}\,\varphi'$ is an $\mathrm{Inc}(\mathbb{N})$-Noetherian ring. Conversely, if these two statements hold for all choices of $N, k_1, \dots, k_N \in \mathbb{N}$, then the main theorem holds.*

Proof. The first statement is immediate — note that the pair (p,l) comprising the first two indices of the variables $x_{p,l,j}$ takes on finitely many, namely $\sum_p k_p$, values.

For the second statement, consider a monomial map $\varphi : R[Y] \to R[Z]$ with $Z = \{z_{i,j} \mid i \in [k], j \in \mathbb{N}\}$ as in the main theorem. Let N be the number of $\mathrm{Sym}(\mathbb{N})$-orbits on Y and let $y_p,\ p \in [N]$ be representatives of the orbits. Set $k_p := k_{y_p}$ for $p \in [N]$, so that πy_p depends only on the restriction of $\pi \in \mathrm{Sym}(\mathbb{N})$ to $[k_p]$. We have thus determined the values of N and the k_p, and we let Y', X be as above.

Let $\psi : R[Y'] \to R[Y]$ be the R-algebra homomorphism defined by sending $y'_{p,J}$ to πy_p for any $\pi \in \mathrm{Sym}(\mathbb{N})$ satisfying $\pi(l) = j_l,\ l \in [k_p]$. This homomorphism is $\mathrm{Sym}(\mathbb{N})$-equivariant. The composition $\varphi'' := \varphi \circ \psi : R[Y'] \to R[Z]$ satisfies the conditions of the main theorem. Since ψ is surjective, it maps any generating set for $\ker\varphi''$ onto a generating set for $\ker\varphi$; moreover, we have $\mathrm{im}\,\varphi'' = \mathrm{im}\,\varphi$. Hence the conclusions of the main theorem for φ'' imply those for φ.

Next write $\varphi''(y_{p,J}) = \prod_{i\in[k], j\in\mathbb{N}} z_{i,j}^{d_{p,i,j}}$. Observe that $d_{p,i,j} = 0$ whenever $j \notin J$, using the fact that any permutation that fixes J also fixes $y_{p,J}$, and hence must also fix $\varphi''(y_{p,J})$ by $\mathrm{Sym}(\mathbb{N})$-equivariance. Now let $\varphi' : K[Y'] \to K[X]$ be as above and define $\rho : R[X] \to R[Z]$ by $\rho(x_{p,l,j}) = \prod_{i\in[k]} z_{i,j}^{d_{p,i,j}}$. By construction, we have $\rho \circ \varphi' = \varphi''$.

Now $\mathrm{im}\,\varphi''$ is a quotient of $\mathrm{im}\,\varphi'$ and $\ker\varphi''$ is generated by $\ker\varphi'$ together with preimages of generators of $\ker(\rho|_{\mathrm{im}\,\varphi'})$, hence the conclusions of the main theorem for φ' imply those for φ'', as desired. □

In what follows, we will drop the accents on the y-variables and write Y for the set of variables $y_{p,J}$, X for the set of variables $x_{p,l,j}$, and φ for the R-algebra homomorphism

$$\varphi : R[Y] \to R[X],\ y_{p,J} \mapsto \prod_{l\in[k_p]} x_{p,l,j_l}. \tag{1}$$

Monomials in the $x_{p,l,j}$ will be denoted x^A where $A \in \prod_{p\in[N]} \mathbb{N}^{[k_p]\times\mathbb{N}}$ is an $[N]$-tuple of finite-by-infinite matrices A_p. Note that $\varphi(y_{p,J})$ equals x^A where only the p-th component A_p of A is nonzero and in fact has all row sums equal to 1, all column sums labeled by J equal to 1, and all other column sums equal to 0. Thus A_p can be thought of as the adjacency matrix of a matching of the maximal size k_p

in the complete bipartite graph with bipartition $[k_p] \sqcup \mathbb{N}$. Thus the monomials in $\operatorname{im}\varphi$ form the abelian monoid generated by such matchings (with p varying). We call a monoid like this a *matching monoid*. In the next section we characterize these monomials among all monomials in the $x_{p,l,j}$, and find a bound on the relations among the $\varphi(y_{p,J})$.

3. Relations among matchings

We retain the setting at the end of the previous section: Y is the set of variables $y_{p,J}$ with p running through $[N]$ and $J \in \mathbb{N}^{[k_p]}$ running through the $[k_p]$-tuples of *distinct* natural numbers; X is the set of variables $x_{p,l,j}$ with $p \in [N]$, $l \in [k_p]$, $j \in \mathbb{N}$, and φ is the map in (1). In this section we describe both the kernel and the image of φ. Note that if some k_p is zero, then the corresponding (single) variable $y_{p,()}$ is mapped by φ to 1. The image of φ does not change if we disregard those p, and the kernel changes only in that we forget about the generators $y_{p,()} - 1$. Hence we may and will assume that all k_p are strictly positive. The following lemma gives a complete characterization of the x^A in the image of φ.

Proposition 3.1. *For an $[N]$-tuple $A \in \prod_{p\in[N]} \mathbb{N}^{[k_p]\times\mathbb{N}}$ the monomial x^A lies in the image of φ if and only if for all $p \in [N]$ the matrix $A_p \in \mathbb{N}^{[k_p]\times\mathbb{N}}$ has all row sums equal to a number $d_p \in \mathbb{N}$ and all column sums less than or equal to d_p.*

We call such A *good*. Note that d_p is unique since all k_p are strictly positive. We call the vector $(d_p)_p$ the *multidegree* of A and of x^A.

Remark 3.2. By replacing $\mathbb{N}$ with $[n]$ for some natural number n greater than or equal to the maximum of the k_p, the proposition boils down to the statement that for each p the lattice polytope in $\mathbb{R}^{[k_p]\times[n]}$ with defining inequalities $\forall_{ij} a_{ij} \geq 0$, $\forall_i \sum_j a_{ij} = 1$, and $\forall_j \sum_i a_{ij} \leq 1$ is normal (in the case where $n = k_p$ this is the celebrated *Birkhoff polytope*). This is a not new result; in fact, this polytope satisfies a stronger property, namely, it is *compressed*. This follows, for instance, from [Sullivant 2006, Theorem 2.4] or from the main theorem of [Ohsugi and Hibi 2001]; see also [Yamaguchi et al. 2014, Section 4.2]. For completeness, we include a proof of the proposition using elementary properties of matchings in bipartite graphs.

Proof of Proposition 3.1. Let x_p denote the vector of variables $x_{p,l,j}$ for $l \in [k_p]$ and $j \in \mathbb{N}$. By definition of φ, the monomial x^A lies in $\operatorname{im}\varphi$ if and only if the monomial $x_p^{A_p}$ lies in $\operatorname{im}\varphi$ for all $p \in [N]$. Thus it suffices to prove that $x_p^{A_p}$ lies in $\operatorname{im}\varphi$ if and only if all row sums of A_p are equal, say to $d \in \mathbb{N}$, and all column sums of A_p are at most d. The "only if" part is clear, since every variable $y_{p,J}$ is mapped to a monomial x_p^B where $B \in \mathbb{N}^{[k_p]\times\mathbb{N}}$ has all row sums 1 and all column sums at most 1. For the "if" part we proceed by induction on d: assume that the

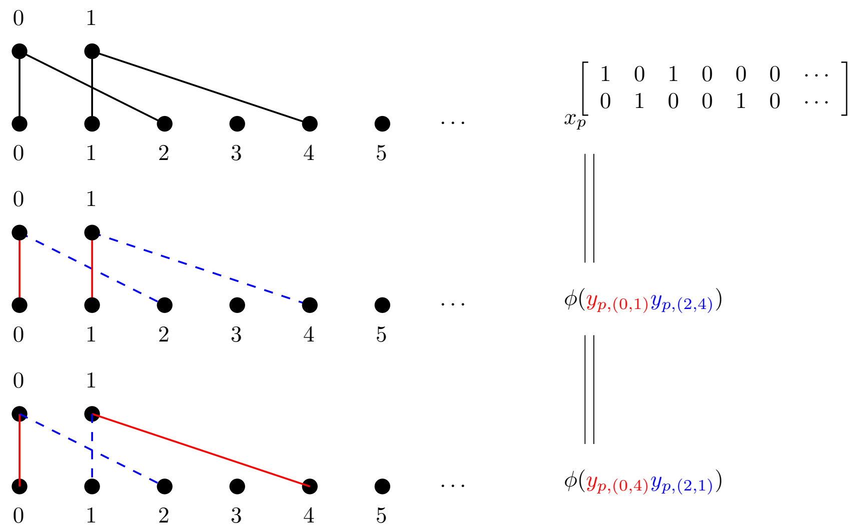


Figure 1. A bipartite graph on $[2] \sqcup \mathbb{N}$ and its corresponding monomial $x_p^{A_p}$ (top). This graph can be decomposed into matchings in two different ways (middle and bottom). Each decomposition represents a monomial in the preimage $\varphi^{-1}(x_p^{A_p})$.

statement holds for $d-1$, and consider a matrix A_p with row sums d and column sums $\leq d$, where d is at least 1. Clearly, the "if" part is true in the case $d = 0$.

Think of A_p as the adjacency matrix of a bipartite graph Γ (with multiple edges) with bipartition $[k_p] \sqcup \mathbb{N}$ (see Figure 1). With this viewpoint in mind, we will invoke some standard results from combinatorics, and refer to [Schrijver 2003, Chapter 16]. The first observation is that Γ contains a matching that covers all vertices in $[k_p]$. Indeed, otherwise, by Hall's marriage theorem, after permuting rows and columns, A_p has the block structure

$$A_p = \begin{bmatrix} A_{11} & 0 \\ A_{12} & A_{22} \end{bmatrix}$$

with $A_{11} \in \mathbb{N}^{[l] \times [l-1]}$ for some l satisfying $1 \leq l \leq k_p$. But then the entries of A_{11} added row-wise add up to ld, and added columnwise add up to at most $(l-1)d$, a contradiction. Hence Γ contains a matching that covers all of $[k_p]$. Next, let $S \subseteq \mathbb{N}$ be the set of column indices where A_p has column sum equal to the upper bound d. We claim that Γ contains a matching that covers all of S. Indeed, otherwise, again by Hall's theorem, after permuting rows and columns A_p has the structure

$$A_p = \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix}$$

with $A_{11} \in \mathbb{N}^{[l-1]\times[l]}$ for some l with $1 \le l \le |S|$; here the first l columns correspond to a subset of the original S. Now the entries of A_{11} added columnwise yield ld, while the entries of A_{11} added row-wise yield at most $(l-1)d$, a contradiction.

Finally, we invoke a standard result in matching theory (see [Schrijver 2003, Theorem 16.8]), namely that since Γ contains a matching that covers all of $[k_p]$ and a matching that covers all of S, it also contains a matching that covers both. Let B be the adjacency matrix of this matching, so that B has all row sums 1 and all column sums ≤ 1, with equality at least in the columns labeled by S. Then $A'_p := A_p - B$ satisfies the induction hypothesis for $d-1$, so $x_p^{A'_p} \in \operatorname{im}\varphi$. Also, $x_p^B = \varphi(y_{p,J})$, where $j_a \in \mathbb{N}$ is the neighbor of $a \in [k_p]$ in the matching given by B. Hence, $x_p^{A_p} = x_p^{A'_p} x_p^B \in \operatorname{im}\varphi$ as claimed. □

This concludes the description of the image of φ. For the kernel, we quote the following result.

Theorem 3.3 [Yamaguchi et al. 2014, Theorem 2.1]. *The kernel of φ from* (1) *is generated by binomials in the $y_{p,J}$ of degree at most* 3.

Indeed, for each fixed p, and replacing $\mathbb{N}$ by some $[n]$ with $n \ge k_p$, the monomial map (1) captures precisely the generalization of the Birkhoff model studied in [Yamaguchi et al. 2014], where each voter chooses k_p among n candidates. Then their Theorem 2.1 yields that the kernel is generated in degrees 2 and 3. Since this holds for each $n \ge k_p$, it also holds for $\mathbb{N}$ instead of $[n]$. Moreover, taking the union over all p of sets of generators for each individual p yields a set of generators for the kernel of φ. A straightforward consequence of the theorem is the following.

Corollary 3.4. *The kernel of φ from* (1) *is generated by finitely many* $\operatorname{Inc}(\mathbb{N})$*-orbits of binomials.*

4. Noetherianity of matching monoid rings

By Corollary 3.4 and Proposition 2.1, the main theorem follows from the following proposition.

Proposition 4.1. *The ring* $R\big[x^A \mid A \in \prod_{p\in[N]} \mathbb{N}^{[k_p]\times\mathbb{N}} \text{ good}\big]$ *is* $\operatorname{Inc}(\mathbb{N})$*-Noetherian.*

Let S be the ring in the proposition, and let $G \subset \prod_{p\in[N]} \mathbb{N}^{[k_p]\times\mathbb{N}}$ be the set of good (N-tuples of) matrices. The monomials of S are precisely x^A, for $A \in G$. The monoids $\operatorname{Sym}(\mathbb{N})$ and $\operatorname{Inc}(\mathbb{N})$ act on G by permuting or shifting columns, so we have $\pi x^A = x^{\pi A}$, where the $\pi(j)$-th column of the matrix $(\pi A)_p$ equals the j-th column of A_p. Let $d_A = (d_{A,p})_p \in \mathbb{N}^{[N]}$ denote the multidegree of A; recall that this means that all row sums of A_p are equal to $d_{A,p}$. To prove Noetherianity we will define a partial order $\preceq$ on G and prove that $\preceq$ is a well-partial-order. Thus we need some basic results from order theory.

A partial order $\preceq$ on a set P is a *well-partial-order* (or *wpo*) if for every infinite sequence $p_1, p_2, \dots$ in P, there is some $i < j$ such that $p_i \preceq p_j$; see [Kruskal 1972] for alternative characterizations. For instance, the natural numbers with the usual total order $\leq$ is a well-partial-order, and so is the componentwise partial order on the Cartesian product of any finite number of well-partially ordered sets. Combining these statements yields Dickson's lemma [1913] that $\mathbb{N}^k$ is well-partially ordered. This can be seen as a special case of Higman's lemma [1952], for a beautiful proof of which we refer to [Nash-Williams 1963].

Lemma 4.2 (Higman's lemma). *Let $(P, \preceq)$ be a well-partial-order and let $P^* := \bigcup_{l=0}^{\infty} P^l$, the set of all finite sequences of elements of P. Define the partial order $\preceq'$ on P^* by $(a_0, \dots, a_{l-1}) \preceq' (b_0, \dots, b_{m-1})$ if and only if there exists a strictly increasing function $\rho : [l] \to [m]$ such that $a_j \preceq b_{\rho(j)}$ for all $j \in [l]$. Then $\preceq'$ is a well-partial-order.*

Our interest in well-partial-orders stems from the following application. Consider a commutative monoid M with an action of a (typically noncommutative) monoid Π by means of monoid endomorphisms. We suggestively call the elements of M monomials. Assume that we have a Π-*compatible monomial order* $\leq$ on M, i.e., a well-order that satisfies $a < b \Rightarrow ac < bc$ and $a < b \Rightarrow \pi a < \pi b$ for all $a, b, c \in \mathrm{M}$ and $\pi \in \Pi$. Then it follows that the divisibility relation $|$ defined by $a|b$ if there exists a $c \in \mathrm{M}$ with $ac = b$ is a partial order, and also that $a \leq \pi a$ for all $a \in \mathrm{M}$. Define a third partial order, the Π-*divisibility order*, $\preceq$ on M by $a \preceq b$ if there exists a $\pi \in \Pi$ and a $c \in \mathrm{M}$ such that $c\pi a = b$. A straightforward computation shows that $\preceq$ is, indeed, a partial order — antisymmetry follows using $a \leq \pi a$.

Proposition 4.3. *If $\preceq$ is a well-partial-order, then for any Noetherian ring R, the R-algebra $R[\mathrm{M}]$ is Π-Noetherian.*

Proof. This statement was proved in [Hillar and Sullivant 2012] for the case where R is a field. The more general case can be proved with the same argument by incorporating work done in [Aschenbrenner and Hillar 2007]. □

Note that the monoid $\{x^A \mid A \in G\}$ that we are considering here can be given a monomial order which respects the $\mathrm{Inc}(\mathbb{N})$-action. For example, take the lexicographic order, where the variables $x_{p,i,j}$ are ordered by their indices: $x_{p,i,j} < x_{p',i',j'}$ if and only if $p < p'$; or $p = p'$ and $j < j'$; or $p = p'$, $j = j'$, and $i < i'$.

The $\mathrm{Inc}(\mathbb{N})$-divisibility order gives a partial order $\preceq$ on the set G of good (N-tuples of) matrices by $A \preceq B$ if and only if there is a monomial $x^C \in S$ and $\pi \in \mathrm{Inc}(\mathbb{N})$ such that $x^C \pi(x^A) = x^B$, or equivalently there is $\pi \in \mathrm{Inc}(\mathbb{N})$ such that $B - \pi A \in G$. Note that $A \preceq B$ not only implies there is some $\pi \in \mathrm{Inc}(\mathbb{N})$ such that all $A_{p,i,j} \leq B_{p,i,\pi(j)}$, but additionally that all (N-tuples of) column sums of $B - \pi A$ are at most $d_B - d_A \in \mathbb{N}^{[N]}$. This prevents us from applying Higman's lemma directly to $(G, \preceq)$. To encode this condition on column sums, for any $A \in G$, let $\tilde{A} \in \prod_{p\in[N]} \mathbb{N}^{[k_p+1]\times\mathbb{N}}$ be the N-tuple of matrices such that for all $p \in [N]$, the first k_p rows of $\tilde{A}_p$ are equal to A_p, and the last row of $\tilde{A}_p$ is such that all column sums equal $d_{A,p}$:

$$\tilde{A}_{p,i,j} = \begin{cases} A_{p,i,j} & \text{for } \ i < k_p, \\ d_{A,p} - \sum_{l=0}^{k_p-1} A_{p,l,j} & \text{for } \ i = k_p. \end{cases}$$

We let $\tilde{G}$ be the set of N-tuples of matrices of the form $\tilde{A}$ with $A \in G$. It is precisely the set of N-tuples of matrices of the form $\tilde{A} \in \prod_{p\in[N]} \mathbb{N}^{[k_p+1]\times\mathbb{N}}$ with the property that there exists a $d_A \in \mathbb{N}^{[N]}$ such that for each $p \in [N]$ the first k_p row sums of A_p are equal to $d_{A,p}$ and all column sums of A_p are equal to $d_{A,p}$. Since $A \in G$ has only finitely many N-tuples of nonzero columns, $\tilde{A}$ will have all but finitely many N-tuples of columns equal to $((0, \dots, 0, d_{A,p})^T)_{p\in[N]}$. Such N-tuples of columns will be called *trivial* (of degree d_A). The N-tuple of j-th columns of $\tilde{A}$ will be denoted $\tilde{A}_{\cdot\cdot j}$. We define the action of $\mathrm{Inc}(\mathbb{N})$ on $\tilde{G}$ as $\pi(\tilde{A}) = \widetilde{\pi(A)}$. Note that for any $j \notin \mathrm{im}(\pi)$, the column $(\pi\tilde{A})_{\cdot\cdot j}$ is trivial of degree d_A, rather than uniformly zero.

Proposition 4.4. *For $A, B \in G$, $A \preceq B$ if and only if there is $\pi \in \mathrm{Inc}(\mathbb{N})$ such that $\pi\tilde{A} \le \tilde{B}$ entrywise.*

Proof. The condition that $(\pi\tilde{A})_{p,i,j} \le \tilde{B}_{p,i,j}$ for all $p \in [N]$, all $i < k_p$, and all $j \in \mathbb{N}$ is equivalent to the condition that $B - \pi A$ is nonnegative. Using the fact that

$$\tilde{B}_{p,k_p,j} - (\pi\tilde{A})_{p,k_p,j} = (d_{B,p} - d_{A,p}) - \sum_{i=0}^{k_p-1} (B_p - \pi A_p)_{i,j},$$

the condition that $\tilde{B}_{p,k_p,j} - (\pi\tilde{A})_{p,k_p,j} \ge 0$ for all $p \in [N]$ and all $j \in \mathbb{N}$ is equivalent to the condition that every N-tuple of column sums of $B - \pi A$ is less than or equal to $d_B - d_A$. Therefore $\pi\tilde{A} \le \tilde{B}$ if and only if $B - \pi A \in G$. □

Example 4.5. Let A and B be the following good matrices in $\mathbb{N}^{[2]\times\mathbb{N}}$:

$$A = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 1 & 0 & \cdots \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 2 & 1 & 1 & 0 & \cdots \end{bmatrix}.$$

Note that $\pi A \le B$ when π is the identity, however $A \not\preceq B$. Consider

$$\tilde{A} = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 1 & 0 & \cdots \\ 0 & 2 & 2 & 2 & 3 & \cdots \end{bmatrix}, \quad \tilde{B} = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 2 & 1 & 1 & 0 & \cdots \\ 1 & 1 & 3 & 3 & 4 & \cdots \end{bmatrix},$$

and note that there is no $\pi \in \mathrm{Inc}(\mathbb{N})$ such that $\pi\tilde{A} \le \tilde{B}$.

We will work with finite truncations of N-tuples of matrices in $\tilde{G}$. Let H be the set of N-tuples of matrices $A \in \bigcup_{\ell=0}^{\infty} \prod_{p\in[N]} \mathbb{N}^{[k_p+1]\times[\ell]}$ such that there exists $d_A \in \mathbb{N}^{[N]}$ such that for all p, all column sums of A_p are equal to $d_{A,p}$ and the first k_p row sums are *at most* $d_{A,p}$; we call d_A the *multidegree* of A. Note that the condition on row sums is relaxed, which will allow us to freely remove columns from matrices while still remaining in the set H. For $A \in$ H the number of columns of A is called the *length* of A and denoted ℓ_A. We give H the partial order $\preceq$ defined as follows. For $A, B \in$ H, $A \preceq B$ if and only if there is a strictly increasing map $\rho : [\ell_A] \to [\ell_B]$ such that $\rho A \leq B$. Just as in $\tilde{G}$, here ρA is defined by $(\rho A)_{\cdot\cdot j} = A_{\cdot\cdot\rho^{-1}(j)}$ for $j \in \mathrm{im}(\rho)$, and $(\rho A)_{\cdot\cdot j}$ trivial (of degree d_A) for $j \in [\ell_B] \setminus \mathrm{im}(\rho)$. For an N-tuple of matrices A and a set $J \subset \mathbb{N}$, let $A_{\cdot\cdot J}$ denote the N-tuple of matrices obtained from A by taking only the columns $A_{\cdot\cdot j}$ with $j \in J$.

Some care must be taken in the definition of H since we allow matrices with no columns. In all other cases, the degree of $A \in$ H is uniquely determined by its entries. However for the length 0 case the degree is arbitrary, so we will consider H as having a distinct length 0 element Z^d with degree d for each $d \in \mathbb{N}^{[N]}$, and we define $Z^d \preceq A$ if and only if $d \leq d_A$. Additionally, define $A_{\cdot\cdot\varnothing} = Z^{d_A}$.

Definition 4.6. For $A \in$ H, the N-tuple of j-th columns of A is *bad* if for some $p \in [N]$, we have $A_{p,k_p,j} < d_{A,p}/2$. If $A_{p,k_p,j} < d_{A,p}/2$, we will call j a *bad index* of A (with respect to p). Let H_t denote the set of N-tuples of matrices in H with exactly t bad indices.

We will use induction on t to show that $(\mathrm{H}_t, \preceq)$ is well-partially ordered for all $t \in \mathbb{N}$. This will in turn be used to prove that $(\mathrm{H}, \preceq)$ and then $(\tilde{G}, \preceq)$ are well-partially ordered. First we prove the base case:

Proposition 4.7. $(\mathrm{H}_0, \preceq)$ *is well-partially ordered.*

Proof. Let $A^{(1)}, A^{(2)}, \ldots$ be any infinite sequence in H_0. We will show that there is an r and an s, with $r < s$, such that $A^{(r)} \preceq A^{(s)}$.

Fix $p \in [N]$. There are now two possibilities: either the degrees of the elements of the sequence $A_p^{(1)}, A_p^{(2)}, \ldots$ are bounded by some $d_p \in \mathbb{N}$, or they are not. In the former case, it follows that the number of nontrivial columns in any $A_p^{(r)}$ is bounded by $d_p k_p$. Then there is a subsequence $B_p^{(1)}, B_p^{(2)}, \ldots$ of $A_p^{(1)}, A_p^{(2)}, \ldots$ such that every element has the same degree and same number of nontrivial columns. In the latter case, $A_p^{(1)}, A_p^{(2)}, \ldots$ has a subsequence with strictly increasing degree and moreover a subsequence $B_p^{(1)}, B_p^{(2)}, \ldots$ with the property that $d_{B^{(s+1)},p} \geq 2d_{B^{(s)},p}$ for all $s \in \mathbb{N}$.

In either case we replace $A^{(1)}, A^{(2)}, \ldots$ by $B^{(1)}, B^{(2)}, \ldots$ without loss of generality. We repeat this procedure for all $p \in [N]$, and we find that $A^{(1)}, A^{(2)}, \ldots$ contains a subsequence $B^{(1)}, B^{(2)}, \ldots$ such that for all $p \in [N]$, one of the following two statements holds.

1: Both $d_{B^{(t)},p}$ and the number of nontrivial columns in B_p are constant.

2: We have $d_{B^{(t+1)},p} \geq 2d_{B^{(t)},p}$ for all t.

It now suffices to show that there are $r < s$ such that $B^{(r)} \preceq B^{(s)}$. Define the partial order $\sqsubseteq$ on H_0 by $A \sqsubseteq B$ if and only if there exists strictly increasing $\rho : [\ell_A] \to [\ell_B]$ such that $A_{\cdot\cdot j} \leq B_{\cdot\cdot\rho(j)}$ for all $j \in [\ell_A]$. By Higman's lemma (Lemma 4.2), $\sqsubseteq$ is a wpo. This means that there exist $r < s$ such that $B^{(r)} \sqsubseteq B^{(s)}$. Fix such a pair $r < s$. We will show that $B^{(r)} \preceq B^{(s)}$.

Let $\rho : [\ell_{B^{(r)}}] \to [\ell_{B^{(s)}}]$ be a strictly increasing map that witnesses $B^{(r)} \sqsubseteq B^{(s)}$. We claim that it also witnesses $B^{(r)} \preceq B^{(s)}$. For this, we have to show that $\rho B^{(r)} \leq B^{(s)}$. By the properties of $\sqsubseteq$, we already have $(\rho B^{(r)})_{\cdot\cdot\rho(j)} \leq B^{(s)}_{\cdot\cdot\rho(j)}$, which is to say that it suffices to show that for all $j \notin \mathrm{im}(\rho)$, we have $d_{B^{(r)}} \leq (B^{(s)}_{p,k_p,j})_{p\in[N]}$.

Let $p \in [N]$. Suppose we are in the case that both $d_{B^{(t)},p}$ and the number of nontrivial columns in B_p are constant. Since ρ must map nontrivial columns of $B^{(r)}_p$ to nontrivial columns of $B^{(s)}_p$, we conclude that if $j \notin \mathrm{im}(\rho)$, then the j-th column of $B^{(s)}_p$ is trivial, and hence $(B^{(s)}_{p,k_p,j}) = d_{B^{(s)},p}$. But the latter equals $d_{B^{(r)},p}$, so certainly $d_{B^{(r)},p} \leq (B^{(s)}_{p,k_p,j})$.

Alternatively, suppose we have $d_{B^{(t+1)},p} \geq 2d_{B^{(t)},p}$ for all t. Since $B^{(s)}_p$ has no bad columns, we have

$$B^{(s)}_{p,k_p,j} \geq \frac{1}{2} d_{B^{(s)},p} \geq d_{B^{(r)},p}.$$

This is exactly what we wanted to show.

So in both cases, we find that $d_{B^{(r)},p} \leq B^{(s)}_{p,k_p,j}$ for all $j \notin \mathrm{im}(\rho)$. This is true for all p, so we have $d_{B^{(r)}} \leq (B^{(s)}_{p,k_p,j})_{p\in[N]}$. We conclude that $B^{(r)} \preceq B^{(s)}$, as we wanted to show. □

Proposition 4.8. $(\mathrm{H}_t, \preceq)$ *is well-partially ordered for all* $t \in \mathbb{N}$.

Proof. The base case, $t = 0$, is given by Proposition 4.7. For $t > 0$, assume by induction that $(\mathrm{H}_{t-1}, \preceq)$ is well-partially ordered. For any $A \in \mathrm{H}_t$, let j_A be the largest bad index of A. Then A can be decomposed into three parts: the N-tuple of matrices of all N-tuples of columns before j_A, $A_{\cdot\cdot j_A}$ itself, and the N-tuple of matrices of all N-tuples of columns after j_A. This decomposition is represented by the map

$$\delta : \mathrm{H}_t \to \mathrm{H}_{t-1} \times \prod_{p\in[N]} \mathbb{N}^{[k_p+1]} \times \mathrm{H}_0$$
$$A \mapsto (A_{\cdot\cdot\{0,\dots,j_A-1\}}, A_{\cdot\cdot j_A}, A_{\cdot\cdot\{j_A+1,\dots,\ell_A-1\}}).$$

Let the partial order $\sqsubseteq$ on $\mathrm{H}_{t-1} \times \prod_{p\in[N]} \mathbb{N}^{[k_p+1]} \times \mathrm{H}_0$ be the product order of the wpos $(\mathrm{H}_{t-1}, \preceq)$, $(\mathbb{N}^{[k+1]}, \leq)$ and $(\mathrm{H}_0, \preceq)$. Note that the product order of any finite number of wpos is also a wpo. Suppose for some $A, B \in \mathrm{H}_t$ that $\delta(A) \sqsubseteq \delta(B)$. This implies that $A_{\cdot\cdot j_A} \leq B_{\cdot\cdot j_B}$ and that there exist strictly increasing maps ρ and σ such

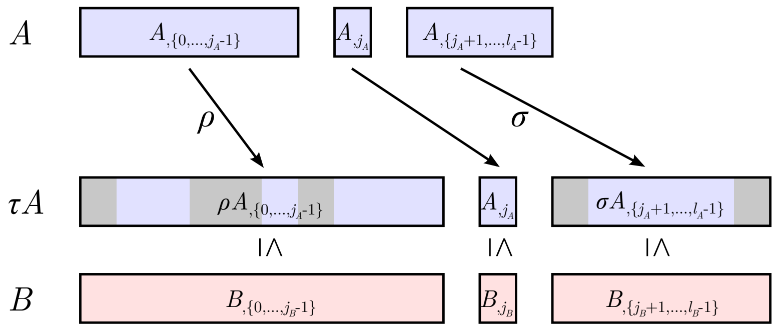


Figure 2. $\delta(A) \sqsubseteq \delta(B)$ implies $A \preceq B$.

that $\rho(A_{\cdot\cdot[j_A]}) \leq B_{\cdot\cdot[j_B]}$ and $\sigma(A_{\cdot\cdot\{j_A+1,\dots,\ell_A-1\}}) \leq B_{\cdot\cdot\{j_B+1,\dots,\ell_B-1\}}$. We combine these into a single strictly increasing map $\tau : [\ell_A] \to [\ell_B]$ defined by

$$\tau(j) = \begin{cases} \rho(j) & \text{for } 0 \leq j < j_A, \\ j_B & \text{for } j = j_A, \\ \sigma(j - j_A - 1) + j_B + 1 & \text{for } j_A < j < \ell_A, \end{cases}$$

illustrated in Figure 2. Then $\tau A \leq B$ so $A \preceq B$. Since $\sqsubseteq$ is a wpo, $(\mathrm{H}_t, \preceq)$ is also a wpo. ☐

Proposition 4.9. $(\mathrm{H}, \preceq)$ *is well-partially ordered.*

Proof. For any $A \in \mathrm{H}$, if j is a bad index of A, then for some $p \in [N]$, we have $d_{A,p}/2 > \sum_{i \in [k_p]} A_{p,i,j}$. Letting $J_p \subset \mathbb{N}$ be the set of bad indices of A with respect to p and let $J \subset \mathbb{N}$ be the union of the J_p. Then

$$|J_p| \frac{d_{A,p}}{2} < \sum_{j \in J_p} \sum_{i \in [k_p]} A_{p,i,j} \leq \sum_{i \in [k_p]} \sum_{j \in \mathbb{N}} A_{p,i,j} \leq k_p d_A,$$

with the last inequality due to the row sum condition on A_p. Therefore $|J_p| \leq 2k_p - 1$, and hence $|J| \leq 2 \sum_{p \in [N]} k_p - N$.

Let $A^{(1)}, A^{(2)}, \dots$ be any infinite sequence in H. Since the numbers of bad N-tuples of columns of elements of H are bounded by $2 \sum_{p \in [N]} k_p - N$ there exists a subsequence which is contained in H_t for some $0 \leq t \leq 2 \sum_{p \in [N]} k_p - N$. By Proposition 4.8 there is $r < s$ with $A^{(r)} \preceq A^{(s)}$. ☐

Proposition 4.10. $(G, \preceq)$ *is well-partially ordered.*

Proof. Let $A^{(1)}, A^{(2)}, \dots$ be any infinite sequence in G. Each $A^{(r)}$ has some $j_r > 0$ such that all N-tuples of columns $A^{(r)}_{\cdot\cdot m}$ are zero for $m \geq j_r$. Consider the sequence $\tilde{A}^{(1)}_{\cdot\cdot[j_1]}, \tilde{A}^{(2)}_{\cdot\cdot[j_2]}, \dots$ in H obtained by truncating each $\tilde{A}^{(r)}$ to the first j_r N-tuples of columns. By Proposition 4.9 there is some $r < s$ and $\rho : [j_r] \to [j_s]$ such that

$\rho\tilde{A}^{(r)}_{\cdot\cdot[j_r]} \le \tilde{A}^{(s)}_{\cdot\cdot[j_s]}$. Note that this implies $d_{A^{(r)}} \le d_{A^{(s)}}$. Extend ρ to some $\pi \in \mathrm{Inc}(\mathbb{N})$ so then

$$(\pi\tilde{A}^{(r)})_{\cdot\cdot[j_s]} = \rho(\tilde{A}^{(r)}_{\cdot\cdot[j_r]}) \le \tilde{A}^{(s)}_{\cdot\cdot[j_s]}.$$

The remaining N-tuples of columns of $\pi\tilde{A}^{(r)}$ and $\tilde{A}^{(s)}$ are trivial, so $\pi\tilde{A}^{(r)} \le \tilde{A}^{(s)}$ follows from the fact that $d_{A^{(r)}} \le d_{A^{(s)}}$. Therefore $A^{(r)} \preceq A^{(s)}$ by Proposition 4.4. □

Now we can apply Proposition 4.3 to the monoid $\{x^A \mid A \in G\}$ which proves that the ring $R[x^A \mid A \in G]$ is $\mathrm{Inc}(\mathbb{N})$-Noetherian. This concludes the proof of Proposition 4.1.

5. Buchberger's algorithm for matching monoid algebras

Assume the general setting of Proposition 4.3: M is a monoid with Π-action and Π-compatible monomial order $\le$. For a polynomial f and an ideal I in $K[M]$, we can define $\mathrm{lm}(f)$, $\mathrm{lc}(f)$, $\mathrm{in}(I)$, division with remainder, and the concept of equivariant Gröbner basis from [Brouwer and Draisma 2011]; all relative to the monomial order $\le$. We now derive a version of Buchberger's algorithm for computing such a Gröbner basis, under an additional assumption. For $a, b \in M$ we define the set of *least common multiples*

$$\mathrm{lcm}(a, b) = \{l \in M : a|l, b|l \text{ and } (a|l', b|l', l'|l \Rightarrow l' = l)\}.$$

We require the following variant of conditions EGB3 and EGB4 from [Brouwer and Draisma 2011]:

EGB34. For all $f, g \in K[M]$, the set of triples in $M \times \Pi f \times \Pi g$ defined by

$$T_{f,g} = \bigl\{(l', f', g') \bigm| f' \in \Pi f,\ g' \in \Pi g,\ l' \in \mathrm{lcm}(\mathrm{lm}(f'), \mathrm{lm}(g'))\bigr\},$$

is a union of a finite number of Π-orbits:

$$T_{f,g} = \bigcup_i \Pi(l_i, f_i, g_i), \quad i \in [r].$$

In particular, EGB34 implies that for all $a, b \in M$ and $\pi \in \Pi$, we have $\pi\ \mathrm{lcm}(a, b) \subseteq \mathrm{lcm}(\pi a, \pi b)$. (This is what condition EGB3 of [loc. cit.] looks like when least common multiples are not unique.)

If EGB34 is fulfilled, then there is a unique *inclusion-minimal* finite set of orbit generators as above, which we denote

$$O_{f,g} = \{(l_i, f_i, g_i) \mid i \in [r]\}.$$

Indeed, suppose that O and O' are both inclusion-minimal sets of orbit generators for $T_{f,g}$. For any triple $t \in O$, there are $t' \in O', \pi \in \Pi$ such that $\pi t' = t$, and similarly $t'' \in O$, $\tau \in \Pi$ such that $\tau t'' = t'$. Now $t = \pi \tau t''$ and since O is minimal, $t = t''$. But since Π is compatible with a monomial order, $\pi \tau t'' = t''$ implies that also the intermediate expression $t' = \tau t''$ equals t''. Hence $O \subseteq O'$ and equality holds by minimality of O'.

Definition 5.1. For monic $f, g \in K[M]$ define the *set of S-polynomials* to be

$$S_{f,g} = \left\{ af' - bg' \;\middle|\; (l', f', g') \in O_{f,g};\; a, b \in M;\; \text{and } a \operatorname{lm}(f') = b \operatorname{lm}(g') = l' \right\}.$$

Furthermore, define Π-*reduction* of a polynomial f with respect to a set $G \subseteq K[M]$ as follows: while there exist $g \in G$ and $\pi \in \Pi$ with $\pi \operatorname{lm}(g) | \operatorname{lm}(f)$, replace f by

$$f' := f - \frac{\operatorname{lc}(f) \operatorname{lm}(f)}{\operatorname{lc}(g) \pi \operatorname{lm}(g)} \pi g;$$

and when no such g and π exist, return the *remainder* f'.

One can generalize Gröbner theory to our equivariant setting for a monoid algebra satisfying EGB34. In particular, Buchberger's criterion holds, and the following procedure produces an equivariant Gröbner basis *if* it terminates.

Algorithm 5.2. $G = \text{BUCHBERGER}(F)$

Require: F is a finite set of monic elements in $K[M]$, the algebra of a monoid M equipped with a Π-action, satisfying the assumptions above and the condition EGB34.

Ensure: G is an equivariant Gröbner basis of $\langle F \rangle$.

$G \leftarrow F$
$S \leftarrow \bigcup_{f,g \in G} S_{f,g}$ {in particular, compute $O_{f,g}$ needed in Definition 5.1}
while $S \neq \varnothing$ **do**
  pick $f \in S$
  $S \leftarrow S \setminus \{f\}$
  $h \leftarrow$ the Π-reduction of f with respect to G
  if $h \neq 0$ **then**
    $G \leftarrow G \cup \{h\}$
    $S \leftarrow S \cup \left(\bigcup_{g \in G} S_{g,h} \right)$
  end if
end while

This algorithm has been implemented for the particular case where $K[M]$ is a polynomial ring and $\Pi = \operatorname{Inc}(\mathbb{N})$ (i.e., the algorithm described in [Brouwer and Draisma 2011]) in the package *EquivariantGB* [Hillar et al. 2013] for the computer algebra system *Macaulay2* [Grayson and Stillman 2002]. When the algebra $K[M]$ is Π-Noetherian, termination of Algorithm 5.2 is guaranteed, but in general we cannot make this claim.

We now turn our attention to the task of computing a finite Inc(ℕ)-generating set of binomials of a general toric map as in the main theorem. By the proof of Proposition 2.1 we may assume that Y is as in (1), i.e., it consists of variables $y_{p,J}$ where p runs through $[N]$ and J runs through all k_p-tuples of distinct natural numbers. Section 2 then leads to the following analysis of this task.

Problem 5.3. Fix the names of algebras and maps in the following diagram:

$$R[Y] \xrightarrow{\varphi} R[X] \xrightarrow{\psi} R[Z].$$

Here φ is the map defined by (1), whose image is the R-algebra spanned by the matching monoid, and ψ is any Sym(ℕ)-equivariant monomial map from $R[X]$ to $R[z_{ij} \mid i \in [k], j \in \mathbb{N}]$. For $\ker(\psi \circ \varphi)$, how does one compute

(a) a finite set of generators up to Inc(ℕ)-symmetry?

(b) a finite Inc(ℕ)-Gröbner basis with respect to a given Inc(ℕ)-compatible monomial order on $K[Y]$?

The algorithm we are about to construct solves Problem 5.3(a); indeed, we do not know whether a finite Inc(ℕ)-Gröbner basis as in part (b) exists! Our algorithm relies on the fact that we may replace $R[X]$ above by the matching monoid algebra $\operatorname{im}\varphi = R[x^A \mid A \text{ good}]$, so as to get the sequence

$$R[Y] \xrightarrow{\varphi} R[x^A \mid A \text{ good}] \xrightarrow{\psi} R[Z]. \tag{2}$$

Most of our computations will take place in the ring $R[x^A \mid A \text{ good}][Z]$, which is itself a matching monoid with N replaced by $N+k$ and $k_p = 1$ for $p \in [N+k] \setminus [N]$. This monoid is Gröbner friendly by the following proposition.

Proposition 5.4. *Let M be a submonoid of $\mathbb{N}^{[k]\times\mathbb{N}}$ that is generated by the* Sym(ℕ)-*orbits of a finite number of matrices. For $\Pi = \text{Inc}(\mathbb{N})$, the monoid algebra $K[M]$ satisfies EGB*34.

Proof. Any such $K[M]$ is the image of some map φ as in the main theorem (with $R = K$), and so is Inc(ℕ)-Noetherian. Similarly $K[M^3] = K[M]^{\otimes 3}$ is Inc(ℕ)-Noetherian. For any $a, b \in M$, the monomial ideal $\langle T_{a,b}\rangle \subseteq K[M^3]$ is Inc(ℕ)-stable. Let $L \subseteq T_{a,b}$ be a minimal finite Inc(ℕ)-generating set of $\langle T_{a,b}\rangle$.

For any $(l, \pi a, \sigma b) \in T_{a,b}$, there is some $(m, a', b') \in L$ and $\tau \in \text{Inc}(\mathbb{N})$ such that $\tau(m, a', b') | (l, \pi a, \sigma b)$. It is clear that $\tau a' = \pi a$ and $\tau b' = \sigma b$. Since a' and b' divide m, πa and σb must divide τm, and in turn τm divides l. But $l \in \operatorname{lcm}(\pi a, \sigma b)$ by assumption, so $l = \tau m$. Therefore $(l, \pi a, \sigma b) = \tau(m, a', b')$. This shows that $T_{a,b}$ is the union of the Inc(ℕ)-orbits of the elements of L, and then $L = O_{a,b}$.

To establish the same fact for a general pair $f, g \in K[M]$ we first determine $O_{a,b}$, where $a = \operatorname{lm}(f)$ and $b = \operatorname{lm}(g)$. For any $(l, \pi f, \sigma g) \in T_{f,g}$, the triple

$(l, \pi a, \sigma b) \in T_{a,b}$ is in the orbit of some $(m, a', b') \in O_{a,b}$. This implies $a' = \tau a$ for some $\tau \in \mathrm{Inc}(\mathbb{N})$, but τ is not unique. Define

$$\Lambda_{a,a'} := \{\tau \in \mathrm{Inc}(\mathbb{N}) \mid a' = \tau a; \text{ and } n \in \operatorname{im}\tau \text{ for all } n > \ell_{a'}\}.$$

Here $\ell_{a'}$ denotes the *length* of a' as in Section 4, the maximum index value among all nonzero columns of a'. Note that $\Lambda_{a,a'}$ is a finite set.

Since πa is in the orbit of a', π factors through some $\tau \in \Lambda_{a,a'}$. So $(l, \pi f, \sigma g) = (\gamma m, \alpha\tau_1 f, \beta\tau_2 g)$ for some $\gamma, \alpha, \beta \in \mathrm{Inc}(\mathbb{N})$, $\tau_1 \in \Lambda_{a,a'}$ and $\tau_2 \in \Lambda_{b,b'}$. Therefore

$$T_{f,g} \subseteq \bigcup_{(m,f',g') \in U_{f,g}} \Pi m \times \Pi f' \times \Pi g'$$

where

$$U_{f,g} = \bigcup_{(m,a',b') \in T_{a,b}} \{(m, \tau_1 f, \tau_2 g) \mid \tau_1 \in \Lambda_{a,a'}, \tau_2 \in \Lambda_{b,b'}\}.$$

For each (m, f', g'), the set $\Pi m \times \Pi f' \times \Pi g'$ is the union of a finite number of $\mathrm{Inc}(\mathbb{N})$-orbits. To prove this one can follow closely the proof of [Brouwer and Draisma 2011] Lemma 3.4. From the finite set of generators we select only those $(\gamma m, \alpha f', \beta g')$ with $\gamma m \in \operatorname{lcm}(\alpha f', \beta g')$, and call this set $O_{(m,f',g')}$. Then $O_{f,g} = \bigcup_{(m,f',g') \in U_{f,g}} O_{(m,f',g')}$ is as desired. □

Algorithm 5.5. $T = $ TORICIDEAL(φ)

Require: $\varphi : R[Y] \to R[Z]$ is a monomial map as in the main theorem.
Ensure: T is a finite set of generators of $\ker\varphi$ as $\mathrm{Inc}(\mathbb{N})$-stable ideal.

1: Replace Y by the set of variables $\{y_{p,J}\}_{p,J}$ as in the proof of Proposition 2.1.

2: Decompose φ with the composition of two maps φ and ψ as in diagram (2).

3: Consider the ideal $I_\psi \subset R[x^A \mid A \text{ good}][Z]$ generated by the finite set F of binomials $\psi(x^A) - x^A$, where $A \in \prod_{p\in[N]} \mathbb{N}^{[k_p]\times\mathbb{N}}$ is good of multidegree

$$d \in \{(1, 0, \dots, 0), \dots, (0, 0, 0, \dots, 1)\} \subseteq \mathbb{N}^{[N]}$$

and $\preceq$-minimal; the $\mathrm{Inc}(\mathbb{N})$-orbits of such monomials x^A generate $R[x^A \mid A \text{ good}]$.

4: Run Algorithm 5.2 for the input F with respect to a monomial order that eliminates the variables Z. Since $R[x^A \mid A \text{ good}][Z]$ is the monoid algebra of a monoid where $\mathrm{Inc}(\mathbb{N})$-divisibility is a wpo, the algorithm terminates. Standard elimination theory implies that $G' = G \cap R[x^A \mid A \text{ good}]$ generates

$$I_\psi \cap R[x^A \mid A \text{ good}] = \ker\psi \cap \operatorname{im}\varphi.$$

5: Let T consist of preimages of elements in G' (one per element) and a finite number of binomials whose orbits generate $\ker\varphi$ (see Corollary 3.4).

Remark 5.6. We can execute Algorithm 5.5 for any coefficient ring R (not necessarily a field), since all polynomials that appear in the computation are binomials with coefficients ± 1.

In the following two remarks we comment on two major subroutines not spelled out in the sketch of the algorithm above.

Remark 5.7. Unlike in the usual Buchberger algorithm, the task of computing S-polynomials in Algorithm 5.2 is far from being trivial. To accomplish that, one needs to compute the set $O_{f,g}$, which can be done following the lines of the proof of Proposition 5.4. While this procedure is *effective*, by no means it is *efficient*.

Remark 5.8. In the last step of Algorithm 5.5 a preimage $\varphi^{-1}(g)$ of an element $g \in G$ can be computed by reducing the problem to one of computing maximal matchings of bipartite graphs, a well studied problem in combinatorics. Any monomial $x^A \in \operatorname{im} \varphi$ can be considered as a collection of N bipartite graphs with adjacency matrices $A_0, \dots, A_{N-1}$ as in Section 3, where each A_p has bipartition $[k_p] \sqcup \mathbb{N}$. Fixing A_p, let $S \subset \mathbb{N}$ be the set of vertices in the second partition with degree d_{A_p} (i.e., the indices of the columns of A_p with column sum equal to d_{A_p}). A matching B covering $[k_p]$ and S can be computed using the Hungarian method or other algorithms for computing weighted bipartite matchings (see [Schrijver 2003, Chapter 17] for more details). The matching B directly corresponds to a variable $y_{p,J} \in Y$ with $\varphi(y_{p,J}) = x^B$. Since B covers S, it follows that $A_p - B$ is a good matrix. Therefore $x^{A_p}/\varphi(y_{p,J})$ is also in $\operatorname{im} \varphi$ and can be decomposed further by repeating the process.

Algorithm 5.5 yields a solution to Problem 5.3(a) as an important theoretical consequence: a finite Inc($\mathbb{N}$)-generating set of the toric ideals in the main theorem is computable. However, in view of Remark 5.7 and a more elementary procedure (albeit with no termination guarantee) given in the following section that solves a harder Problem 5.3(b) for a small example, we postpone a practical implementation of Algorithm 5.5.

6. An example, and a more naïve implementation

A more elementary approach to Problem 5.3 — indeed, to the hardest variant — is, for a given order on $[Y, Z]$, to directly apply the algorithm of [Brouwer and Draisma 2011] to the graph of the entire map $\psi \circ \varphi$, rather than computing generators for the kernels of ψ and φ separately as in Algorithm 5.5. The advantages of this approach are that it is simpler to implement, and that it produces not just a generating set, but an Inc($\mathbb{N}$)-equivariant Gröbner basis. The disadvantage is that *we do not know* whether the procedure is guaranteed to terminate. We now set up a version of the usual equivariant Buchberger algorithm that is particularly easy to implement, and conclude with one nontrivial computational example.

For convenience let $\omega = \psi \circ \varphi$. Let $I_\omega \subset R[Y, Z]$ be the ideal corresponding to the graph of ω, so I_ω is generated by the binomials of the form $y - \omega(y)$ for each variable $y \in Y$. Choosing a representative $y_p = y_{p,(0,\dots,k_p-1)}$ of each $\mathrm{Sym}(\mathbb{N})$-orbit in Y, the ideal is $\mathrm{Inc}(\mathbb{N})$-generated by the finite set

$$F := \{\sigma y_p - \omega(\sigma y_p) \mid p \in [N],\ \sigma \in \mathrm{Sym}([k_p])\}.$$

Choose an $\mathrm{Inc}(\mathbb{N})$-compatible monomial order $\leq$ on $R[Y, Z]$ that eliminates Z. Then apply to F the equivariant Gröbner basis algorithm from [loc. cit.] (which is essentially Algorithm 5.2). Note that since we are working in a polynomial ring $R[Y, Z]$, rather than a more complicated monoid ring $R[X \mid X \text{ good}][Z]$, every pair of monomials has only one lcm, which is straightforward to compute. If the procedure terminates with output G, then $G \cap R[Y]$ is an $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of $I_\omega \cap R[Y] = \ker \omega$.

This procedure can be adapted to make use of existing, fast implementations of traditional Gröbner basis algorithms. For each $n \in \mathbb{N}$ truncate to the first n index values by defining

$$Y_n := \{y_{p,J} \mid J \in [n]^{k_p}\},$$
$$Z_n := \{z_{i,j} \in Z \mid j \in [n]\},$$
$$F_n := \{y - \omega(y) \mid y \in Y_n\}.$$

Let I_n be the ideal in $R[Y_n, Z_n]$ generated by F_n. Each I_n is $\mathrm{Sym}([n])$-stable and $\bigcup_{n\in\mathbb{N}} I_n = I_\omega$. Let $\mathrm{Inc}(m, n)$ be the set of all strictly increasing maps $[m] \to [n]$, and equip $K[Y_n, Z_n]$ with the restriction of the $\mathrm{Inc}(\mathbb{N})$-monomial order $\leq$.

Algorithm 6.1. $G = \textsc{truncatedBuchberger}(\omega)$

Require: $\varphi : R[Y] \to R[Z]$ is a monomial map in the main theorem.
Ensure: G is an $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of $\ker \varphi$.

$n \leftarrow \max_{p\in[N]} k_p$
while true **do**
  $F_n \leftarrow \{y - \omega(y) \mid y \in Y_n\}$
  $G_n \leftarrow \textsc{GröbnerBasis}(F_n)$
  $m \leftarrow \lfloor (n+1)/2 \rfloor$
  if $m \geq \max_{p\in[N]} k_p$ and $G_n = \mathrm{Inc}(m, n) G_m$ **then**
    $G \leftarrow G_m \cap R[Y]$
    return G
  end if
  $n \leftarrow n + 1$
end while

Here GRÖBNERBASIS denotes any algorithm to compute a traditional Gröbner basis. If TRUNCATEDBUCHBERGER(ω) terminates, this implies that there is some $m \geq \max_{p\in[N]} k_p$ such that $\mathrm{Inc}(m,n)G_m$ satisfies Buchberger's criterion for some $n \geq 2m-1$. Then G_m satisfies the equivariant Buchberger criterion, so G_m is an equivariant Gröbner basis. Because we require that $m \geq \max_{p\in[N]} k_p$, the set G_m generates I_ω up to $\mathrm{Inc}(\mathbb{N})$-action. Finally $G = G_m \cap R[Y]$ is an equivariant Gröbner basis for $\ker\omega$.

Example 6.2. Set $Y := \{y_{j_0,j_1} \mid j_0, j_1 \in \mathbb{N},\ j_0 \neq j_1\}$ and $Z := \{z_i \mid i \in \mathbb{N}\}$, each consisting of a single $\mathrm{Sym}(\mathbb{N})$-orbit, and define the monomial map $\omega\colon R[Y] \to R[Z]$ by

$$\omega : y_{j_0,j_1} \mapsto z_{j_0}^2 z_{j_1}.$$

Whether $\ker\omega$ is finitely generated was posed as an open question in [Hillar and Martín del Campo 2013] (Remark 1.6). This is answered in the affirmative by Theorem 1.1, but by applying Algorithm 6.1 we have also explicitly computed an $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis. The Gröbner basis computations were carried out using the software package *4ti2* [Hemmecke et al. 2008], which features algorithms specifically designed for computing Gröbner bases of toric ideals. The monomial order on Y is lexicographic, where variables are ordered by $y_{i,j} < y_{i',j'}$ if $i < i'$, or $i = i'$ and $j < j'$.

The result displayed in Table 1 consists of 51 generators with indices from $\{0, 1, 2, 3, 4, 5\}$ and degrees up to 5. Note that a minimal generating set resulting from a study of the family of equivariant toric maps of the form

$$y_{ij} \mapsto z_i^a z_j^b, \quad i, j \in \mathbb{N}, i \neq j,$$

for fixed $a, b \in \mathbb{N}$ in [Kahle et al. 2014] is much smaller.

Remark 6.3. As pointed out in the Introduction, the technique laid out in this article does not settle the question whether the finite generatedness of $\ker\varphi$ in the main theorem persists when $\mathrm{Inc}(\mathbb{N})$ acts with finitely many orbits on Y and the monomial map φ is required to be merely $\mathrm{Inc}(\mathbb{N})$-equivariant (though we do know that $\mathrm{im}\,\varphi$ needs not be $\mathrm{Inc}(\mathbb{N})$-Noetherian in this case).

However, a naïve elimination procedure terminates, for instance, for the $\mathrm{Inc}(\mathbb{N})$-analogue of Example 6.2, i.e., for the same map, but with the smaller set of variables

$$Y := \{y_{j_0,j_1} \mid j_0, j_1 \in \mathbb{N},\ j_0 > j_1\}.$$

A computation that can be carried out with *EquivariantGB* [Hillar et al. 2013] produces a finite number of generators of the kernel:

$$\{y_{3,1}y_{2,0} - y_{3,0}y_{2,1},\ y_{3,2}^2 y_{1,0} - y_{3,1}y_{3,0}y_{2,1},\ y_{4,2}y_{3,2}y_{1,0} - y_{4,0}y_{3,1}y_{2,1}\}.$$

degree 3

$\triangleleft\ y_{1,2}y_{0,1}^2 - y_{1,0}^2 y_{0,2}\ \triangleright$

$\triangleleft\ y_{2,0}y_{0,1}^2 - y_{1,0}y_{0,2}^2\ \triangleright$

$y_{2,1}y_{0,2}^2 - y_{2,0}^2 y_{0,1}$

$\triangleleft\ y_{2,1}y_{1,0}y_{0,2} - y_{2,0}y_{1,2}y_{0,1}\ \triangleright$

$y_{2,1}y_{1,0}^2 - y_{1,2}^2 y_{0,1}$

$y_{2,1}^2 y_{0,2} - y_{2,0}^2 y_{1,2}$

$y_{2,1}^2 y_{1,0} - y_{2,0}y_{1,2}^2$

$y_{2,1}y_{1,0}y_{0,3} - y_{2,0}y_{1,3}y_{0,1}$

$y_{2,1}^2 y_{0,3} - y_{2,0}^2 y_{1,3}$

$y_{2,3}y_{1,2}y_{0,2} - y_{2,0}^2 y_{1,3}$

$y_{3,0}y_{1,2}y_{0,2} - y_{2,0}y_{1,3}y_{0,3}$

$y_{3,0}y_{1,2}^2 - y_{2,0}y_{1,3}^2$

$y_{3,0}y_{2,1}^2 - y_{2,3}y_{2,0}y_{1,3}$

$y_{3,1}y_{0,2}^2 - y_{2,1}y_{0,3}^2$

$y_{3,1}y_{1,0}y_{0,2} - y_{3,0}y_{1,2}y_{0,1}$

$y_{3,1}y_{1,2}y_{0,2} - y_{2,1}y_{1,3}y_{0,3}$

$y_{3,1}y_{2,3}y_{0,3} - y_{3,0}^2 y_{2,1}$

$y_{3,1}^2 y_{0,2} - y_{3,0}^2 y_{1,2}$

$y_{3,2}y_{1,3}y_{0,3} - y_{3,0}^2 y_{1,2}$

$y_{3,2}y_{2,0}y_{1,3} - y_{3,0}y_{2,3}y_{1,2}$

$y_{3,2}y_{2,0}y_{1,4} - y_{3,0}y_{2,4}y_{1,2}$

$y_{3,2}y_{2,1}y_{0,3} - y_{3,1}y_{2,3}y_{0,2}$

$y_{3,2}y_{2,1}y_{0,4} - y_{3,1}y_{2,4}y_{0,2}$

$y_{4,0}y_{2,3}y_{1,3} - y_{3,0}y_{2,4}y_{1,4}$

$y_{4,1}y_{2,3}y_{0,3} - y_{3,1}y_{2,4}y_{0,4}$

$y_{4,2}y_{1,3}y_{0,3} - y_{3,2}y_{1,4}y_{0,4}$

$y_{4,2}y_{2,0}y_{1,3} - y_{4,0}y_{2,3}y_{1,2}$

$y_{4,2}y_{2,1}y_{0,3} - y_{4,1}y_{2,3}y_{0,2}$

degree 2

$\triangleleft\ y_{1,3}y_{0,2} - y_{1,2}y_{0,3}\ \triangleright$

$\triangleleft\ y_{2,0}y_{1,0} - y_{1,2}y_{0,2}\ \triangleright$

$y_{2,1}y_{0,1} - y_{1,2}y_{0,2}$

$y_{2,3}y_{0,1} - y_{2,1}y_{0,3}$

$y_{2,3}y_{1,0} - y_{2,0}y_{1,3}$

$y_{3,1}y_{2,0} - y_{3,0}y_{2,1}$

$y_{3,2}y_{0,1} - y_{3,1}y_{0,2}$

$y_{3,2}y_{1,0} - y_{3,0}y_{1,2}$

degree 4

$y_{2,1}y_{1,2}y_{0,3}y_{0,2} - y_{2,0}^2 y_{1,3}y_{0,1}$

$y_{3,1}y_{2,3}y_{1,3}y_{0,4} - y_{3,0}^2 y_{2,1}y_{1,4}$

$y_{3,1}y_{2,3}^2 y_{0,4} - y_{3,0}^2 y_{2,4}y_{2,1}$

$y_{3,2}y_{2,3}y_{1,3}y_{0,4} - y_{3,0}^2 y_{2,4}y_{1,2}$

$y_{4,1}y_{2,3}y_{1,4}y_{0,4} - y_{4,0}^2 y_{2,1}y_{1,3}$

$y_{4,1}y_{3,2}y_{1,4}y_{0,4} - y_{4,0}^2 y_{3,1}y_{1,2}$

$y_{4,1}y_{3,4}y_{2,4}y_{0,5} - y_{4,0}^2 y_{3,1}y_{2,5}$

degree 5

$y_{2,1}y_{1,2}^2 y_{0,3}^2 - y_{2,0}^2 y_{1,3}^2 y_{0,1}$

$y_{2,1}y_{1,2}^2 y_{0,4}y_{0,3} - y_{2,0}^2 y_{1,4}y_{1,3}y_{0,1}$

$y_{3,2}y_{2,3}^2 y_{1,4}y_{0,4} - y_{3,0}^2 y_{2,4}^2 y_{1,2}$

$y_{3,2}y_{2,3}^2 y_{1,4}y_{0,5} - y_{3,0}^2 y_{2,5}y_{2,4}y_{1,2}$

$y_{4,1}y_{2,3}y_{1,4}^2 y_{0,5} - y_{4,0}^2 y_{2,1}y_{1,5}y_{1,3}$

$y_{4,1}y_{3,2}y_{1,4}^2 y_{0,5} - y_{4,0}^2 y_{3,1}y_{1,5}y_{1,2}$

$y_{4,3}y_{4,0}^2 y_{3,2}y_{3,1} - y_{4,2}y_{4,1}y_{3,4}^2 y_{0,3}$

$y_{5,1}y_{4,2}y_{3,5}^2 y_{0,3} - y_{5,0}^2 y_{4,3}y_{3,2}y_{3,1}$

Table 1. An Inc($\mathbb{N}$)-equivariant Gröbner basis for the kernel of ω in Example 6.2. The five highlighted binomials form a Sym($\mathbb{N}$)-equivariant Markov basis according to [Kahle et al. 2014].

Acknowledgments

We thank a referee for pointing out the results of [Yamaguchi et al. 2014] on the Markov degree of the generalized Birkhoff model (which are stronger than a bound that we had in the original version of this paper) and for the remark that the integral polytopes capturing this model are not only normal but compressed (Remark 3.2).

References

[Allman and Rhodes 2008] E. S. Allman and J. A. Rhodes, "Phylogenetic ideals and varieties for the general Markov model", *Adv. in Appl. Math.* **40**:2 (2008), 127–148. MR 2008m:60145 Zbl 1131.92046

[Aschenbrenner and Hillar 2007] M. Aschenbrenner and C. J. Hillar, "Finite generation of symmetric ideals", *Trans. Amer. Math. Soc.* **359**:11 (2007), 5171–5192. MR 2008g:13030 Zbl 1129.13008

[Brouwer and Draisma 2011] A. E. Brouwer and J. Draisma, "Equivariant Gröbner bases and the Gaussian two-factor model", *Math. Comp.* **80**:274 (2011), 1123–1133. MR 2012g:13049 Zbl 1211.13018

[Cohen 1987] D. E. Cohen, "Closure relations. Buchberger's algorithm, and polynomials in infinitely many variables", pp. 78–87 in *Computation theory and logic*, Lecture Notes in Comput. Sci. **270**, Springer, Berlin, 1987. MR 89a:68113 Zbl 0641.68056

[Dickson 1913] L. E. Dickson, "Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Factors", *Amer. J. Math.* **35**:4 (1913), 413–422. MR 1506194 Zbl 44.0220.02

[Draisma 2010] J. Draisma, "Finiteness for the k-factor model and chirality varieties", *Adv. Math.* **223**:1 (2010), 243–256. MR 2011e:14091 Zbl 1211.13020

[Draisma and Eggermont 2015] J. Draisma and R. H. Eggermont, "Finiteness results for Abelian tree models", *J. Eur. Math. Soc.* (*JEMS*) **17**:4 (2015), 711–738. MR 3336833

[Draisma and Kuttler 2009] J. Draisma and J. Kuttler, "On the ideals of equivariant tree models", *Math. Ann.* **344**:3 (2009), 619–644. MR 2010e:62245

[Draisma and Kuttler 2014] J. Draisma and J. Kuttler, "Bounded-rank tensors are defined in bounded degree", *Duke Math. J.* **163**:1 (2014), 35–63. MR 3161311 Zbl 1314.14109

[Grayson and Stillman 2002] D. R. Grayson and M. E. Stillman, "Macaulay2, a software system for research in algebraic geometry", 2002, http://www.math.uiuc.edu/Macaulay2/.

[Gross and Petrović 2013] E. Gross and S. Petrović, "Combinatorial degree bound for toric ideals of hypergraphs", *Internat. J. Algebra Comput.* **23**:6 (2013), 1503–1520. MR 3109456 Zbl 1273.05237

[Haws et al. 2014] D. Haws, A. Martín del Campo, A. Takemura, and R. Yoshida, "Markov degree of the three-state toric homogeneous Markov chain model", *Beitr. Algebra Geom.* **55**:1 (2014), 161–188. MR 3167787 Zbl 06299286

[Hemmecke et al. 2008] R. Hemmecke, R. Hemmecke, and P. Malkin, "4ti2 — A software package for algebraic, geometric and combinatorial problems on linear spaces", 2008, www.4ti2.de. Version 1.3.2.

[Higman 1952] G. Higman, "Ordering by divisibility in abstract algebras", *Proc. London Math. Soc.* (3) **2** (1952), 326–336. MR 14,238e Zbl 0047.03402

[Hillar and Martín del Campo 2013] C. J. Hillar and A. Martín del Campo, "Finiteness theorems and algorithms for permutation invariant chains of Laurent lattice ideals", *J. Symbolic Comput.* **50** (2013), 314–334. MR 2996883 Zbl 1263.13031

[Hillar and Sullivant 2012] C. J. Hillar and S. Sullivant, "Finite Gröbner bases in infinite dimensional polynomial rings and applications", *Adv. Math.* **229**:1 (2012), 1–25. MR 2012k:16056 Zbl 1233.13012

[Hillar et al. 2013] C. Hillar, R. Krone, and A. Leykin, "EquivariantGB: Equivariant Gröbner bases in Macaulay2", 2013, http://people.math.gatech.edu/~rkrone3/EquivariantGB.html.

[Kahle et al. 2014] T. Kahle, R. Krone, and A. Leykin, "Equivariant lattice generators and Markov bases", pp. 264–271 in *ISSAC 2014—Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, edited by K. Nabeshima, ACM, New York, 2014. MR 3239935

[Kiraly and Rosen 2013] F. J. Kiraly and Z. Rosen, "Symmetries and finiteness for algebraic matroids", Poster at MEGA, 2013.

[Kruskal 1972] J. B. Kruskal, "The theory of well-quasi-ordering: A frequently discovered concept", *J. Combinatorial Theory Ser. A* **13** (1972), 297–305. MR 46 #5184 Zbl 0244.06002

[de Loera et al. 1995] J. A. de Loera, B. Sturmfels, and R. R. Thomas, "Gröbner bases and triangulations of the second hypersimplex", *Combinatorica* **15**:3 (1995), 409–424. MR 97b:13035 Zbl 0838.52015

[Nash-Williams 1963] C. S. J. A. Nash-Williams, "On well-quasi-ordering finite trees", *Proc. Cambridge Philos. Soc.* **59**:04 (1963), 833–835. MR 27 #3564 Zbl 0122.25001

[Norén 2015] P. Norén, "The three-state toric homogeneous Markov chain model has Markov degree two", *J. Symbolic Comput.* **68**:part 2 (2015), 285–296. MR 3283866 Zbl 1315.13045

[Ohsugi and Hibi 2001] H. Ohsugi and T. Hibi, "Convex polytopes all of whose reverse lexicographic initial ideals are squarefree", *Proc. Amer. Math. Soc.* **129**:9 (2001), 2541–2546. MR 2002d:13037 Zbl 0984.13014

[Pachter and Sturmfels 2005] L. Pachter and B. Sturmfels (editors), *Algebraic statistics for computational biology*, Cambridge University Press, Cambridge, 2005. MR 2006i:92002 Zbl 1108.62118

[Schrijver 2003] A. Schrijver, *Combinatorial optimization. Polyhedra and efficiency*, Algorithms and Combinatorics **24**, Springer, Berlin, 2003. MR 2004b:90004b Zbl 1041.90001

[Snowden 2013] A. Snowden, "Syzygies of Segre embeddings and Δ-modules", *Duke Math. J.* **162**:2 (2013), 225–277. MR 3018955 Zbl 1279.13024

[Sullivant 2006] S. Sullivant, "Compressed polytopes and statistical disclosure limitation", *Tohoku Math. J.* (2) **58**:3 (2006), 433–445. MR 2008g:52020 Zbl 1121.52028

[Yamaguchi et al. 2014] T. Yamaguchi, M. Ogawa, and A. Takemura, "Markov degree of the Birkhoff model", *J. Algebraic Combin.* **40**:1 (2014), 293–311. MR 3226827 Zbl 1302.62052

Communicated by Ravi Vakil
Received 2014-11-06 Revised 2015-03-06 Accepted 2015-06-12

j.draisma@tue.nl — *Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands*
Vrije Universiteit and Centrum voor Wiskunde en Informatica, Amsterdam, Netherlands

r.h.eggermont@tue.nl — *Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands*

krone@math.gatech.edu — *School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332-0160, United States*

leykin@math.gatech.edu — *School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332-0160, United States*

mathematical sciences publishers msp

ALGEBRA AND NUMBER THEORY 9:8 (2015)
dx.doi.org/10.2140/ant.2015.9.1881

On differential modules associated to de Rham representations in the imperfect residue field case

Shun Ohkubo

Let K be a complete discrete valuation field of mixed characteristic $(0, p)$ with possibly imperfect residue fields, and let G_K the absolute Galois group of K. In the first part of this paper, we prove that Scholl's generalization of fields of norms over K is compatible with Abbes–Saito's ramification theory. In the second part, we construct a functor $\mathbb{N}_{\mathrm{dR}}$ that associates a de Rham representation V to a (φ, ∇)-module in the sense of Kedlaya. Finally, we prove a compatibility between Kedlaya's differential Swan conductor of $\mathbb{N}_{\mathrm{dR}}(V)$ and the Swan conductor of V, which generalizes Marmora's formula.

Introduction

Hodge theory relates the singular cohomology of complex projective manifolds X to the spaces of harmonic forms on X. Its p-adic analogue, p-adic Hodge theory, enables us to compare the p-adic étale cohomology $H^m_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ of proper smooth varieties X over the p-adic field $\mathbb{Q}_p$ with the de Rham cohomology of X. Precisely speaking, the natural action of the absolute Galois group $G_{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ on the p-adic étale cohomology can be recovered after tensoring both cohomologies with $\mathbb{B}_{\mathrm{dR}}$, which is the ring of p-adic periods introduced by Jean-Marc Fontaine. If X has

MSC2010: 11S15.
Keywords: p-adic Hodge theory, ramification theory.

semistable reduction, then one can obtain a more precise comparison theorem between the p-adic étale cohomology of X and the log-cristalline cohomology of the special fiber of X. Thus, we have a satisfactory p-adic étale cohomology theory on proper smooth varieties over $\mathbb{Q}_p$.

A p-adic representation V of $G_{\mathbb{Q}_p}$ is a finite dimensional $\mathbb{Q}_p$-vector space with a continuous linear $G_{\mathbb{Q}_p}$-action. Fontaine [1994] defined the notions of de Rham, crystalline, and semistable representations, which form important subcategories of the category of p-adic representations of $G_{\mathbb{Q}_p}$. Then, he associated linear algebraic objects such as filtered vector spaces with extra structures to objects in each category. Fontaine's classification is compatible with geometry in the following sense: for a proper smooth variety X over $\mathbb{Q}_p$, the p-adic representation $H^m_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ of $G_{\mathbb{Q}_p}$ is only de Rham in general. However, if X has a semistable reduction (resp. good reduction), then $H^m_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ is semistable (resp. crystalline).

There also exists a more analytic description of general p-adic representations. Let $\mathbb{B}_{\mathbb{Q}_p}$ be the fraction field of the p-adic completion of $\mathbb{Z}_p[[t]][1/t]$. We define the action of $\Gamma_{\mathbb{Q}_p} := G_{\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p}$ on $\mathbb{B}_{\mathbb{Q}_p}$ by $\gamma(t) = (1+t)^{\chi(g)} - 1$, where $\chi : \Gamma_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ is the cyclotomic character. We also define a Frobenius lift φ on $\mathbb{B}_{\mathbb{Q}_p}$ by $\varphi(t) = (1+t)^p - 1$. An étale $(\varphi, \Gamma_{\mathbb{Q}_p})$-module over $\mathbb{B}_{\mathbb{Q}_p}$ is a finite dimensional $\mathbb{B}_{\mathbb{Q}_p}$-vector space M endowed with compatible actions of φ and $\Gamma_{\mathbb{Q}_p}$such that the Frobenius slopes of M are all zero. Using Fontaine–Wintenberger's isomorphism

$$G_{\mathbb{Q}_p(\mu_{p^\infty})} \cong G_{\mathbb{F}_p((t))},$$

of Galois groups, Fontaine [1990] proved an equivalence between the category of p-adic representations and the category of étale $(\varphi, \Gamma_{\mathbb{Q}_p})$-modules over $\mathbb{B}_{\mathbb{Q}_p}$. We consider the overconvergent subring

$$\mathbb{B}^\dagger_{\mathbb{Q}_p} := \left\{ \sum_{n\in\mathbb{Z}} a_n t^n \in \mathbb{B}_{\mathbb{Q}_p};\ a_n \in \mathbb{Q}_p, |a_n|\rho^n \to 0 \text{ for some } \rho \in (0,1] \text{ and } n \to -\infty \right\}$$

of $\mathbb{B}_{\mathbb{Q}_p}$. Frédéric Cherbonnier and Pierre Colmez [1998] proved that the category of étale $(\varphi, \Gamma_{\mathbb{Q}_p})$-modules over $\mathbb{B}_{\mathbb{Q}_p}$ is equivalent to the category of étale $(\varphi, \Gamma_{\mathbb{Q}_p})$-modules over $\mathbb{B}^\dagger_{\mathbb{Q}_p}$. As a consequence of Cherbonnier–Colmez' theorem, p-adic analysis over the Robba ring

$$\mathcal{R}_{\mathbb{Q}_p} := \bigcup_{\rho'\in(0,1)} \left\{ \sum_{n\in\mathbb{Z}} a_n t^n;\ a_n \in \mathbb{Q}_p, |a_n|\rho^n \to 0 \text{ for all } \rho \in (\rho', 1] \text{ and } n \to \pm\infty \right\}$$

comes into play. Actually, via the above equivalences, Laurent Berger [2002] associated a p-adic differential equation $\mathbb{N}_{\text{dR}}(V)$ over $\mathcal{R}_{\mathbb{Q}_p}$ to a de Rham representation V. By using this functor $\mathbb{N}_{\text{dR}}$ and the quasi-unipotence of p-adic differential equations due to Yves André, Zoghman Mebkhout and Kiran Kedlaya, Berger proved Fontaine's p-adic local monodromy conjecture, which is a p-adic analogue of Grothendieck's l-adic monodromy theorem. We note that in the above theory,

$G_{\mathbb{Q}_p}$ is usually replaced by G_K, where K is a complete valuation field of mixed characteristic $(0, p)$ with a perfect residue field.

Recently, based on earlier work of Gerd Faltings and Osamu Hyodo, Fabrizio Andreatta and Olivier Brinon [2008] started to generalize Fontaine's theory in the relative situation: instead of complete discrete valuation rings with perfect residue fields, they work over higher dimensional ground rings R such as the generic fiber of the Tate algebra $\mathbb{Z}_p\{T_1, T_1^{-1}, \dots, T_d, T_d^{-1}\}$. In this paper, we work in the most basic case of Andreatta–Brinon's setup. That is, our ground ring K is still a complete valuation field, but it has a nonperfect residue field k_K such that $p^d = [k_K : k_K^p] < \infty$. Such a complete discrete valuation field arises as the completion of a ground ring along the special fiber in Andreatta–Brinon's setup.

Even in our situation, a generalization of Fontaine's theory could be useful as in the proof of Kato's divisibility result [2004] in the Iwasawa main conjecture for GL_2. Using compatible systems of K_2 of affine modular curves $Y(p^n N)$ for varying n, Kato defines (p-adic) Euler systems in Galois cohomology groups over $\mathbb{Q}_p$ whose coefficients are related to cusp forms. A key ingredient in this paper is that Kato's Euler systems are related with some products of Eisenstein series via Bloch–Kato's dual exponential map exp*. In the proof of this fact, p-adic Hodge theory for "the field of q-expansions" $\mathcal{K}$ plays an important role, where $\mathcal{K}$ is the fraction field of the p-adic completion of $\mathbb{Z}_p[\zeta_{p^N}][[q^{1/N}]][q^{-1}]$. Roughly speaking, Tate's universal elliptic curve together with its torsion points induces a morphism $\mathrm{Spec}(\mathcal{K}(\zeta_{p^n}, q^{p^{-n}})) \to Y(p^n N)$. Using a generalization of Fontaine's ring $\mathbb{B}_{\mathrm{dR}}$ over $\mathcal{K}$, Kato defines a dual exponential map for Galois cohomology groups over $\mathcal{K}(\zeta_{p^n}, q^{p^{-n}})$, and proves its compatibility with exp*. Then, the image of Kato's Euler system under exp* is calculated by using Kato's generalized explicit reciprocity law for p-divisible groups over $\mathcal{K}(\zeta_{p^n}, q^{p^{-n}})$.

To explain our results, we recall Anthony Scholl's theory [2006] of field of norms, which is a generalization of Fontaine–Wintenberger's theorem when k_K is nonperfect. In the rest of the introduction we restrict ourselves for simplicity to the "Kummer tower case": we choose a lift $\{t_j\}_{1\le j\le d}$ of a p-basis of k_K and define a tower $\mathfrak{K} := \{K_n\}_{n>0}$ of fields by $K_n := K(\mu_{p^n}, t_1^{p^{-n}}, \dots, t_d^{p^{-n}})$ for $n > 0$, and set $K_\infty := \bigcup_n K_n$. Then, the Frobenius on $\mathcal{O}_{K_{n+1}}/p\mathcal{O}_{K_{n+1}}$ factors through $\mathcal{O}_{K_n}/p\mathcal{O}_{K_n} \hookrightarrow \mathcal{O}_{K_{n+1}}/p\mathcal{O}_{K_{n+1}}$, and the limit $X_{\mathfrak{K}}^+ := \varprojlim_n \mathcal{O}_{K_n}/p\mathcal{O}_{K_n}$ is a complete valuation ring of characteristic p. Here, we denote the integer ring of a valuation field F by $\mathcal{O}_F$. Let $X_{\mathfrak{K}}$ be the fraction field of $X_{\mathfrak{K}}^+$. Then, Scholl proved that a similar limit procedure gives an equivalence of categories $\mathbf{FÉt}_{K_\infty} \cong \mathbf{FÉt}_{X_{\mathfrak{K}}}$, where $\mathbf{FÉt}_A$ denotes the category of finite étale algebras over A. In particular, we obtain an isomorphism of Galois groups

$$\tau : G_{K_\infty} \xrightarrow{\sim} G_{X_{\mathfrak{K}}}.$$

The Galois group of a complete valuation field F is canonically endowed with nonlog and log ramification filtrations in the sense of [Abbes and Saito 2002]. By using the ramification filtrations, one can define Artin and Swan conductors of Galois representations, which are important arithmetic invariants. It is natural to ask that Scholl's isomorphism τ is compatible with ramification theory. The first goal of this paper is to answer this question in the following form:

Theorem 0.0.1 (Theorem 3.5.3). *Let V be a p-adic representation of G_K, where the G_K-action of V factors through a finite quotient. Then, the Artin and Swan conductors of $V|_{K_n}$ are stationary and their limits coincide with the Artin and Swan conductors of $\tau^*(V|_{K_\infty})$.*

We briefly mention the idea of the proof in the Artin case. Note that in the perfect residue field case, the result follows from the fact that the upper numbering ramification filtration is a renumbering of the lower numbering one, and this latter filtration is compatible with the field of norms construction; see [Marmora 2004, Lemme 5.4]. However, in the imperfect residue field case, since Abbes–Saito's ramification filtration is not a renumbering of the lower numbering one, we proceed as follows. Let L/K be a finite Galois extension. Let $X_{\mathfrak{L}}$ be an extension of $X_{\mathfrak{K}}$ corresponding to the tower $\mathfrak{L} = \{L_n := LK_n\}_{n>0}$ under Scholl's equivalence. Then, it suffices to prove that the nonlog ramification filtrations of G_{L_n/K_n} and $G_{X_{\mathfrak{L}}/X_{\mathfrak{K}}}$ coincide with each other. Abbes–Saito's nonlog ramification filtration of a finite extension E/F of complete discrete valuation fields is described by a certain family of rigid analytic spaces $as^a_{E/F}$ for $a \in \mathbb{Q}_{\geq 0}$ attached to E/F. In terms of Abbes–Saito's setup, we only have to prove that the number of connected components of $as^a_{X_{\mathfrak{L}}/X_{\mathfrak{K}}}$ and $as^a_{L_n/K_n}$ are the same for sufficiently large n. An optimized proof of this assertion is as follows: we construct a characteristic 0 lift R of $X^+_{\mathfrak{K}}$, which is realized as the ring of functions on the open unit ball over a complete valuation ring. We can find a prime ideal $\mathfrak{p}_n$ of R such that $R/\mathfrak{p}_n$ is isomorphic to $\mathcal{O}_{K_n}$. Then, we construct a lift $AS^a_{X_{\mathfrak{L}}/X_{\mathfrak{K}}}$ over $\mathrm{Spec}(R)$ of $as^a_{X_{\mathfrak{L}}/X_{\mathfrak{K}}}$, whose generic fiber at $\mathfrak{p}_n$ is isomorphic to $as^a_{L_n/K_n}$. We may also regard $AS^a_{X_{\mathfrak{L}}/X_{\mathfrak{K}}}$ as a family of rigid spaces parametrized by $\mathrm{Spec}(R)$. What we actually prove is that in such a family of rigid spaces over $\mathrm{Spec}(R)$, the number of the connected components of the fiber varies "continuously". This is done by Gröbner basis arguments over complete regular local rings, extending the method of Liang Xiao [2010]. The continuity result implies our assertion since the point $\mathfrak{p}_n \in \mathrm{Spec}(R)$ "converges" to the point $(p) \in \mathrm{Spec}(R)$.

Note that Shin Hattori reproved [2014] the above ramification compatibility of Scholl's isomorphism τ by using Peter Scholze's perfectoid spaces [2012], which form a geometric interpretation of the Fontaine–Wintenberger theorem. We briefly explain Hattori's proof. Let $\mathbb{C}_p$ (resp. $\mathbb{C}_p^\flat$) be the completion of the algebraic closure of K_∞ (resp. $X_{\mathfrak{K}}$). Scholze proved the tilting equivalence between certain adic spaces (resp. perfectoid spaces) over $\mathbb{C}_p$ and $\mathbb{C}_p^\flat$. Let C be a perfectoid field and Y a subvariety of $\mathbb{A}^n_C$. A perfection of Y is the perfectoid space defined as the pull-back of Y under the canonical projection $\varprojlim_{T_i\mapsto T_i^p}\mathbb{A}^n_C \to \mathbb{A}^n_C$, where $T_1,\dots,T_n$ denotes a coordinate of $\mathbb{A}^n_C$. Hattori proved that the tilting of the perfections of $(as^a_{L_n/K_n})_{\mathbb{C}_p}$ and $(as^a_{X_{\mathfrak{L}}/X_{\mathfrak{K}}})_{\mathbb{C}_p^\flat}$ are isomorphic under the tilting equivalence. Since the underlying topological spaces are homeomorphic under taking perfections and the tilting equivalence, he obtained the ramification compatibility.

The second goal of this paper is to generalize Berger's functor $\mathbb{N}_{\mathrm{dR}}$ and prove a ramification compatibility of $\mathbb{N}_{\mathrm{dR}}$ which extends Theorem 0.0.1. Precisely, we construct a functor from the category of de Rham representations to the category of (φ,∇)-modules over the Robba ring. Our target objects (φ,∇)-modules are defined by Kedlaya [2007] as generalizations of p-adic differential equations. Kedlaya also defined the differential Swan conductor $\mathrm{Swan}^\nabla(M)$ for a (φ,∇)-module M, which is a generalization of the irregularity of p-adic differential equations. Then, we prove the following de Rham version of Theorem 0.0.1:

Theorem 0.0.2 (Theorem 4.7.1). *Let V be a de Rham representation of G_K. Then we have*

$$\mathrm{Swan}^\nabla(\mathbb{N}_{\mathrm{dR}}(V)) = \lim_{n\to\infty}\mathrm{Swan}(V|_{K_n}),$$

where Swan *on the right-hand side means Abbes–Saito's Swan conductor. Moreover, the sequence* $\{\mathrm{Swan}(V|_{K_n})\}_{n>0}$ *is eventually stationary.*

Both Theorems 0.0.1 and 0.0.2 are due to Adriano Marmora [2004] when the residue field is perfect. Even when the residue field is perfect, our proof of Theorem 0.0.2 is slightly different from Marmora's proof since we use a dévissage argument to reduce to the pure slope case. As is addressed in [Kedlaya 2007, §3.7], it seems to be possible to define a ramification invariant of $\mathbb{N}_{\mathrm{dR}}(V)$ in terms of (φ,Γ_K)-modules so that one can compute $\mathrm{Swan}(V)$ instead of $\mathrm{Swan}(V|_{K_n})$. It is also important to extend the construction of $\mathbb{N}_{\mathrm{dR}}$ to the general relative case: one may expect that a relative version of slope theory, described in [Kedlaya 2013] for example, will be an important tool.

Structure of the paper

In Section 1, we gather various basic results used in this paper. These contain some p-adic Hodge theory, Abbes–Saito's ramification theory, Kedlaya's theory of overconvergent rings, and Scholl's fields of norms. In Section 2, we prove some ring theoretic properties of overconvergent rings by using Kedlaya's slope theory. In Section 3, we develop a Gröbner basis argument over complete regular local rings and overconvergent rings. We apply the Gröbner basis argument to study families of rigid spaces, and use it to prove Theorem 0.0.1. In Section 4, we generalize Berger's gluing argument to construct a differential module $\mathbb{N}_{\mathrm{dR}}(V)$ for de Rham representations V. We also study the graded pieces of $\mathbb{N}_{\mathrm{dR}}(V)$ with respect to Kedlaya's slope filtration to reduce Theorem 0.0.2 to Theorem 0.0.1 by dévissage.

Convention

Throughout this paper, let p be a prime number. All rings are assumed to be commutative unless otherwise stated. For a ring R, denote by $\pi_0^{\mathrm{Zar}}(R)$ the set of connected components of $\mathrm{Spec}(R)$ with respect to the Zariski topology. For a field E, fix an algebraic closure, denoted by E^{alg} or $\overline{E}$, and a separable closure E^{sep}. Let $G_{F/E}$ be the Galois group of a finite extension F/E, and let G_E be the absolute Galois group of E. For a field k of characteristic p, let $k^{\mathrm{pf}} := k^{p^{-\infty}}$ be the perfect closure in a fixed algebraic closure of k.

For a complete valuation field K, we let $\mathcal{O}_K$ be its integer ring, π_K a uniformizer, and k_K the residue field. Let $v_K : K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation satisfying $v_K(\pi_K) = 1$. We let K^{ur} be the p-adic completion of the maximal unramified extension of K and denote by I_K the inertia subgroup of G_K. We assume that K is of mixed characteristic $(0, p)$ and that $[k_K : k_K^p] = p^d < \infty$ in the rest of this paragraph. Let e_K be the absolute ramification index. Let $\mathbb{C}_p$ be the p-adic completion of K^{alg} and let v_p be the p-adic valuation of $\mathbb{C}_p$, normalized by $v_p(p) = 1$. We fix a system of p-power roots of unity $\{\zeta_{p^n}\}_{n>0}$ in K^{alg}, i.e., ζ_p is a primitive p-th root of unity and $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for all $n \in \mathbb{N}_{>0}$. Let $\chi : G_K \to \mathbb{Z}_p^\times$ be the cyclotomic character defined by $g(\zeta_{p^n}) = \zeta_{p^n}^{\chi(g)}$ for all $n > 0$. We denote the fraction field of a Cohen ring of k_K by K_0. Denote a lift of a p-basis of k_K in $\mathcal{O}_K$ by $\{t_j\}_{1\le j\le d}$. For a given $\{t_j\}_{1\le j\le d}$, we can choose an embedding $K_0 \hookrightarrow K$ such that $\{t_j\}_{1\le j\le d} \subset \mathcal{O}_{K_0}$, see [Ohkubo 2013, §1.1]. Unless otherwise stated, we always choose $\{t_j\}_{1\le j\le d}$ and an embedding $K_0 \hookrightarrow K$ in this way, and we fix sequences of p-power roots $\{t_j^{p^{-n}}\}_{n\ge 0, 1\le j\le d}$ of $\{t_j\}_{1\le j\le d}$ in K^{alg}, i.e., we have $\big(t_j^{p^{-n-1}}\big)^p = t_j^{p^{-n}}$ for all $n > 0$. For such a sequence, we define K^{pf} as the p-adic completion of $\bigcup_n K\big(\{t_j^{p^{-n}}\}_{1\le j\le d}\big)$. This is a complete discrete valuation field with perfect residue field k_K^{pf}, and we regard $\mathbb{C}_p$ as the p-adic completion of the algebraic closure of K^{pf}.

For a ring R, let $W(R)$ be the Witt ring with coefficients in R. If R is of characteristic p, then we denote the absolute Frobenius on R by φ and also denote the ring homomorphism $W(\varphi) : W(R) \to W(R)$ by φ. Let $[x] \in W(R)$ be the Teichmüller lift of $x \in R$.

For an integer $h > 0$, define $\mathbb{Q}_{p^h} := W(\mathbb{F}_{p^h})[1/p]$. Let K be a complete discrete valuation field, and $F/\mathbb{Q}_p$ a finite extension. A finite dimensional F-vector space V with continuous semilinear G_K-action is called an F-representation of G_K. If moreover $F = \mathbb{Q}_p$, then we call V a p-adic representation of G_K. We denote the category of F-representations of G_K by $\mathrm{Rep}_F(G_K)$. We say that V is finite (resp.

of finite geometric monodromy) if G_K (resp. I_K) acts on V via a finite quotient. We denote the category of finite (resp. finite geometric monodromy) F-representations of G_K by $\mathrm{Rep}_F^{f}(G_K)$ (resp. $\mathrm{Rep}_F^{f.g.}(G_K)$).

For homomorphisms $f, g : M \to N$ of abelian groups, we denote by $M^{f=g}$ the kernel of the map $f - g$. For $x \in \mathbb{R}$, let $\lfloor x \rfloor := \inf\{n \in \mathbb{Z};\ n \geq x\}$ be the least integer greater than or equal to x. We let $\mathbb{N} = \mathbb{Z}_{\geq 0}$ be the set of all natural numbers.

1. Preliminaries

In this section, we fix notation and recall basic results needed in this paper.

1.1. ***Fréchet spaces.*** We will define some basic terminology of topological vector spaces. Although we will use both valuations and norms to consider topologies, we will define our terminology in terms of valuations for simplicity. See [Kedlaya 2010] or [Schneider 2002] for details.

Notation 1.1.1. Let M be an abelian group. A valuation v of M is a map $v : M \to \mathbb{R} \cup \{\infty\}$ such that $v(x - y) \geq \inf\{v(x), v(y)\}$ for all $x, y \in R$ and $v(x) = \infty$ if and only if $x = 0$. Moreover, when $M = R$ is a ring, v is multiplicative if $v(xy) = v(x) + v(y)$ for all $x, y \in R$. A ring equipped with a multiplicative valuation is called a valuation ring. If (R, v) is a valuation ring and (M, v_M) is an R-module with valuation v_M, then we say that v_M is an R-valuation if $v_M(\lambda x) = v(\lambda) + v_M(x)$ holds for all $\lambda \in R$ and $x \in M$.

Let (R, v) be a valuation ring and M a finite free R-module. For an R-basis $e_1, \dots, e_n$ of M, we define the R-valuation v_M on M (compatible with v) associated to $e_1, \dots, e_n$ by $v_M\bigl(\sum_{1\leq i\leq n} a_i e_i\bigr) = \inf_i v(a_i)$ for $a_i \in R$ ([Kedlaya 2010, Definition 1.3.2]). The topology defined by v_M is independent of the choice of a basis of M ([Kedlaya 2010, Definition 1.3.3]). Hence, we do not refer to a basis to consider v_M and we just denote v_M by v unless otherwise stated.

For any valuation v on M, we define the associated nonarchimedean norm $|\cdot| : M \to \mathbb{R}$ by $|x| := a^{-v(x)}$ for a fixed $a \in \mathbb{R}_{>1}$ (nonarchimedean means that it satisfies the strong triangle inequality). Conversely, for any nonarchimedean norm $|\cdot|$, $v(\cdot) = -\log_a |\cdot|$ is a valuation. We will apply various definitions made for norms to valuations, and vice versa in this manner.

Notation 1.1.2. Let (K, v) be a complete valuation field. Let $\{w_r\}_{r\in I}$ be a family of K-valuations of a K-vector space V. Consider the topology $\mathcal{T}$ of V whose neighborhoods at 0 are generated by $\{x \in V;\ w_r(x) \geq n\}$ for all $r \in I$ and $n \in \mathbb{N}$. We call $\mathcal{T}$ the topology of V defined by $\{w_r\}_{r\in I}$ and denote the topological space V with this topology by $(V, \{w_r\}_{r\in I})$, or simply by V. If $\mathcal{T}$ is equivalent to the topology defined by $\{w_r\}_{r\in I_0}$ for some countable subset $I_0 \subset I$, we call $\mathcal{T}$ the K-Fréchet topology defined by $\{w_r\}_{r\in I}$. For a K-vector space, it is well-known that a K-Fréchet topology is metrizable (and vice versa). Moreover, when V is complete, we call V a K-Fréchet space. Note that V is just a K-Banach space when $\#I_0 = 1$. Also, note that a topological K-vector space V is a K-Fréchet space if and only if V is isomorphic to an inverse limit of K-Banach spaces whose transition maps consist of bounded K-linear maps. More precisely, let V be a K-Fréchet space with valuations $w_0 \geq w_1 \geq \dots$, and V_n the completion of V with respect to w_n. Then the canonical map $V \to \varprojlim_n V_n$ is an isomorphism of K-Fréchet spaces. Also, note that if V and W are K-Fréchet spaces, then $\mathrm{Hom}_K(V, W)$ is again a K-Fréchet space with respect to the operator norm.

Let $(R, \{w_r\}_{r\in I})$ be a K-Fréchet space for a ring R. If $\{w_r\}_{r\in I}$ are multiplicative, then we call R a K-Fréchet algebra. For a finite free R-module M, we choose a basis of M and let $\{w_{r,M}\}_{r\in I}$ be the R-valuations compatible with $\{w_r\}_{r\in I}$. Obviously, $(M, \{w_{r,M}\}_{r\in I})$ is a K-Fréchet space. Unless otherwise stated, we always endow a finite free R-module with such a family of valuations.

In the rest of the paper, we omit the prefix "K" unless otherwise stated.

Recall that the category of Fréchet spaces is closed under quotients, completed tensor products and direct sums and that the open mapping theorem holds.

1.2. *Continuous derivations over K.* In this subsection, we recall the continuous Kähler differentials ([Hyodo 1986, §4]). Let K be a complete discrete valuation field of mixed characteristic $(0, p)$ such that $[k_K : k_K^p] = p^d < \infty$.

Definition 1.2.1. Let $\widehat{\Omega}^1_{\mathcal{O}_K}$ be the p-adic Hausdorff completion of $\Omega^1_{\mathcal{O}_K/\mathbb{Z}}$ and put $\widehat{\Omega}^1_K := \widehat{\Omega}^1_{\mathcal{O}_K}[1/p]$. Let $d : K \to \widehat{\Omega}^1_K$ be the canonical derivation.

Recall that $\widehat{\Omega}^1_K$ is a finite K-vector space with basis $\{dt_j\}_{1\leq j\leq d}$. Moreover, if K is absolutely unramified, then $\widehat{\Omega}^1_{\mathcal{O}_K}$ is a finite free $\mathcal{O}_K$-module with basis $\{dt_j\}_{1\leq j\leq d}$. Also, $\widehat{\Omega}^1_\bullet$ is compatible with base change, i.e., $L \otimes_K \widehat{\Omega}^1_K \cong \widehat{\Omega}^1_L$ for any finite extension L/K.

Notation 1.2.2. Let R be a topological ring and M a topological R-module. We let $\mathrm{Der}_{\mathrm{cont}}(R, M)$ be the R-module of continuous derivations $d : R \to M$.

One can prove the next lemma by dévissage and the universality of the usual Kähler differentials.

Lemma 1.2.3. *For an inductive limit M of K-Fréchet spaces, we have the canonical isomorphism*

$$d^* : \mathrm{Hom}_K(\widehat{\Omega}^1_K, M) \xrightarrow{\sim} \mathrm{Der}_{\mathrm{cont}}(K, M).$$

Definition 1.2.4. Let $\{\partial_j\}_{1\leq j\leq d} \subset \mathrm{Der}_{\mathrm{cont}}(K_0, K_0) \cong \mathrm{Hom}_{K_0}(\Omega^1_{K_0}, K_0)$ be the dual basis of $\{dt_j\}_{1\leq j\leq d}$. We call $\{\partial_j\}$ the derivations associated to $\{t_j\}$. We also denote by ∂_j the canonical extension of ∂_j to $\partial_j : K^{\mathrm{alg}} \to K^{\mathrm{alg}}$. Since $\partial_j(t_i) = \delta_{ij}$, we may denote ∂_j by $\partial/\partial t_j$.

1.3. ***Some Galois extensions.*** In this subsection, we will fix some notation of a certain Kummer extension which will be studied later. See [Hyodo 1986, §1] for details. In this subsection, let $\widetilde{K}$ be an absolutely unramified complete discrete valuation field of mixed characteristic $(0, p)$ with $[k_{\widetilde{K}} : k_{\widetilde{K}}^p] = p^d < \infty$. We put

$$\widetilde{K}_n := \widetilde{K}(\zeta_{p^n}, t_1^{p^{-n}}, \dots, t_1^{p^{-n}}) \text{ for } n > 0,\ \widetilde{K}_\infty := \bigcup_{n>0} \widetilde{K}_n,\ \widetilde{K}_{\text{arith}} := \bigcup_{n>0} \widetilde{K}(\zeta_{p^n}),$$

$$\Gamma_{\widetilde{K}}^{\text{geom}} := G_{\widetilde{K}_\infty/\widetilde{K}_{\text{arith}}},\quad \Gamma_{\widetilde{K}}^{\text{arith}} := G_{\widetilde{K}_{\text{arith}}/\widetilde{K}},$$
$$\Gamma_{\widetilde{K}} := G_{\widetilde{K}_\infty/\widetilde{K}},\qquad H_{\widetilde{K}} := G_{\widetilde{K}^{\text{alg}}/\widetilde{K}_\infty}.$$

Then, we have isomorphisms

$$\Gamma_{\widetilde{K}}^{\text{arith}} \cong \mathbb{Z}_p^\times,\quad \Gamma_{\widetilde{K}}^{\text{geom}} \cong \mathbb{Z}_p^d,$$

which are compatible with the action of $\Gamma_{\widetilde{K}}^{\text{arith}}$ on $\Gamma_{\widetilde{K}}^{\text{geom}}$. The isomorphisms are defined as follows: an element $a \in \mathbb{Z}_p^\times$ corresponds to $\gamma_a \in \Gamma_{\widetilde{K}}^{\text{arith}}$ such that $\gamma_a(\zeta_{p^n}) = \zeta_{p^n}^a$ for all n. An element $b = (b_j) \in \mathbb{Z}_p^d$ corresponds to $\gamma_b \in \Gamma^{\text{geom}}$ for $1 \le j \le d$ such that $\gamma_b(\zeta_{p^n}) = \zeta_{p^n}$ for all $n \in \mathbb{N}$ and $\gamma_b(t_j^{p^{-n}}) = \zeta_{p^n}^{b_j} t_j^{p^{-n}}$. By regarding $\Gamma_{\widetilde{K}}^{\text{arith}}$ as a subgroup $G_{\widetilde{K}_\infty/\bigcup_n \widetilde{K}\left(t_1^{p^{-n}},\dots,t_1^{p^{-n}}\right)}$ of $\Gamma_{\widetilde{K}}$, we obtain isomorphisms

$$\eta = (\eta_0, \dots, \eta_d) : \Gamma_{\widetilde{K}} \cong \Gamma_{\widetilde{K}}^{\text{arith}} \ltimes \Gamma_{\widetilde{K}}^{\text{geom}} \cong \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^d.$$

Since we have a canonical isomorphism

$$\mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^d \cong \begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p & \dots & \mathbb{Z}_p \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \le \mathrm{GL}_{d+1}(\mathbb{Z}_p),$$

the group $\Gamma_{\widetilde{K}}$ can be regarded as a classical p-adic Lie group with Lie algebra

$$\mathfrak{g} := \mathrm{Lie}(\Gamma_{\widetilde{K}}) \cong \mathbb{Q}_p \ltimes \mathbb{Q}_p^d = \begin{pmatrix} \mathbb{Q}_p & \dots & \mathbb{Q}_p \\ & 0 & \end{pmatrix} \subset \mathfrak{gl}_{d+1}(\mathbb{Q}_p).$$

For an integer $n > 0$ and a finite extension $L/\widetilde{K}$, we put

$$L_n := \widetilde{K}_n L,\qquad L_\infty := \widetilde{K}_\infty L,$$
$$\Gamma_L := G_{L_\infty/L},\quad H_L := G_{\widetilde{K}^{\text{alg}}/L_\infty}.$$

Then, Γ_L is an open subgroup of $\Gamma_{\widetilde{K}}$. Hence, there exists an open normal subgroup of Γ_L which is isomorphic to an open subgroup of $(1+2p\mathbb{Z}_p) \ltimes \mathbb{Z}_p^d$ by the map η. Also, we may identify the p-adic Lie algebra of Γ_L with $\mathfrak{g}$. Finally, we define closed subgroups of Γ_L

$$\Gamma_{L,0} := \{\gamma \in \Gamma_L;\ \eta_j(\gamma) = 0 \ \text{ for all } 1 \le j \le d\},$$
$$\Gamma_{L,j} := \{\gamma \in \Gamma_L;\ \eta_0(\gamma) = 1, \eta_i(\gamma) = 0 \text{ for all } 1 \le i \le d, i \ne j\} \ \text{ for } 1 \le j \le d.$$

1.4. ***Basic construction of Fontaine's rings.*** In this subsection, we recall the definition of rings of p-adic periods due to Fontaine, see [Ohkubo 2013, §3] for details.

Let K be a complete discrete valuation field of mixed characteristic (0, p) with $[k_K : k_K^p] = p^d < \infty$. Let $\widetilde{\mathbb{E}}^+ := \varprojlim_n \mathcal{O}_{\mathbb{C}_p}/p\mathcal{O}_{\mathbb{C}_p}$, where the transition maps are given by the Frobenius. This is a complete valuation ring of characteristic p whose (algebraically closed) fractional field is denoted by $\widetilde{\mathbb{E}}$. We have a canonical identification

$$\widetilde{\mathbb{E}} \cong \left\{(x^{(n)})_{n\in\mathbb{N}} \in \mathbb{C}_p^{\mathbb{N}};\ (x^{(n+1)})^p = x^{(n)} \text{ for all } n \in \mathbb{N}\right\}.$$

For $x \in \mathbb{C}_p$, we denote by $\tilde{x} \in \widetilde{\mathbb{E}}$ an element $\tilde{x} = (x^{(n)})$ such that $x^{(0)} = x$. In particular, we put $\varepsilon := (1, \zeta_p, \zeta_{p^2}, \dots)$, $\tilde{t}_j := (t_j, t_j^{1/p}, \dots) \in \widetilde{\mathbb{E}}^+$. We define the valuation $v_{\widetilde{\mathbb{E}}}$ of $\widetilde{\mathbb{E}}$ by $v_{\widetilde{\mathbb{E}}}((x^{(n)})) = v_p(x^{(0)})$. We put

$$\widetilde{\mathbb{A}}^+ := W(\widetilde{\mathbb{E}}^+) \subset \widetilde{\mathbb{A}} := W(\widetilde{\mathbb{E}}),$$
$$\widetilde{\mathbb{B}}^+ := \widetilde{\mathbb{A}}^+[1/p] \subset \widetilde{\mathbb{B}} := \widetilde{\mathbb{A}}[1/p],$$
$$\pi := [\varepsilon] - 1, \quad q := \pi/\varphi^{-1}(\pi) = \sum_{0\le i<p} \left[\varepsilon^{1/p}\right]^i \in \widetilde{\mathbb{A}}^+$$

and we define a surjective ring homomorphism

$$\theta : \widetilde{\mathbb{B}}^+ \to \mathbb{C}_p$$
$$\sum_{n\gg-\infty} p^n[x_n] \mapsto p^n x_n^{(0)},$$

which maps $\widetilde{\mathbb{A}}^+$ to $\mathcal{O}_{\mathbb{C}_p}$. Note that q is a generator of the kernel of $\theta|_{\widetilde{\mathbb{A}}^+}$.

Let $\mathcal{K}$ be a closed subfield of $\mathbb{C}_p$ whose value group $v_p(\mathcal{K}^\times)$ is discrete. We will define rings

$$\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}, \quad \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}, \quad \mathbb{B}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}.$$

Let $\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}$ be the universal p-adically formal pro-infinitesimal $\mathcal{O}_{\mathcal{K}}$-thickening of $\mathcal{O}_{\mathbb{C}_p}$. More precisely, if $\theta_{\mathbb{C}_p/\mathcal{K}} : \mathcal{O}_{\mathcal{K}} \otimes_{\mathbb{Z}} \widetilde{\mathbb{A}}^+ \to \mathcal{O}_{\mathbb{C}_p}$ denotes the linear extension of θ, then $\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}$ is the $(p, \ker\theta_{\mathbb{C}_p/\mathcal{K}})$-adic Hausdorff completion of $\mathcal{O}_{\mathcal{K}} \otimes_{\mathbb{Z}} \widetilde{\mathbb{A}}^+$. The map $\theta_{\mathbb{C}_p/\mathcal{K}}$ extends to $\theta_{\mathbb{C}_p/\mathcal{K}} : \mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}} \to \mathcal{O}_{\mathbb{C}_p}$. Note that $\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathbb{Q}_p}$ is canonically identified with $\widetilde{\mathbb{A}}^+$. Let $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}$ be the $\ker\theta_{\mathbb{C}_p/\mathcal{K}}$-adic Hausdorff completion of $\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}[1/p]$ and $\theta_{\mathbb{C}_p/\mathcal{K}} : \mathbb{B}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}} \to \mathbb{C}_p$ the canonical map induced by $\theta_{\mathbb{C}_p/\mathcal{K}}$.

Let

$$u_j := t_j - [\tilde{t}_j] \in \mathbb{A}_{\mathrm{inf},\mathbb{C}_p/K_0},$$
$$t := \log([\varepsilon]) := \sum_{n\geq 1}(-1)^{n-1}\frac{([\varepsilon]-1)^n}{n} \in \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p} \subset \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}.$$

Finally, we define $\mathbb{B}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}} := \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}[1/t]$. These constructions are functorial with respect to $\mathbb{C}_p$ and $\mathcal{K}$. In particular:

$$\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathbb{Q}_p} \subset \mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}, \quad \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p} \subset \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}, \quad \mathbb{B}_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p} \subset \mathbb{B}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}.$$

Therefore, any continuous $\mathcal{K}$-algebra automorphism of $\mathbb{C}_p$ acts on these rings. We also have the following explicit descriptions:

$$\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/K_0} \cong \widetilde{\mathbb{A}}^+[\![u_1,\dots,u_d]\!], \quad \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/K} \cong \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}[\![u_1,\dots,u_d]\!]$$

and $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}$ is a complete discrete valuation field with uniformizer t and residue field $\mathbb{C}_p$. Also, $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/K}$ and $\mathbb{B}_{\mathrm{dR},\mathbb{C}_p/K}$ are invariant after replacing K by a finite extension. In particular, these rings are endowed with canonical K^{alg}-algebra structures.

For $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G_K)$, we define $\mathbb{D}_{\mathrm{dR}}(V) := (\mathbb{B}_{\mathrm{dR},\mathbb{C}_p/K}\otimes_{\mathbb{Q}_p} V)^{G_K}$, which is a finite dimensional K-vector space with $\dim_K \mathbb{D}_{\mathrm{dR}}(V) \leq \dim_{\mathbb{Q}_p} V$. When the dimensions are equal, we call V de Rham and denote the category of de Rham representations of G_K by $\mathrm{Rep}_{\mathrm{dR}}(G_K)$.

We endow $\varprojlim_k \mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}[1/p]/(\ker\theta_{\mathbb{C}_p/\mathcal{K}})^k$ with the inverse limit topology, equipping $\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}[1/p]/(\ker\theta_{\mathbb{C}_p/\mathcal{K}})^k$ with the $\mathcal{K}$-Banach space structure whose unit disc is the image of $\mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}$. The identification of $\mathbb{B}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}$ and $\varprojlim_k \mathbb{A}_{\mathrm{inf},\mathbb{C}_p/\mathcal{K}}[1/p]/(\ker\theta_{\mathbb{C}_p/\mathcal{K}})^k$ gives $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}$ its canonical topology and it is a $\mathcal{K}$-Fréchet algebra.

The ring $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}$ is endowed with a continuous $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}$-linear connection

$$\nabla^{\mathrm{geom}} : \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}} \to \mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}} \otimes_{\mathcal{K}} \widehat{\Omega}^1_{\mathcal{K}},$$

which is induced by the canonical derivation $d : \mathcal{K} \to \widehat{\Omega}^1_{\mathcal{K}}$. More precisely, if we denote by $\{\partial_j\}_{1\leq j\leq d}$ the derivations of $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/K}$ given by $\nabla^{\mathrm{geom}}(x) = \sum_j \partial_j(x)\otimes dt'_j$, then ∂_j is the unique $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}$-linear extension of $\partial/\partial t_j : K \to K$. Thus, we can regard the above connection as a connection associated to a "coordinate" $t_1,\dots,t_d$ of K, hence we put the superscript "geom". We denote the kernel of ∇^{geom} by $\mathbb{B}^{\nabla+}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}$, which coincides with the image of $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}$. Therefore, we may identify $\mathbb{B}^{\nabla+}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}$ with $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}$.

We also define a subring $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig},\mathbb{C}_p/\mathbb{Q}_p}$ of $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}$ as follows: let $\mathbb{A}_{\mathrm{cris},\mathbb{C}_p/\mathbb{Q}_p}$ be the universal p-adically formal $\mathbb{Z}_p$-thickening of $\mathcal{O}_{\mathbb{C}_p}$, i.e., the p-adic Hausdorff completion of the PD-envelope of $\widetilde{\mathbb{A}}^+$ with respect to the ideal $\ker\theta_{\mathbb{C}_p/\mathbb{Q}_p}$, compatible with the canonical PD-structure on the ideal (p). Since the construction is functorial, the Frobenius $\varphi:\widetilde{\mathbb{A}}^+\to\widetilde{\mathbb{A}}^+$ acts on both $\mathbb{A}_{\mathrm{cris},\mathbb{C}_p/\mathbb{Q}_p}$ and $\mathbb{B}^+_{\mathrm{cris},\mathbb{C}_p/\mathbb{Q}_p}:=\mathbb{A}_{\mathrm{cris},\mathbb{C}_p/\mathbb{Q}_p}[1/p]$. We define $\mathbb{B}^{\nabla+}_{\mathrm{rig},\mathbb{C}_p/\mathbb{Q}_p}:=\bigcap_{n\in\mathbb{N}}\varphi^n(\mathbb{B}^+_{\mathrm{cris},\mathbb{C}_p/\mathbb{Q}_p})$, which is the maximal subring of $\mathbb{B}^+_{\mathrm{cris},\mathbb{C}_p/\mathbb{Q}_p}$ that is stable under φ. By construction, $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig},\mathbb{C}_p/\mathbb{Q}_p}$ is a subring of $\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p}\cong\mathbb{B}^{\nabla+}_{\mathrm{dR},\mathbb{C}_p/\mathcal{K}}$.

Finally, for simplicity, we denote

$$\mathbb{B}^{\nabla+}_{\mathrm{dR}}:=\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p},\quad \mathbb{B}^{\nabla}_{\mathrm{dR}}:=\mathbb{B}_{\mathrm{dR},\mathbb{C}_p/\mathbb{Q}_p},\quad \mathbb{B}^+_{\mathrm{dR}}:=\mathbb{B}^+_{\mathrm{dR},\mathbb{C}_p/K},\\ \mathbb{B}_{\mathrm{dR}}:=\mathbb{B}_{\mathrm{dR},\mathbb{C}_p/K},\quad \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}:=\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig},\mathbb{C}_p/\mathbb{Q}_p}$$

when no confusion arises.

1.5. ***Ramification theory of Abbes–Saito.*** In this subsection, we review Abbes–Saito's ramification theory, see [Abbes and Saito 2002, 2003] for details.

Let K be a complete discrete valuation field with residue field of characteristic p. Let L/K be a finite separable extension. Let $Z=\{z_0,\dots,z_n\}$ be a set of generators of $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra. View $\mathcal{O}_K\langle Z_0,\dots,Z_n\rangle$ as a Tate algebra, and let $Z_i\mapsto z_i$ be the corresponding surjective $\mathcal{O}_K$-algebra homomorphism from $\mathcal{O}_K\langle Z_0,\dots,Z_n\rangle$ to $\mathcal{O}_L$ with kernel I_Z. For $a\in\mathbb{Q}_{>0}$, we define the nonlog Abbes–Saito space by

$$as^a_{L/K,Z}:=D^{n+1}(|\pi_K|^{-a}f;\ f\in I_Z)=\{x\in D^{n+1};\ |f(x)|\le|\pi_K|^a\ \ \forall f\in I_Z\},$$

which is an affinoid subdomain of the $(n+1)$-dimensional polydisc D^{n+1}. Let $\pi_0^{\mathrm{geom}}(as^a_{L/K,Z})$ be the geometric connected components of $as^a_{L/K,Z}$, i.e., the connected components of $as^a_{L/K,Z}\times_K K^{\mathrm{alg}}$ with respect to the Zariski topology. We define a G_K-set $\mathcal{F}^a(L):=\pi_0^{\mathrm{geom}}(as^a_{L/K,Z})$ and let

$$b(L/K):=\inf\{a\in\mathbb{R};\ \#\mathcal{F}^a(L)=[L:K]\}\in\mathbb{Q}.$$

be the nonlog ramification break. If L/K is Galois, then $\mathcal{F}^a(L)$ can be identified with a quotient of $G_{L/K}$. Moreover, the system $\{\mathcal{F}^a(L)\}_a$ of G_K-sets defines a filtration $\{G^a_{L/K}\}_{a\in\mathbb{Q}_{\ge0}}$ of $G_{L/K}$ such that $\mathcal{F}^a(L)\cong G_{L/K}/G^a_{L/K}$ as G_K-sets.

There exists a log variation of this construction by considering the following log structure. Let $P\subset Z$ be a subset containing a uniformizer, and take a lift $g_j\in\mathcal{O}_K\langle Z_0,\dots,Z_n\rangle$ of $z_j^{e_K}/\pi_K^{v_L(z_j)}$ for each $z_j\in P$. For each pair $(z_i,z_j)\in P\times P$, we take a lift $h_{i,j}\in\mathcal{O}_K\langle Z_0,\dots,Z_n\rangle$ of $z_j^{v_L(z_i)}/z_i^{v_L(z_j)}$. For $a\in\mathbb{Q}_{>0}$, we define the log Abbes–Saito space by

$$as^a_{L/K,Z,P}:=D^{n+1}\begin{pmatrix}|\pi_K|^{-a}f\\ |\pi_K|^{-a-v_L(z_i)}(X_i^{e_{L/K}}-\pi_K g_i)\\ |\pi_K|^{-a-v_L(z_i)v_L(z_j)/e_{L/K}}(X_j^{v_L(z_i)}-X_i^{v_L(z_j)}h_{i,j})\end{pmatrix}$$

as an affinoid subdomain of D^{n+1}. Here, f ranges over I_Z and the indices z_i and (z_i, z_j) range over P and $P \times P$ respectively. As before, we define the G_K-set $\mathcal{F}^a_{\log}(L) := \pi_0^{\mathrm{geom}}(as^a_{L/K,Z,P})$ and define the log ramification break by

$$b_{\log}(L/K) := \inf\{a \in \mathbb{R};\ \#\mathcal{F}^a_{\log}(L) = [L:K]\} \in \mathbb{Q}.$$

A similar procedure as before defines the log ramification filtration $\{G^a_{L/K,\log}\}_{a\in\mathbb{Q}_{\geq 0}}$ of $G_{L/K}$.

In this paper, we consider only the following simple Abbes–Saito spaces. With the notation as above, let $p_0, \dots, p_m$ be a system of generators of the kernel of the surjection $\mathcal{O}_K\langle X_0, \dots, X_n\rangle \to \mathcal{O}_L$. Assume that z_0 is a uniformizer of L and $p_0 = X_0^{e_{L/K}} - \pi_K g_0$ for some $g_0 \in \mathcal{O}_K\langle X_0, \dots, X_n\rangle$. In this case, we have a simple log structure: we put $P := \{z_0\}$ and we choose g_0 as a lift of $z_0^{e_{L/K}}/\pi_K$. We also choose 1 as $h_{1,1}$. Hence, Abbes–Saito spaces are given by

$$as^a_{L/K,Z} = D^{n+1}(|\pi_K|^{-a} p_j \text{ for } 0 \leq j \leq m),$$

$$as^a_{L/K,Z,P} = D^{n+1}(|\pi_K|^{-a-1} p_0, |\pi_K|^{-a} p_j \text{ for } 1 \leq j \leq m).$$

Let $F/\mathbb{Q}_p$ be a finite extension and V an F-representation of G_K with finite local monodromy. We define Abbes–Saito's Artin and Swan conductors by

$$\mathrm{Art}^{\mathrm{AS}}(V) := \sum_{a\in\mathbb{Q}_{\geq 0}} a \cdot \dim_F(V^{\bigcap_{b>a} G^b_K} / V^{G^a_K}),$$
$$\mathrm{Swan}^{\mathrm{AS}}(V) := \sum_{a\in\mathbb{Q}_{\geq 0}} a \cdot \dim_F(V^{\bigcap_{b>a} G^b_{K,\log}} / V^{G^a_{K,\log}}).$$

Note that the above construction does not depend on other choices, like Z and P. Also, note that both the Artin and Swan conductors are additive and compatible with unramified base change. When k_K is perfect, the log (resp. nonlog) ramification filtration is compatible with the usual upper numbering filtration (resp. shift by one). Moreover, our Artin and Swan conductors coincide with the classical Artin and Swan conductors when k_K is perfect.

Theorem 1.5.1 (Hasse–Arf theorem, [Xiao 2012, Theorem 4.5.14]). *Assume that K is of mixed characteristic. Let $F/\mathbb{Q}_p$ be a finite extension and $V \in \mathrm{Rep}_F^{f.g.}(G_K)$. Then, we have $\mathrm{Art}(V) \in \mathbb{Z}$ if K is not absolutely unramified; we have $\mathrm{Swan}^{\mathrm{AS}}(V) \in \mathbb{Z}$ if $p \neq 2$, and $\mathrm{Swan}^{\mathrm{AS}}(V) \in 2^{-1}\mathbb{Z}$ if $p = 2$.*

Xiao gives more precise results in the equal characteristic case, as we will see in Theorem 1.7.10.

1.6. ***Overconvergent rings.*** In this subsection, we will recall basic definitions of overconvergent rings associated to complete valuation fields of characteristic p, following [Kedlaya 2004, §2–3] and [Kedlaya 2005, §2].

Construction 1.6.1 ([Kedlaya 2005, §2.1–2.2]). Let (E, v) be a complete valuation field of characteristic p. Assume that either E is perfect or that v is a discrete valuation. We will construct an overconvergent ring associated to E. We first consider the case where E is perfect. Note that any element of $W(E)[1/p]$ is uniquely expressed as $\sum_{k\gg-\infty} p^k[x_k]$ with $x_k \in E$. For $n \in \mathbb{Z}$, we define a "partial valuation" on $W(E)[1/p]$ by

$$v^{\leq n}\biggl(\sum_{k\gg-\infty} p^k[x_k]\biggr) := \inf_{k\leq n} v(x_k).$$

For $r \in \mathbb{R}_{>0}$, we define

$$w_r(x) := \inf_n \{r v^{\leq n}(x) + n\},$$

$$W(E)_r := \{x \in W(E);\, w_r(x) < \infty\}.$$

Then, $W(E)_r[1/p]$ is a subring of $W(E)[1/p]$ and w_r is a multiplicative valuation of $W(E)_r[1/p]$. Moreover, we have $W(E)_r \subset W(E)_{r'}$ for $r' \leq r$. We put $W_{\mathrm{con}}(E) := \varinjlim_{r\to 0} W(E)_r$.

Next, we consider the general case, i.e., we do not need to assume that E is perfect in the following. Let Γ be a Cohen ring of E with a Frobenius lift φ. Then, we can obtain a Frobenius-compatible embedding $\Gamma \hookrightarrow W(E^{\mathrm{pf}}) \hookrightarrow W(\widehat{E}^{\mathrm{alg}})$, where $\widehat{E}^{\mathrm{alg}}$ is the completion of E^{alg}. By using this embedding, we can define $v^{\leq n}$ and w_r on Γ. Moreover, we define $\Gamma_r := \Gamma \cap W(\widehat{E}^{\mathrm{alg}})_r$ and $\Gamma_{\mathrm{con}} := \varinjlim_{r\to 0} \Gamma_r = \Gamma \cap W_{\mathrm{con}}(\widehat{E}^{\mathrm{alg}})$. We say that Γ has enough r-units if the canonical map $\Gamma_r \to E$ is surjective. We say that Γ has enough units if Γ has enough r-units for some $r > 0$. Note that if E is perfect, then Γ has enough r-units for any r. In general, by [Kedlaya 2004, Proposition 3.11], Γ has enough r-units for all sufficiently small r. In the following, we fix r_0 such that Γ has enough r-units for all $r \leq r_0$. Note that Γ_r is a PID for $r < r_0$, and Γ_{con} is a Henselian local ring with maximal ideal (p), residue field E and fraction field $\Gamma_{\mathrm{con}}[1/p]$ [Kedlaya 2005, Lemma 2.1.12]. We endow $\Gamma_r[1/p]$ with the Fréchet topology defined by the family of valuations $\{w_s\}_{0<s\leq r}$. Let $\Gamma_{\mathrm{an},r}$ be the completion of $\Gamma_r[1/p]$ with respect to the Fréchet topology and $\Gamma_{\mathrm{an,con}} := \varinjlim_{r\to 0} \Gamma_{\mathrm{an},r}$. We extend $v^{\leq n}$ and w_r to $v^{\leq n}, w_r : \Gamma_{\mathrm{an},r} \to \mathbb{R}$ and we endow $\Gamma_{\mathrm{an},r}$ (resp. $\Gamma_{\mathrm{an,con}}$) with the Fréchet topology defined by $\{w_s\}_{0<s\leq r}$ (resp. the inductive limit topology of Fréchet topologies). Note that $\varphi(\Gamma_r) \subset \Gamma_{r/p}$; hence, φ extends to a map $\varphi : \Gamma_{\mathrm{an},r} \to \Gamma_{\mathrm{an},r/p}$. In particular, Γ_{con} and $\Gamma_{\mathrm{an,con}}$ are canonically endowed with endomorphisms φ. Also, note that $\Gamma_{\mathrm{an},r}$ for all $r < r_0$ and hence, $\Gamma_{\mathrm{an,con}}$ are Bézout integral domains [Kedlaya 2005, Theorem 2.9.6].

In the rest of this subsection, we will see explicit descriptions of Γ_{con}, together with its finite étale extensions, by using rings of overconvergent power series ring.

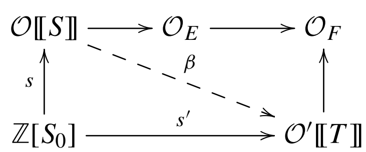
Notation 1.6.2. Let $\mathcal{O}$ be a complete discrete valuation ring of mixed characteristic $(0, p)$. Let $\mathcal{O}\{\{S\}\}$ be the p-adic Hausdorff completion of $\mathcal{O}((S)) := \mathcal{O}[\![S]\!][S^{-1}]$. For $r \in \mathbb{Q}_{>0}$, we define the ring of overconvergent power series over $\mathcal{O}$ as

$$\mathcal{O}((S))^{\dagger,r} := \{f \in \mathcal{O}\{\{S\}\};\ f \text{ converges on } 0 < v_p(S) \le r\},\ \mathcal{O}((S))^{\dagger} := \bigcup_{r>0} \mathcal{O}((S))^{\dagger,r}.$$

Recall that $\big(\mathcal{O}((S))^{\dagger}, (\pi_{\mathcal{O}})\big)$ is a Henselian discrete valuation ring [Matsuda 1995, Proposition 2.2]. We also define the Robba ring $\mathcal{R}$ associated to $\mathcal{O}((S))^{\dagger}$ by

$$\mathcal{R} := \left\{ f = \sum_{n\in\mathbb{Z}} a_n S^n;\ a_n \in \mathrm{Frac}(\mathcal{O}),\ f \text{ converges on } 0 < v_p(S) \le r \text{ for some } r > 0 \right\}.$$

Construction 1.6.3. We construct a realization of a finite étale extension of $\mathcal{O}((S))^{\dagger}$ as an overconvergent power series ring. Let Γ be a Cohen ring of a complete discrete valuation field E of characteristic p. By fixing an isomorphism $f : \Gamma \cong \mathcal{O}\{\{S\}\}$, where $\mathcal{O}$ is a Cohen ring of k_E, we identify Γ and E with $\mathcal{O}\{\{S\}\}$ and $k_E((S))$. Let Γ'/Γ be a finite étale extension, with Γ' connected and F/E the corresponding residue field extension. Then, Γ' is again a Cohen ring of F. We identify F with $k_F((T))$ and fix a Cohen ring $\mathcal{O}'$ of k_F. We claim that there exists an isomorphism $f' : \Gamma' \cong \mathcal{O}'\{\{T\}\}$ such that f' modulo p is the identity, $f'(\mathcal{O}[\![S]\!]) \subset \mathcal{O}'[\![T]\!]$ and $f' : \mathcal{O}[\![S]\!] \to \mathcal{O}'[\![T]\!]$ is finite flat. We can write $S = T^{e_{F/E}}\bar{u}$ in $\mathcal{O}_F$ with some $\bar{u} \in \mathcal{O}_F^{\times}$. We fix a lift $u \in \mathcal{O}'[\![T]\!]^{\times}$ of $\bar{u}$ with respect to the projection $\mathcal{O}'[\![T]\!] \to \mathcal{O}_F$ and let $s' : \mathbb{Z}[S_0] \to \mathcal{O}'[\![T]\!];\ S_0 \mapsto T^{e_{F/E}}u$ be a ring homomorphism. Let $s : \mathbb{Z}[S_0] \to \mathcal{O}[\![S]\!]$ be the ring homomorphism sending S_0 to S. By the formal smoothness of s (see [Ohkubo 2013, §1A]), there exists a local ring homomorphism $\beta : \mathcal{O}[\![S]\!] \to \mathcal{O}'[\![T]\!]$:



By the local criteria of flatness and Nakayama's lemma, β is finite flat. By the definition of s and s', β induces a map $\beta : \mathcal{O}((S)) \to \mathcal{O}'((T))$, and hence a map $\hat{\beta} : \mathcal{O}\{\{S\}\} \to \mathcal{O}'\{\{T\}\}$. Since $\hat{\beta}$ is finite étale with residue field extension F/E, there exists a canonical isomorphism $f' : \Gamma' \cong \mathcal{O}'\{\{T\}\}$, which satisfies the desired properties by the construction of β.

The relation $S = T^{e_{F/E}}u$ for $u \in \mathcal{O}'[\![T]\!]^{\times}$ gives $f'(\mathcal{O}((S))^{\dagger,r}) \subset \mathcal{O}'((T))^{\dagger,r/e_{F/E}}$. In the limit $r \to \infty$, we obtain a flat morphism $f' : \mathcal{O}((S))^{\dagger} \to \mathcal{O}'((T))^{\dagger}$. Finally, we prove the finiteness of $f' : \mathcal{O}((S))^{\dagger} \to \mathcal{O}'((T))^{\dagger}$. We fix a basis $\omega_1, \dots, \omega_g$ of $\mathcal{O}'[\![T]\!]$ as an $\mathcal{O}[\![S]\!]$-module. Then, we only have to prove that $x \in \mathcal{O}'((T^{e_{F/E}}))^{\dagger,r}$

can be written as $\sum_i \omega_i \sum_n a_{i,n} S^n$ with $\sum_n a_{i,n} S^n \in \mathcal{O}((S))^{\dagger, re_{F/E}}$. By the relation $Su^{-1} = T^{e_{F/E}}$ again, any element $x \in \mathcal{O}'((T^{e_{F/E}}))^{\dagger,r}$ can be written as $\sum_{n\in\mathbb{Z}} a_n S^n$ with $a_n \in \mathcal{O}'[\![T]\!]$ such that $|a_n||p|^{e_{F/E}nr} \to 0$ for $n \to -\infty$, where $|\cdot|$ is a norm of $\mathcal{O}'[\![T]\!]$ associated to the p-adic valuation. We write $a_n = \sum_i a_{n,i}\omega_i$. Then, we have $|a_n| = \sup_i |a_{n,i}|$, where $|\cdot|$ on the RHS is a norm of $\mathcal{O}[\![S]\!]$ associated to the p-adic valuation. Hence, $\sum_n a_{n,i} S^n$ belongs to $\mathcal{O}((S))^{\dagger, re_{F/E}}$, which implies the assertion.

Lemma 1.6.4 [Kedlaya 2005, Lemma 2.3.5, Corollary 2.3.7]. *Let Γ be a Cohen ring of a complete discrete valuation field E of characteristic p and $\varphi : \Gamma \to \Gamma$ a Frobenius lift. By fixing an isomorphism $f : \Gamma \cong \mathcal{O}\{\{S\}\}$, we identify Γ and E with $\mathcal{O}\{\{S\}\}$ and $k_E((S))$. Assume that $\varphi(S) \in \mathcal{O}((S))^{\dagger}$. Then, we have*

$$\Gamma_r = \mathcal{O}((S))^{\dagger,r}, \quad \Gamma_{\mathrm{con}} = \mathcal{O}((S))^{\dagger}$$

for all sufficiently small $r > 0$.

Moreover, let F/E be a finite separable extension, Γ'/Γ the corresponding finite étale extension and $\varphi : \Gamma' \to \Gamma'$ the corresponding Frobenius lift extending φ. We fix an isomorphism $f' : \Gamma' \cong \mathcal{O}'\{\{T\}\}$ as in Construction 1.6.3. Then, f' induces isomorphisms

$$\Gamma'_r \cong \mathcal{O}'((T))^{\dagger, r/e_{F/E}}, \quad \Gamma'_{\mathrm{con}} \cong \mathcal{O}'((T))^{\dagger}$$

for all sufficiently small $r > 0$.

Proof. Let φ be the Frobenius lift of $\mathcal{O}'\{\{T\}\}$ obtained by identifying $\mathcal{O}'\{\{T\}\}$ with Γ'. We only have to check that the assumption $\varphi(T) \in \mathcal{O}'((T))^{\dagger}$ in [Kedlaya 2005, Convention 2.3.1] is satisfied. This follows from the fact that $\mathcal{O}'((T))^{\dagger}$ is integrally closed in $\mathcal{O}'\{\{T\}\}$, which in turn is a consequence of Raynaud's criteria of integral closedness for Henselian pairs [Raynaud 1970, Théorème 3(b), Chapitre XI]. □

Finally, we define (pure) φ-modules over overconvergent rings.

Definition 1.6.5 [Kedlaya 2005, Definition 4.6.1]. Let R be $\Gamma[1/p]$, $\Gamma_{\mathrm{con}}[1/p]$, or $\Gamma_{\mathrm{an,con}}$ (Construction 1.6.1) and let $\sigma := \varphi^h$ for some $h \in \mathbb{N}_{>0}$. A σ-module over R is a finite free R-module M endowed with a semilinear σ-action such that $1 \otimes \sigma : M \otimes_{R,\sigma} R \to M$ is an isomorphism. Assume that E is algebraically closed. Then, any σ-module over $\Gamma[1/p]$ or $\Gamma_{\mathrm{an,con}}$ admits a Dieudonné–Manin decomposition [Kedlaya 2005, Theorem 4.5.7] and we define the slope multiset of M as the multiset of the p-adic valuations of the "eigenvalues". For a σ-module M over $\Gamma_{\mathrm{con}}[1/p]$, we define the slope multiset of M as the slope multiset of $\Gamma \otimes_{\Gamma_{\mathrm{con}}[1/p]} M$, which coincides with that of $\Gamma_{\mathrm{an,con}} \otimes_{\Gamma_{\mathrm{con}}[1/p]} M$. For a general E, we define the slope multiset after the base change $\Gamma \to W(\widehat{E}^{\mathrm{alg}})$. A σ-module over R is pure of slope s if the slope multiset consists of only s. If M is a σ-module that is pure of slope 0, then we call M étale.

Let φ be a Frobenius lift of $\Gamma := \mathcal{O}\{\{S\}\}$ with $\varphi(S) \subset \mathcal{O}((S))^\dagger$. By Lemma 1.6.4, we can view $\mathcal{O}((S))^\dagger[1/p]$ and $\mathcal{R}$ in Notation 1.6.2 as $\Gamma_{\mathrm{con}}[1/p]$ and $\Gamma_{\mathrm{an,con}}$, and we can give similar definitions for $R = \mathcal{O}((S))^\dagger[1/p]$ and $\mathcal{R}$.

When R is one of the above rings, we denote the category of σ-modules (resp. étale σ-modules, σ-modules of pure slope s) over R by $\mathrm{Mod}_R(\sigma)$ (resp. $\mathrm{Mod}_R^{\mathrm{et}}(\sigma)$, $\mathrm{Mod}_R^s(\sigma)$).

1.7. ***Differential Swan conductor.*** The aim of this subsection is to recall the definition of the differential Swan conductor. The following coordinate free definition of the continuous Kähler differentials for overconvergent rings will be useful.

Definition 1.7.1. Let Γ be an absolutely unramified complete discrete valuation ring of mixed characteristic $(0, p)$. For a subring R of Γ, we define Ω^1_R as the R-submodule of $\widehat{\Omega}^1_\Gamma$ generated by the image of R under $d : \Gamma \to \widehat{\Omega}^1_\Gamma$.

Lemma 1.7.2. *Let $\Gamma := \mathcal{O}\{\{S\}\}$ and $\Gamma^\dagger := \mathcal{O}((S))^\dagger$, where $\mathcal{O}$ is a Cohen ring of a field k of characteristic p. Assume that $[k : k^p] = p^d < \infty$. Then, $\Omega^1_{\Gamma^\dagger}$ is the unique $\Gamma^\dagger$-submodule $\mathcal{M}$ of $\widehat{\Omega}^1_\Gamma$ such that*

(i) *$\mathcal{M}$ is of finite type over $\Gamma^\dagger$.*

(ii) *The image of $\Gamma^\dagger$ under $d : \Gamma \to \widehat{\Omega}^1_\Gamma$ is contained in $\mathcal{M}$.*

(iii) *The canonical map $\Gamma \otimes_{\Gamma^\dagger} \mathcal{M} \to \widehat{\Omega}^1_\Gamma$ is an isomorphism.*

Also, if $\varphi : \Gamma \to \Gamma$ is a Frobenius lift $\varphi(\Gamma^\dagger) \subset \Gamma^\dagger$, $\Omega^1_{\Gamma^\dagger}$ is stable under $\varphi : \widehat{\Omega}^1_\Gamma \to \widehat{\Omega}^1_\Gamma$.

We omit the proof since it is elementary. Note that if $\{t_j\} \subset \mathcal{O}$ is a lift of a p-basis of k, then $\Omega^1_{\Gamma^\dagger}$ is a free of rank $d+1$ with basis $dS, dt_1, \ldots, dt_d$.

Corollary 1.7.3. *With the notation as in Lemma 1.6.4, the canonical isomorphism $\Gamma' \otimes_\Gamma \widehat{\Omega}^1_\Gamma \cong \widehat{\Omega}^1_{\Gamma'}$ descends to a canonical isomorphism $\Gamma'_{\mathrm{con}} \otimes_{\Gamma_{\mathrm{con}}} \Omega^1_{\Gamma_{\mathrm{con}}} \cong \Omega^1_{\Gamma'_{\mathrm{con}}}$.*

Notation 1.7.4. In the rest of this section, let the notation be as in Lemma 1.7.2. We fix a Frobenius lift $\varphi : \Gamma \to \Gamma$ satisfying $\varphi(\Gamma^\dagger) \subset \Gamma^\dagger$. Let $\mathcal{R}$ be the Robba ring associated to $\Gamma^\dagger$ and assume that $\varphi(\mathcal{R}) \subset \mathcal{R}$. We put $\Omega^1_{\mathcal{R}} := \mathcal{R} \otimes_{\Gamma^\dagger} \Omega^1_{\Gamma^\dagger}$. Note that the canonical derivation $d : \Gamma^\dagger \to \Omega^1_{\Gamma^\dagger}$ extends to $d : \mathcal{R} \to \Omega^1_{\mathcal{R}}$.

Definition 1.7.5. A ∇-module M over $\mathcal{R}$ is a finite free module over $\mathcal{R}$ together with a connection $\nabla = \nabla_M : M \to M \otimes_{\mathcal{R}} \Omega^1_{\mathcal{R}}$ such that the composition of ∇_M with the map $M \otimes_{\mathcal{R}} \Omega^1_{\mathcal{R}} \to M \otimes_{\mathcal{R}} \bigwedge^2_{\mathcal{R}} \Omega^1_{\mathcal{R}}$ induced by ∇ is the zero map. For $h \in \mathbb{N}_{>0}$, a (φ^h, ∇)-module M over $\mathcal{R}$ is a φ^h-module over $\mathcal{R}$ endowed with a ∇-module structure commuting with the action of φ^h. We call a (φ^h, ∇)-module pure (resp. étale) if the underlying φ^h-module is pure (resp. étale). Similarly, we define étale or pure (φ^h, ∇)-modules over $\Gamma^\dagger$ and Γ. Denote by $\mathrm{Mod}^s_R(\varphi^h, \nabla)$ the category of pure (φ^h, ∇)-modules over R, where R is either Γ, $\Gamma^\dagger[1/p]$ or $\mathcal{R}$.

Theorem 1.7.6 [Kedlaya 2007, Theorem 3.4.6]. *For a (φ, ∇)-module M over $\mathcal{R}$, there exists a canonical slope filtration*

$$0 = \mathrm{Fil}^0(M) \subset \cdots \subset \mathrm{Fil}^l(M) = M,$$

whose graded pieces are (φ, ∇)-modules of pure slope $s_1 < \cdots < s_l$.

Construction 1.7.7 [Kedlaya 2007, Definition 3.3.4]. Let $F/\mathbb{Q}_p$ be a finite unramified extension and $V \in \mathrm{Rep}_F^{f.g.}(G_E)$. Let $\Gamma^{\dagger,\mathrm{ur}}$ be the maximal unramified extension of $\Gamma^\dagger$. We put $\Omega^1_{\Gamma^{\dagger,\mathrm{ur}}} := \varinjlim \Omega^1_{\Gamma_1^\dagger}$, where the limit runs all the finite étale extensions $\Gamma_1^\dagger/\Gamma^\dagger$ with $\Gamma_1^\dagger$ connected. We consider the connection

$$\begin{aligned} \nabla : \Gamma^{\dagger,\mathrm{ur}} \otimes_{\mathcal{O}_F} V &\to \Omega^1_{\Gamma^{\dagger,\mathrm{ur}}} \otimes_{\mathcal{O}_F} V \\ \lambda \otimes y &\mapsto d\lambda \otimes y. \end{aligned} \tag{*}$$

Since $\Omega^1_{\Gamma^{\dagger,\mathrm{ur}}} \cong \Gamma^{\dagger,\mathrm{ur}} \otimes_{\Gamma^\dagger} \Omega^1_{\Gamma^\dagger}$ as G_E-modules by Corollary 1.7.3, we obtain a connection

$$\nabla : D^\dagger(V) \to \Omega^1_{\Gamma^\dagger} \otimes_{\Gamma^\dagger} D^\dagger(V),$$

where $D^\dagger(V) := (\Gamma^{\dagger,\mathrm{ur}} \otimes_{\mathcal{O}_F} V)^{G_E}$ is a finite dimensional $\Gamma^\dagger[1/p]$-module of rank $\dim_F V$, by taking G_E-invariants of (*). Thus, we obtain a rank preserving functor

$$D^\dagger : \mathrm{Rep}_F^{f.g.}(G_E) \to \mathrm{Mod}_{\Gamma^\dagger[1/p]}(\nabla).$$

By extending scalars, we also obtain a rank preserving functor

$$D^\dagger_{\mathrm{rig}} : \mathrm{Rep}_F^{f.g.}(G_E) \to \mathrm{Mod}_{\mathcal{R}}(\nabla).$$

Note that if V is endowed with a semilinear action of φ^h for $h \in \mathbb{N}$, then $D^\dagger(V)$ and $D^\dagger_{\mathrm{rig}}(V)$ are also endowed with semilinear φ^h-actions.

Definition 1.7.8. For a ∇-module M over $\mathcal{R}$, let $\mathrm{Swan}^\nabla(M)$ be the differential Swan conductor of M as in [Kedlaya 2007, Definition 2.8.1].

Recall that the differential Swan conductor is defined in terms of the behavior of the logarithmic radius of convergence [Xiao 2010, Definition 2.3.20], which depends only on the Jordan–Hölder factors of a given ∇-module by definition. In particular, we have:

Lemma 1.7.9 (The additivity of the differential Swan conductor). *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of ∇-modules over $\mathcal{R}$. Then, we have* $\mathrm{Swan}^\nabla(M) = \mathrm{Swan}^\nabla(M') + \mathrm{Swan}^\nabla(M'')$.

The following is Xiao's Hasse–Arf Theorem in the characteristic p case.

Theorem 1.7.10 [Xiao 2010, Theorem 4.4.1, Corollary 4.4.3]. *Let V be an F-representation of G_E of finite local monodromy. Then, we have*

$$\mathrm{Swan}^{\mathrm{AS}}(V) = \mathrm{Swan}^\nabla(D^\dagger_{\mathrm{rig}}(V)).$$

Moreover, these invariants are nonnegative integers.

1.8. ***Scholl's fields of norms.*** In this subsection, we recall some results of [Scholl 2006, §1.3], which are a generalization of Fontaine–Wintenberger's fields of norms. Throughout this subsection, let K be a complete discrete valuation field of mixed characteristic $(0, p)$ with $[k_K : k_K^p] = p^d < \infty$.

Definition 1.8.1. Let $K_1 \subset K_2 \subset \dots$ be finite extensions of K and put $K_\infty = \bigcup K_n$. We say that a tower $\mathfrak{K} := \{K_n\}_{n>0}$ is strictly deeply ramified if there exists $n_0 > 0$ and an element $\xi \in \mathcal{O}_{K_{n_0}}$ such that $0 < v_p(\xi) \leq 1$, and such that the following condition holds: for every $n \geq n_0$, the extension K_{n+1}/K_n has degree p^{d+1}, and there exists a surjection $\Omega^1_{\mathcal{O}_{K_{n+1}}/\mathcal{O}_{K_n}} \to (\mathcal{O}_{K_{n+1}}/\xi\mathcal{O}_{K_{n+1}})^{d+1}$ of $\mathcal{O}_{K_{n+1}}$-modules.

Let $\mathfrak{K} = \{K_n\}_{n>0}$ be a strictly deeply ramified tower. For $n \geq n_0$, we have $e_{K_{n+1}/K_n} = p$ and $k_{K_{n+1}} = k_K^{1/p}$, and the Frobenius $\mathcal{O}_{K_{n+1}}/\xi\mathcal{O}_{K_{n+1}} \to \mathcal{O}_{K_{n+1}}/\xi\mathcal{O}_{K_{n+1}}$ induces a surjection $f_n : \mathcal{O}_{K_{n+1}}/\xi\mathcal{O}_{K_{n+1}} \to \mathcal{O}_{K_n}/\xi\mathcal{O}_{K_n}$. We also choose a uniformizer π_{K_n} of K_n with $\pi_{K_{n+1}}^p \equiv \pi_{K_n} \mod \xi\mathcal{O}_{K_n}$. Then, we define $X^+ := X^+(\mathfrak{K}, \xi, n_0) := \varprojlim_{n\geq n_0} \mathcal{O}_{K_n}/\xi\mathcal{O}_{K_n}$, with transition maps $\{f_n\}$. Let $\mathrm{pr}_n : X^+ \to \mathcal{O}_{K_n}/\xi\mathcal{O}_{K_n}$ be the n-th projection for $n \geq n_0$. We put $\Pi := (\pi_{K_n} \mod \xi\mathcal{O}_{K_n}) \in X^+$. Let $k_{\mathfrak{K}} := \varprojlim_{n\geq n_0} k_{K_n}$ where the transition maps are induced by f_n's. Since $k_{K_{n+1}} = k_{K_n}^{1/p}$, the projections $\mathrm{pr}_n : k_{\mathfrak{K}} \to k_{K_n}$ are isomorphisms for all $n \geq n_0$. Moreover, X^+ is a complete discrete valuation ring of characteristic p, with uniformizer Π and residue field $k_{\mathfrak{K}}$. The construction does not depend on ξ or n_0, and X^+ is invariant after changing $\{K_n\}_n$ by $\{K_{n+m}\}_n$ for some m. Hence, we may denote $X^+(\mathfrak{K}, \xi, n_0)$ by $X^+_{\mathfrak{K}}$ and denote the fractional field of $X^+_{\mathfrak{K}}$ by $X_{\mathfrak{K}}$. Note that if K_n/K is Galois for all n, then $X^+_{\mathfrak{K}}$ and $X_{\mathfrak{K}}$ are canonically endowed with $G_{K_\infty/K}$-actions by construction.

Example 1.8.2 (Kummer tower case). Let $K = \widetilde{K}$ and $\{L_n\}$ be as in Section 1.3. Then, $\{L_n\}$ is strictly deeply ramified [Ohkubo 2010, Example 6.2].

Let L_∞/K_∞ be a finite extension. We choose a finite extension L/K such that $L_\infty = LK_\infty$. Then, the tower $\mathfrak{L} := \{L_n := LK_n\}$ depends only on L_∞ up to shifting, and is also strictly deeply ramified with respect to any $\xi' \in K_{n_0}$ with $0 < v_p(\xi') < v_p(\xi)$ ([Scholl 2006, Theorem 1.3.3]). Note that if L_n/K is Galois for all n, then $X^+_{\mathfrak{L}}$ and $X_{\mathfrak{L}}$ are canonically endowed with $G_{L_\infty/K}$-actions by construction.

Theorem 1.8.3 [Scholl 2006, Theorem 1.3.4]. *Let the notation be as above. Denote the category of finite étale algebras over K_∞ (resp. $X_{\mathfrak{K}}$) by $\boldsymbol{F\acute{E}t}_{K_\infty}$ (resp. $\boldsymbol{F\acute{E}t}_{X_{\mathfrak{K}}}$). Then, the functor*

$$X_\bullet : \boldsymbol{F\acute{E}t}_{K_\infty} \to \boldsymbol{F\acute{E}t}_{X_{\mathfrak{K}}}$$
$$L_\infty \mapsto X_{\mathfrak{L}}$$

is an equivalence of Galois categories. In particular, the corresponding fundamental groups are isomorphic, i.e., $G_{K_\infty} \cong G_{X_{\mathfrak{K}}}$. Moreover, the sequences $\{[L_n : K_n]\}_n$, $\{e_{L_n/K_n}\}_n$ and $\{[k_{L_n} : k_{K_n}]\}_n$ are stationary for sufficiently large n. Their limits are equal to $[X_{\mathfrak{L}} : X_{\mathfrak{K}}]$, $e_{X_{\mathfrak{L}}/X_{\mathfrak{K}}}$ and $[k_{X_{\mathfrak{L}}} : k_{X_{\mathfrak{K}}}]$.

1.9. ***(φ, Γ_K)-modules.*** Throughout this subsection, let K be a complete discrete valuation field of mixed characteristic $(0, p)$. In this subsection, we will recall the theory of (φ, Γ_K)-modules in the Kummer tower case [Andreatta 2006]. To avoid complications, especially when verifying the assumption [Scholl 2006, (2.1.2)], we will assume the following to work under the settings of [Andreatta 2006; Andreatta and Brinon 2008; 2010].

Assumption 1.9.1 [Andreatta 2006, §1]. Let $\mathcal{V}$ be a complete discrete valuation field of mixed characteristic $(0, p)$ with perfect residue field. Let R_0 be the p-adic Hausdorff completion of $\mathcal{V}[T_1, \dots, T_d][1/T_1 \dots T_d]$ and $\widetilde{R}$ a ring obtained from R_0 by iterating finitely many times the following operations:

(ét) The p-adic Hausdorff completion of an étale extension.

(loc) The p-adic Hausdorff completion of the localization with respect to a multiplicative system.

(comp) The Hausdorff completion with respect to an ideal containing p.

We assume that there exists a finite flat morphism $\widetilde{R} \to \mathcal{O}_K$, which sends T_j to t_j.

Note that $\widetilde{R}$ is an absolutely unramified complete discrete valuation ring. Denote $\widetilde{R}$ by $\mathcal{O}_{\widetilde{K}}$ and $\mathrm{Frac}(\widetilde{R})$ by $\widetilde{K}$. Let $L/\widetilde{K}$ be a finite extension. In the rest of this subsection, we will use the notation from Sections 1.3 and 1.4. We also apply the results of Section 1.8 to the Kummer tower $\{L_n\}_{n>0}$.

Notation 1.9.2 [Andreatta and Brinon 2008, §4.1]. We will denote

$$\mathbb{E}_L^+ := X_{\mathfrak{L}}^+, \quad \mathbb{E}_L := X_{\mathfrak{L}}.$$

For any nonzero $\xi \in p\mathcal{O}_{L_\infty}$, we put

$$\widetilde{\mathbb{E}}_L^+ := \varprojlim_{x \mapsto x^p} \mathcal{O}_{L_\infty}/\xi\mathcal{O}_{L_\infty}, \quad \widetilde{\mathbb{E}}_L := \mathrm{Frac}(\widetilde{\mathbb{E}}_L^+),$$

where both rings are independent of the choice of ξ. We also put

$$\widetilde{\mathbb{A}}_L^+ := W(\widetilde{\mathbb{E}}_L^+), \quad \widetilde{\mathbb{A}}_L := W(\widetilde{\mathbb{E}}_L), \quad \widetilde{\mathbb{B}}_L := \widetilde{\mathbb{A}}_L[1/p].$$

By definition, we have $\mathbb{E}_L^+ \subset \widetilde{\mathbb{E}}_L^+$ and $\mathbb{E}_L \subset \widetilde{\mathbb{E}}_L$, and $\widetilde{\mathbb{E}}_L$ can be viewed as a closed subring of $\widetilde{\mathbb{E}}$. In particular, the rings $\widetilde{\mathbb{A}}_L^+$, $\widetilde{\mathbb{A}}_L$ and $\widetilde{\mathbb{B}}_L$ can be viewed as subrings of $\widetilde{\mathbb{A}}^+$, $\widetilde{\mathbb{A}}$ and $\widetilde{\mathbb{B}}$. Note that the completion of an algebraic closure of $\mathbb{E}_L$ coincides with $\widetilde{\mathbb{E}}$. Moreover, $\widetilde{\mathbb{E}}$ is perfect and $(\widetilde{\mathbb{E}}_L, v_{\widetilde{\mathbb{E}}})$ is a perfect complete valuation field, whose integer ring is $\widetilde{\mathbb{E}}_L^+$. By using the $G_{\widetilde{K}}$-actions on $\widetilde{\mathbb{E}}$ and $\widetilde{\mathbb{A}}$, we can write

$$\widetilde{\mathbb{E}}_L^+ = (\widetilde{\mathbb{E}}^+)^{H_L}, \quad \widetilde{\mathbb{E}}_L = \widetilde{\mathbb{E}}^{H_L}, \quad \widetilde{\mathbb{A}}_L = \widetilde{\mathbb{A}}^{H_L}, \quad \widetilde{\mathbb{B}}_L = \widetilde{\mathbb{B}}^{H_L},$$

see [Andreatta and Brinon 2008, Lemma 4.1].

Lemma 1.9.3 (a special case of [Andreatta and Brinon 2008, Proposition 4.42]). *We put* $\mathbb{A}^+_{W(k_{\mathcal{V}})} := W(k_{\mathcal{V}})[\![\pi]\!] \subset \widetilde{\mathbb{A}}^+$, *where* $\pi = [\varepsilon] - 1 \in \widetilde{\mathbb{A}}^+$. *Let* $L/\widetilde{K}$ *be a finite extension. The weak topology of* $\widetilde{\mathbb{A}}_L \cong \widetilde{\mathbb{E}}_L^{\mathbb{N}}$ *is the product topology* $\widetilde{\mathbb{E}}_L^{\mathbb{N}}$, *where* $\widetilde{\mathbb{E}}_L$ *is endowed with the valuation topology. Then, there exists a unique subring* $\mathbb{A}_L$ *of* $\widetilde{\mathbb{A}}_L$ *such that*:

(i) $\mathbb{A}_L$ *is complete for the weak topology.*

(ii) $p\widetilde{\mathbb{A}}_L \cap \mathbb{A}_L = p\mathbb{A}_L$.

(iii) *One has an commutative diagram*

$$\begin{array}{ccc} \mathbb{A}_L & \twoheadrightarrow & \mathbb{E}_L \\ \downarrow & & \downarrow \\ \widetilde{\mathbb{A}}_L & \twoheadrightarrow & \widetilde{\mathbb{E}}_L \end{array}$$

(iv) $[\varepsilon], [\tilde{t}_j] \in \mathbb{A}_L$ *for all* j.

(v) *There exists an* $\mathbb{A}^+_{W(k)}$*-subalgebra* $\mathbb{A}^+_L$ *of* $\mathbb{A}_L$ *and* $r_L \in \mathbb{Q}_{>0}$ *such that*:
  (a) *There exists* $a \in \mathbb{N}$ *such that* $p/\pi^a \in \mathbb{A}^+_L$ *and* $\mathbb{A}^+_L/(p/\pi^a) \cong \mathbb{E}^+_L$.
  (b) *If* $\alpha, \beta \in \mathbb{N}_{>0}$ *are such that* $\alpha/\beta < pr_L/(p-1)$, *then* $\mathbb{A}^+_L \subset \widetilde{\mathbb{A}}^+_L\{p^\alpha/\pi^\beta\}$; *here,* $\widetilde{\mathbb{A}}^+_L\{p^\alpha/\pi^\beta\}$ *denotes the* p*-adic Hausdorff completion of* $\widetilde{\mathbb{A}}^+_L[p^\alpha/\pi^\beta]$.
  (c) $\mathbb{A}^+_L$ *is complete for the weak topology.*

Moreover, by the uniqueness, $\mathbb{A}_L$ *is stable under the actions of* φ *and* $G_{L_\infty/K}$ *if* $L/\widetilde{K}$ *is Galois.*

Definition 1.9.4. Let $\mathbb{A}$ be the p-adic Hausdorff completion of $\bigcup_{L/\widetilde{K}} \mathbb{A}_L$, which is a subring of $\widetilde{\mathbb{A}}$ that is stable under the actions of both G_K and φ. We also put $\mathbb{B}_L := \mathbb{A}_L[1/p]$ and $\mathbb{B} := \mathbb{A}[1/p]$.

Remark 1.9.5. (i) As remarked in [Andreatta and Brinon 2008, §4.3], $\mathbb{A}_L$ is the unique finite étale $\mathbb{A}_{\widetilde{K}}$-algebra corresponding to $\mathbb{E}_L/\mathbb{E}_{\widetilde{K}}$; in particular, $\mathbb{A}_L$ is a Cohen ring of $\mathbb{E}_L$.

(ii) The action of $\Gamma_{\widetilde{K}}$ on $\mathbb{A}_{\widetilde{K}}$ is determined by the action of $\Gamma_{\widetilde{K}}$ on $\pi, [\tilde{t}_1], \dots, [\tilde{t}_d]$, since $\varepsilon - 1, \tilde{t}_1, \dots, \tilde{t}_d$ form a p-basis of $\mathbb{E}_{\widetilde{K}}$. Explicit descriptions are given by:

$$\gamma_a(\pi) = (1+\pi)^a - 1, \quad \gamma_a([\tilde{t}_j]) = [\tilde{t}_j] \text{ for } a \in \mathbb{Z}_p^\times,$$

$$\gamma_b(\pi) = \pi, \quad \gamma_b([\tilde{t}_j]) = (1+\pi)^{b_j}[\tilde{t}_j] \text{ for } b = (b_j) \in \mathbb{Z}_p^d.$$

Definition 1.9.6. For $h \in \mathbb{N}_{>0}$, an étale (φ^h, Γ_L)-module M over $\mathbb{B}_L$ is an étale φ^h-module over $\mathbb{B}_L$ endowed with a semilinear continuous G_K-action that commutes with the action of φ^h. Denote by $\mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}_L}(\varphi^h, \Gamma_L)$ the category of étale (φ^h, Γ_L)-modules over $\mathbb{B}_L$.

For $V \in \mathrm{Rep}_{\mathbb{Q}_{p^h}}(G_L)$, let $\mathbb{D}(V) := (\mathbb{B} \otimes_{\mathbb{Q}_{p^h}} V)^{H_L}$. For $M \in \mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}_L}(\varphi^h, \Gamma_L)$, let $\mathbb{V}(M) := (\mathbb{B} \otimes_{\mathbb{B}_K} M)^{\varphi^h=1}$.

Theorem 1.9.7 ([Andreatta 2006, Theorem 7.11] or [Andreatta and Brinon 2008, Théorème 4.34]). *Let $h \in \mathbb{N}_{>0}$. Then, the functor $\mathbb{D}$ gives a rank preserving equivalence of categories*

$$\mathbb{D} : \mathrm{Rep}_{\mathbb{Q}_{p^h}}(G_L) \to \mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}_L}(\varphi^h, \Gamma_L)$$

with quasi-inverse $\mathbb{V}$.

1.10. *Overconvergence of p-adic representations.* In this subsection, we will recall the overconvergence of p-adic representations in [Andreatta and Brinon 2008]. We still keep the notations of Section 1.9 and Assumption 1.9.1.

Definition 1.10.1. We apply Construction 1.6.1 to $(\widetilde{\mathbb{E}}, v_{\widetilde{\mathbb{E}}})$ with $\Gamma = \widetilde{\mathbb{A}}$ and write

$$\widetilde{\mathbb{A}}^{\dagger,r} := \Gamma_r,\ \widetilde{\mathbb{A}}^{\dagger} := \Gamma_{\mathrm{con}},\quad \widetilde{\mathbb{B}}^{\dagger,r} := \Gamma_r[1/p],\quad \widetilde{\mathbb{B}}^{\dagger} := \Gamma_{\mathrm{con}}[1/p],$$

$$\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} := \Gamma_{\mathrm{an},r},\quad \widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} := \Gamma_{\mathrm{an,con}}.$$

We define $v^{\leq n}_{\widetilde{\mathbb{E}}}$ and w_r the same way. For a finite extension $L/\widetilde{K}$, we apply a similar construction to the following $(E, v_{\widetilde{\mathbb{E}}})$ with Γ and we denote:

Γ	E	Γ_r	Γ_{con}	$\Gamma_r[1/p]$	$\Gamma_{\mathrm{con}}[1/p]$	$\Gamma_{\mathrm{an},r}$	$\Gamma_{\mathrm{an,con}}$
$\mathbb{A}$	$\mathbb{E}$	$\mathbb{A}^{\dagger,r}$	$\mathbb{A}^{\dagger}$	$\mathbb{B}^{\dagger,r}$	$\mathbb{B}^{\dagger}$	$\mathbb{B}^{\dagger,r}_{\mathrm{rig}}$	$\mathbb{B}^{\dagger}_{\mathrm{rig}}$
$\widetilde{\mathbb{A}}_L$	$\widetilde{\mathbb{E}}_L$	$\widetilde{\mathbb{A}}^{\dagger,r}_L$	$\widetilde{\mathbb{A}}^{\dagger}_L$	$\widetilde{\mathbb{B}}^{\dagger,r}_L$	$\widetilde{\mathbb{B}}^{\dagger}_L$	$\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},L}$	$\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig},L}$
$\mathbb{A}_L$	$\mathbb{E}_L$	$\mathbb{A}^{\dagger,r}_L$	$\mathbb{A}^{\dagger}_L$	$\mathbb{B}^{\dagger,r}_L$	$\mathbb{B}^{\dagger}_L$	$\mathbb{B}^{\dagger,r}_{\mathrm{rig},L}$	$\mathbb{B}^{\dagger}_{\mathrm{rig},L}$

By construction, we have $\widetilde{\mathbb{B}}^{\dagger} = \bigcup_r \widetilde{\mathbb{B}}^{\dagger,r}$, $\mathbb{B}^{\dagger} = \bigcup_r \mathbb{B}^{\dagger,r}$, $\widetilde{\mathbb{B}}^{\dagger,r}_K = \widetilde{\mathbb{B}}_K \cap \widetilde{\mathbb{B}}^{\dagger,r}$, $\widetilde{\mathbb{B}}^{\dagger}_K = \bigcup_r \widetilde{\mathbb{B}}^{\dagger,r}_K$, $\mathbb{B}^{\dagger,r}_K = \mathbb{B}_K \cap \mathbb{B}^{\dagger,r}$ and $\mathbb{B}^{\dagger}_K = \bigcup_r \mathbb{B}^{\dagger,r}_K$. We endow $\widetilde{\mathbb{B}}^{\dagger,r}$, $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$, ..., etc. with the Fréchet topologies defined by $\{w_s\}_{0<s\leq r}$.

We can describe $\mathbb{A}^{\dagger}_L$ by the ring of overconvergent power series.

Lemma 1.10.2 (cf. [Berger 2002, Proposition 1.4]). *Let $\mathcal{O}$ be a Cohen ring of $k_{\mathbb{E}_{\widetilde{K}}}$. Then, there exists an isomorphism $\mathbb{A}_{\widetilde{K}} \cong \mathcal{O}\{\{\pi\}\}$, which induces an isomorphism $\mathbb{A}^{\dagger,r}_{\widetilde{K}} \cong \mathcal{O}((\pi))^{\dagger}$ for all sufficiently small $r > 0$. Similarly, there exists an isomorphism $\mathbb{A}_L \cong \mathcal{O}'\{\{\pi'\}\}$, which induces an isomorphism $\mathbb{A}^{\dagger,r}_L \cong \mathcal{O}'((\pi'))^{\dagger,r/e_{\mathbb{E}_L/\mathbb{E}_{\widetilde{K}}}}$, where $\mathcal{O}'$ is a Cohen ring of $k_{\mathbb{E}_L}$.*

Proof. Fix any isomorphism $\mathbb{A}_{\widetilde{K}} \cong \mathcal{O}\{\{\pi\}\}$ (Remark 1.9.5(i)). Since $\varphi(\pi) = [\varepsilon]^p - 1 = (1+\pi)^p - 1 \in \mathcal{O}\{\{\pi\}\}^{\dagger}$, the assertion follows from Lemma 1.6.4. □

Notation 1.10.3. The isomorphism in Lemma 1.10.2 enables us to apply the results of Section 1.7. In particular, for any finite extension $L/\widetilde{K}$, we have a canonical continuous derivation

$$d : \mathbb{B}^{\dagger}_{\mathrm{rig},L} \to \Omega^{1}_{\mathbb{B}^{\dagger}_{\mathrm{rig},L}},$$

with $\Omega^{1}_{\mathbb{B}^{\dagger}_{\mathrm{rig},L}} := \mathbb{B}^{\dagger}_{\mathrm{rig},L} \otimes_{\mathbb{A}^{\dagger}_{L}} \Omega^{1}_{\mathbb{A}^{\dagger}_{L}}$ a free $\mathbb{B}^{\dagger}_{\mathrm{rig},L}$-module with basis $d\pi, d[\tilde{t}_1], \dots, d[\tilde{t}_d]$. Hence, we have a notion of (φ, ∇)-modules over $\mathbb{B}^{\dagger}_{\mathrm{rig},L}$ and the associated differential Swan conductors.

Definition 1.10.4. Let $h \in \mathbb{N}_{>0}$. An étale (φ^h, Γ_L)-module M over $\mathbb{B}^{\dagger}_{L}$ is an étale φ^h-module over $\mathbb{B}^{\dagger}_{L}$ endowed with a continuous semilinear G_K-action that commutes with the φ^h-action. Denote by $\mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}^{\dagger}_{L}}(\varphi^h, \Gamma_L)$ the category of étale (φ^h, Γ_L)-modules over $\mathbb{B}^{\dagger}_{L}$.

For $V \in \mathrm{Rep}_{\mathbb{Q}_{p^h}}(G_L)$, let

$$\mathbb{D}^{\dagger,r}(V) := (\mathbb{B}^{\dagger,r} \otimes_{\mathbb{Q}_{p^h}} V)^{H_L}, \qquad \mathbb{D}^{\dagger}(V) = \bigcup_r \mathbb{D}^{\dagger,r}(V),$$

$$\mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V) := \mathbb{B}^{\dagger,r}_{\mathrm{rig},L} \otimes_{\mathbb{B}^{\dagger,r}_{L}} \mathbb{D}^{\dagger,r}(V), \quad \mathbb{D}^{\dagger}_{\mathrm{rig}}(V) = \bigcup_r \mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V).$$

For $M \in \mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}^{\dagger}_{L}}(\varphi^h, \Gamma_L)$, let $\mathbb{V}(M) := (\mathbb{B}^{\dagger} \otimes_{\mathbb{B}^{\dagger}_{L}} M)^{\varphi^h=1}$.

Theorem 1.10.5 [Andreatta and Brinon 2008, Theorem 4.35]. *Let $h \in \mathbb{N}_{>0}$. The functor $\mathbb{D}^{\dagger}$ gives a rank preserving equivalence of categories*

$$\mathbb{D}^{\dagger} : \mathrm{Rep}_{\mathbb{Q}_{p^h}}(G_L) \to \mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}^{\dagger}_{L}}(\varphi^h, \Gamma_L)$$

with quasi-inverse $\mathbb{V}$. Moreover, $\mathbb{D}^{\dagger}$ and $\mathbb{V}$ are compatible with $\mathbb{D}$ and $\mathbb{V}$ in Theorem 1.9.7. Furthermore, $\mathbb{D}^{\dagger,r}(V)$ is free of rank $\dim_{\mathbb{Q}_{p^h}} V$ over $\mathbb{B}^{\dagger,r}_{K}$ for all sufficiently small r, and we have a canonical isomorphism $\mathbb{B}^{\dagger}_{K} \otimes_{\mathbb{B}^{\dagger,r}_{K}} \mathbb{D}^{\dagger,r}(V) \xrightarrow{\sim} \mathbb{D}^{\dagger}(V)$.

The functor $\mathbb{D}^{\dagger}_{\mathrm{rig}}$ will be studied in Section 4.5.

2. Adequateness of overconvergent rings

In this section, we will prove the "adequateness", which ensures that the elementary divisor theorem holds, for overconvergent rings defined in Section 1.6. The adequateness of overconvergent rings seems to be well-known to the experts: at least when the overconvergent ring is isomorphic the Robba ring, the adequateness follows from Lazard's results [1962] as in [Berger 2002, Proposition 4.12(5)]). Since the author could not find an appropriate reference, we give a proof.

Definition 2.0.1 [Helmer 1943, §2]. An integral domain R is adequate if the following hold:

(i) R is a Bézout ring, that is, any finitely generated ideal of R is principal.

(ii) For any $a, b \in R$ with $a \neq 0$, there exists a decomposition $a = a_1 a_2$ such that $(a_1, b) = R$ and $(a_3, b) \neq R$ for any nonunit factor a_3 of a_2.

Recall that if R is an adequate integral domain, then the elementary divisor theorem holds for free R-modules, see [Helmer 1943, Theorem 3]. Precisely speaking, let $N \subset M$ be finite free R-modules of ranks n and m respectively. Then, there exists a basis of $e_1, \dots, e_m$ (resp. $f_1, \dots, f_n$) of M (resp. N) and nonzero elements $\lambda_1 \mid \cdots \mid \lambda_n \in R$ such that $f_i = \lambda_i e_i$ for $1 \leq i \leq n$.

In the rest of this section, let the notation be as in Construction 1.6.1. We fix $r_0 > 0$ such that Γ has enough r_0-units and let $r \in (0, r_0)$ unless otherwise stated. Recall that $\Gamma_{\mathrm{an},r}$ is a Bézout integral domain.

Definition 2.0.2. We recall basic terminologies, see also [Kedlaya 2004, §3.5]. For $x \in \Gamma_{\mathrm{an},r}$ nonzero, we define the Newton polygon of x as the lower convex hull of the set of points $(v^{\leq n}(x), n)$, minus any segments of slope less than $-r$ on the left end and/or any segments of nonnegative slope on the right end of the polygon. We define the slopes of x as the negatives of the slopes of the Newton polygon of x. We also define the multiplicity of a slope $s \in (0, r]$ of x as the positive difference in y-coordinates between the endpoints of the segment of the Newton polygon of slope $-s$, or 0 if there is no such segment. If x has only one slope s, we say that x is pure of slope s.

A slope factorization of a nonzero element x of $\Gamma_{\mathrm{an},r}$ is a Fréchet-convergent product $x = \prod_{1 \leq i \leq n} x_i$ for n either a positive integer or ∞, where each x_i is pure of slope s_i with $s_1 > s_2 > \dots$ (cf. an explanation before [Kedlaya 2004, Lemma 3.26]).

Recall that the multiplicity is compatible with multiplication, i.e., the multiplicity of a slope s of xy is the sum of its multiplicities as a slope of x and of y [Kedlaya 2004, Corollary 3.22]. Also, recall that $x \in \Gamma_{\mathrm{an},r}$ is a unit if and only if x has no slopes [Kedlaya 2005, Corollary 2.5.12].

Lemma 2.0.3 [Kedlaya 2004, Lemma 3.26]. *Every nonzero element of $\Gamma_{\mathrm{an},r}$ has a slope factorization.*

For simplicity, we denote $\Gamma_{\mathrm{an},r}$ by R in the rest of this subsection. The lemma below is an immediate consequence of R being Bézout and the additivity of the multiplicity of a slope.

Lemma 2.0.4. (i) *Let $x, y \in R$ such that x is pure of slope s and let z be a generator of (x, y). Then, z is also pure of slope s, with multiplicity less than or equal to the multiplicity of slope s of x. In particular, if the multiplicity of the slope s of y is equal to zero, then z is a unit and we have $(x, y) = R$.*

(ii) *Let $x, y \in R$ such that x is pure of slope s. Then, the decreasing sequence of the ideals $\{(x, y^n)\}_{n \in \mathbb{N}}$ is eventually stationary.*

Lemma 2.0.5 (the uniqueness of slope factorizations). *Let $x \in R$ be a nonzero element. Let $x = \prod_i x_i = \prod_i x'_i$ be slope factorizations whose slopes are $s_1 > s_2 > \dots$ and $s'_1 > s'_2 > \dots$. Let m_i and m'_i be the multiplicities of s_i and s'_i for x_i and x'_i. Then, we have $s_i = s'_i$ and $x_i = x'_i u_i$ for some $u_i \in R^\times$. In particular, we have $m_i = m'_i$.*

Proof. We can easily reduce to the case $i = 1$. Since the multiplicity of the slope s_1 of $\prod_{i>1} x'_i$ is equal to zero, we have $(x_1, \prod_{i>1} x'_i) = R$ by Lemma 2.0.4(i). Hence, we have $(x_1, x) = (x_1, x_1 \prod_{i>1} x_i) = (x_1)$. By assumption, we have $s_1 \neq s'_j$ except for at most one j. Just as before, we have

$$(x_1, x) = \Bigl(x_1, x'_j \prod_{i \neq j} x'_i\Bigr) = (x_1, x'_j) = \Bigl(x_1 \prod_{i>1} x_i, x'_j\Bigr) = (x, x'_j) = \Bigl(x'_j \prod_{i \neq j} x'_i, x'_j\Bigr) = (x'_j),$$

i.e., $(x_1) = (x'_j)$. Hence, there exists $u \in R^\times$ such that $x_1 = x'_j u$. By the same argument, $x'_1 = x_l u'$ for some l and $u' \in R^\times$. Since $\{s_i\}$ and $\{s'_i\}$ are strictly decreasing, we must have $j = l = 1$, which implies the assertion. □

Lemma 2.0.6. *The integral domain $\Gamma_{\mathrm{an},r}$ is adequate. In particular, the elementary divisor theorem holds over $\Gamma_{\mathrm{an},r}$.*

Proof. We only have to prove that condition (ii) in Definition 2.0.1 is satisfied. Let $a, b \in R$ with $a \neq 0$. If $b = 0$, then it suffices to put $a_1 = 1$, $a_2 = a$. If b is a unit, then it suffices to put $a_1 = a$, $a_2 = 1$. Therefore, we may assume that b is neither a unit nor zero. Let $b = \prod_{i>0} b_i$ be a slope factorization with slopes $s_1 > s_2 > \dots$. By Lemma 2.0.4(ii), there exists $z_i \in R$ such that $(a, b_i^n) = (z_i)$ for all sufficiently large n. By [Kedlaya 2004, Proposition 3.13], we may assume that z_i admits a semi-unit decomposition, meaning that z_i is equal to a convergent sum of the form $1 + \sum_{j<0} u_{i,j} p^j$, where $u_{i,j} \in R^\times \cup \{0\}$. As in the proof of [Kedlaya 2004, Lemma 3.26], we can prove that $\{z_1 \dots z_i\}_{i>0}$ converges. Next, we claim that there exists $u_i \in R$ such that $a = z_1 \dots z_i u_i$. We proceed by induction on i. By definition, we have $a = z_1 u_1$ for some u_1. Assume that we have defined u_i. Since the multiplicity of the slope s_{i+1} of z_j is equal to zero for $1 \le j \le i$, we have $(z_j, z_{i+1}) = R$ for $1 \le j \le i$. Hence, we have $(z_{i+1}) = (a, z_{i+1}) = (z_1 \dots z_i u_i, z_{i+1}) = (u_i, z_{i+1})$, which implies $z_{i+1} \mid u_i$. Therefore, $u_{i+1} := u_i / z_{i+1}$ satisfies the condition. By this proof, we can choose $u_i = u_1/(z_1 \dots z_i)$. We put $a_1 := \lim_{i\to\infty} u_i = u_1 / \prod_{i>1} z_i$ and $a_2 := \prod_{i>0} z_i$, which is a slope factorization of a_2. We prove that the factorization $a = a_1 a_2$ satisfies the condition. We first prove $(a_1, b) = R$. By the uniqueness of slope factorizations, we only have to prove $(a_1, b_i) = R$ for all i. Fix $i \in \mathbb{N}_{>0}$. Then, for all sufficiently large $n \in \mathbb{N}$, we have

$$\begin{aligned}(z_i) = (a, b_i^n) = (a, b_i^{n+1}) = (a_1 a_2, b_i^{n+1}) &\subset (a_1, b_i)(a_2, b_i^n) \\ &\subset (a_1, b_i)(z_i, b_i^n) = (a_1, b_i)(z_i).\end{aligned}$$

Since $z_i \neq 0$, we have $R \subset (a_1, b_i)$, which implies the assertion. Finally, we prove $(a_3, b) \neq R$ for any nonunit $a_3 \in R$ dividing a_2. By replacing a_3 by any factor of a slope factorization of a_3, we may assume that a_3 is pure. By the uniqueness of slope factorizations, a_3 divides z_i for some i. Since $z_i \mid b_i^n$ for sufficiently large n, we also have $a_3 \mid b_i^n$. Hence, we have $(a_3, b_i) \neq R$, and in particular, $(a_3, b) \neq R$. $\square$

3. Variations of Gröbner basis argument

In this section, we will systematically develop a basic theory of Gröbner bases over various rings. Our theory generalizes the basic theory of Gröbner bases over fields ([Cox et al. 1997], particularly, §2). As a first application, we will prove the continuity of connected components of flat families of rigid analytic spaces over annuli (Proposition 3.4.5(iii)). As a second application, we prove the ramification compatibility of Scholl's fields of norms (Theorem 3.5.3).

The idea to use a Gröbner basis argument to study Abbes–Saito's rigid spaces of positive characteristic is in [Xiao 2010, §1]. Some results of this section, particularly Sections 3.2 and 3.3, are already proved there, however we do not use Xiao's results. We will work under a slightly stronger assumption and deduce stronger results, with much clearer and simpler proofs, than Xiao's. Note that this section is independent from the other parts of this paper, except Sections 1.5 and 1.8.

Notation 3.0.1. Throughout this section, we will use multi-index notation. We write $\underline{n} = (n_1, \dots, n_l) \in \mathbb{N}^l$, $|\underline{n}| := n_1 + \cdots + n_l$ and $\underline{X}^{\underline{n}} = X_1^{n_1} \dots X_l^{n_l}$ for variables $\underline{X} = (X_1, \dots, X_l)$. We also denote by $\underline{X}^{\mathbb{N}}$ the set of monic monomials $\{\underline{X}^{\underline{n}} \mid \underline{n} \in \mathbb{N}^l\}$.

In this section, when we consider a topology on a ring, we will use a norm $|\cdot|$ rather than a valuation.

3.1. ***Convergent power series.*** In this subsection, we consider rings of strictly convergent power series over the ring of rigid analytic functions over annuli, which play an analogous role to Tate algebra in the classical situation. We also gather basic definitions and facts on these rings for the rest of this section.

Definition 3.1.1. Let R be a ring. For $f = \sum_{\underline{n}} a_{\underline{n}} \underline{X}^{\underline{n}} \in R[\![\underline{X}]\!]$ with $a_{\underline{n}} \in R$, we call each $a_{\underline{n}} \underline{X}^{\underline{n}}$ a term of f. If $f = a_{\underline{n}} \underline{X}^{\underline{n}}$ with $a_{\underline{n}} \in R$, then we call f a monomial. If $a_{\underline{n}} = 1$, then f is called monic.

Definition 3.1.2 [Bosch et al. 1984, Section 1.4.1, Definition 1]. Let $(R, |\cdot|)$ be a normed ring. We define a Gauss norm on $R[\underline{X}]$ by $|\sum_{\underline{n}} a_{\underline{n}} \underline{X}^{\underline{n}}| := \sup_{\underline{n}} |a_{\underline{n}}|$. A formal power series $\sum_{\underline{n}} a_{\underline{n}} \underline{X}^{\underline{n}} \in R[\![\underline{X}]\!]$ is strictly convergent if $|a_{\underline{n}}| \to 0$ as $|\underline{n}| \to \infty$. We denote the ring of strictly convergent power series over R by $R\langle \underline{X} \rangle$. The above norm $|\cdot|$ can be uniquely extended to $|\cdot| : R\langle \underline{X} \rangle \to \mathbb{R}_{\geq 0}$. Note that if R is complete with respect to $|\cdot|$, then $R\langle \underline{X} \rangle$ is also complete with respect to $|\cdot|$, see [Bosch et al. 1984, Section 1.4.1, Proposition 3].

We recall basic facts on rings of strictly convergent power series. Let R be a complete normed ring, whose topology is equivalent to the $\mathfrak{a}$-adic topology for an ideal $\mathfrak{a}$. Then, $R\langle \underline{X}\rangle$ is canonically identified with the $\mathfrak{a}$-adic Hausdorff completion of $R[\underline{X}]$. We further assume that R is Noetherian. Then, $R\langle \underline{X}\rangle$ is R-flat. Moreover, for any ideal $\mathfrak{b}$ of R, we have a canonical isomorphism

$$R\langle \underline{X}\rangle \otimes_R (R/\mathfrak{b}) \cong (R/\mathfrak{b})\langle \underline{X}\rangle,$$

where the RHS means the $\mathfrak{a}$-adic Hausdorff completion of $(R/\mathfrak{b})[\underline{X}]$.

For a complete discrete valuation ring $\mathcal{O}$ with $F = \mathrm{Frac}(\mathcal{O})$, we denote by $\mathcal{O}\langle \underline{X}\rangle$ (resp. $F\langle \underline{X}\rangle$) the rings of convergent power series over $\mathcal{O}$ (resp. F).

Lemma 3.1.3. *Assume that R is a complete normed Noetherian ring, whose topology is equivalent to the $\mathfrak{a}$-adic topology for some ideal $\mathfrak{a}$ of R. Let $I \subset R\langle \underline{X}\rangle$ be an ideal such that $R\langle \underline{X}\rangle/I$ is R-flat. Then, I is also R-flat. Moreover, for any ideal $J \subset R$, we have $I \cap J \cdot R\langle \underline{X}\rangle = JI$. In particular, if $f \in I$ is divisible by $s \in R$ in $R\langle \underline{X}\rangle$, then $f/s \in I$.*

We omit the proof since it is an easy exercise in flatness.

Notation 3.1.4. In the rest of this subsection, we fix the notation as follows. Let $\mathcal{O}$ be a Cohen ring of a field k of characteristic p and fix a norm $|\cdot|$ on $\mathcal{O}$ corresponding to the p-adic valuation. We put

$$R^+ := \mathcal{O}[\![S]\!] \subset R := \mathcal{O}((S))$$

and for $r \in \mathbb{Q}_{>0}$, we define a norm

$$|\cdot|_r : R \to \mathbb{R}_{\geq 0}$$
$$\sum_{n \gg -\infty} a_n S^n \mapsto \sup_n |a_n||p|^{rn},$$

which is multiplicative by [Kedlaya 2010, Proposition 2.1.2]. Recall the definition

$$R^{\dagger,r} = \left\{ \sum_{n\in\mathbb{Z}} a_n S^n \in \mathcal{O}\{\{S\}\};\ |a_n S^n|_r \to 0 \text{ as } n \to -\infty \right\}$$

from Notation 1.6.2. Note that we may canonically identify $R^{\dagger,r}/pR^{\dagger,r}$ with $k((S))$. We can extend $|\cdot|_r$ to $|\cdot|_r : R^{\dagger,r} \to \mathbb{R}_{\geq 0}$ by $|\sum_n a_n S^n|_r := \sup_n |a_n S^n|_r$. We define subrings of $R^{\dagger,r}$ by

$$R_0^{\dagger,r} := \{f \in R^{\dagger,r};\ |f|_r \leq 1\},$$

$$\mathcal{R}_0^{\dagger,r} := R_0^{\dagger,r} \cap R = \{f \in R;\ |f|_r \leq 1\}.$$

Note that for $a, b \in \mathbb{N}$ with $b > 0$, $|p^a/S^b|_r \leq 1$ if and only if $a/b \geq r$. Also, note that $R^{\dagger,r} = R_0^{\dagger,r}[S^{-1}]$ since $|S|_r < 1$. We may regard $R^{\dagger,r}$ as the ring of rigid analytic functions on the annulus $[p^r, 1)$ whose values at the boundary $|S| = 1$ are bounded by 1.

Lemma 3.1.5. (i) *The R^+-algebra $\mathcal{R}_0^{\dagger,r}$ is finitely generated.*

(ii) *The topologies of $R_0^{\dagger,r}$ defined by $|\cdot|_r$ and by the ideal (p, S) are equivalent.*

(iii) *The rings $R_0^{\dagger,r}$ and $R^{\dagger,r}$ are complete with respect to $|\cdot|_r$, and $\mathcal{R}_0^{\dagger,r}$ is dense in $R_0^{\dagger,r}$.*

(iv) *The rings $\mathcal{R}_0^{\dagger,r}$, $R_0^{\dagger,r}$, and $R^{\dagger,r}$ are Noetherian integral domains.*

Proof. Let $a, b \in \mathbb{N}_{>0}$ denote relatively prime integers such that $r = a/b$.

(i) It is straightforward to check that $\mathcal{R}_0^{\dagger,r}$ is generated as an R^+-algebra by $p^{\lfloor rb' \rfloor}/S^{b'}$ for $b' \in \{0, \dots, b\}$.

(ii) For $n \in \mathbb{N}$, we have

$$\sup\left\{|x|_r;\ x \in (p, S)^n R_0^{\dagger,r}\right\} \leq \left\{\inf(|p|, |S|_r)\right\}^n$$

and the RHS converges to 0 as $n \to \infty$. Hence, the (p, S)-adic topology of $R_0^{\dagger,r}$ is finer than the topology defined by $|\cdot|_r$. To prove that the topology of $R_0^{\dagger,r}$ defined by $|\cdot|_r$ is finer than the (p, S)-adic topology, it suffices to prove that

$$\left\{x \in R_0^{\dagger,r};\ |x|_r \leq |(pS)^n|_r\right\} \subset (p, S)^n R_0^{\dagger,r}$$

for all $n \in \mathbb{N}$. Let $x = \sum_{m\in\mathbb{Z}} a_m S^m \in \text{LHS}$ with $a_m \in \mathcal{O}$. Then, we have $|a_m S^{m-n}|_r \leq |p^n| \leq 1$. Hence, $x = S^n \sum_{m\in\mathbb{Z}} a_m S^{m-n} \in S^n \cdot R_0^{\dagger,r}$, which implies the assertion.

(iii) If $f = \sum_{n\in\mathbb{Z}} a_n S^n \in R_0^{\dagger,r}$ with $a_n \in \mathcal{O}$, then $\left\{\sum_{n\geq -m} a_n S^n\right\}_{m\in\mathbb{N}} \subset \mathcal{R}_0^{\dagger,r}$ converges to f, which implies the last assertion. Since $R_0^{\dagger,r}$ is an open subring of $R^{\dagger,r}$, we only have to prove completeness of $R_0^{\dagger,r}$. Let $\{f_m\}_{m\in\mathbb{N}} \subset R_0^{\dagger,r}$ be a sequence such that $|f_m|_r \to 0$ as $m \to \infty$. We only have to prove that the limit $\sum_m f_m$ exists in $R_0^{\dagger,r}$ with respect to $|\cdot|_r$. Write $f_m = \sum_{n\in\mathbb{Z}} a_n^{(m)} S^n$ with $a_n^{(m)} \in \mathcal{O}$. For $n \in \mathbb{Z}$, we have

$$|a_n^{(m)}| \leq \frac{|f_m|_r}{|S^n|_r} = |p|^{-nr} |f_m|_r,$$

hence, $|a_n^{(m)}| \to 0$ as $m \to \infty$. Moreover, $a_n := \sum_{m\in\mathbb{N}} a_n^{(m)} \in \mathcal{O}$ converges to 0 as $n \to -\infty$. Hence, the formal Laurent series $f := \sum_{n\in\mathbb{Z}} a_n S^n$ belongs to $\mathcal{O}\{\{S\}\}$. Since

$$|a_n S^n|_r \leq \sup_{m\in\mathbb{N}} |a_n^{(m)} S^n|_r \leq \sup_{m\in\mathbb{N}} |f_m|_r \leq 1,$$

we have $f \in R_0^{\dagger,r}$. For $m \in \mathbb{N}$, we have

$$|f - (f_0 + \cdots + f_m)|_r \le \sup_n |a_n S^n - (a_n^{(0)} + \cdots + a_n^{(m)}) S^n|_r$$
$$\le \sup_n \sup_{l>m} |a_n^{(l)} S^n|_r = \sup_{l>m} \sup_n |a_n^{(l)} S^n|_r \le \sup_{l>m} |f_l|_r$$

and the last term converges to 0 as $m \to \infty$, which implies $f = \sum_m f_m$.

(iv) This follows from (i), (ii) and (iii). □

Definition 3.1.6. Let $R^+\langle \underline{X} \rangle$ be the (p, S)-adic Hausdorff completion of $R^+[\underline{X}]$. We also define $R_0^{\dagger,r}\langle \underline{X} \rangle$ and $R^{\dagger,r}\langle \underline{X} \rangle$ as the rings of strictly convergent power series over $R_0^{\dagger,r}$ and $R^{\dagger,r}$ with respect to $|\cdot|_r$. We endow $R_0^{\dagger,r}\langle \underline{X} \rangle$ and $R^{\dagger,r}\langle \underline{X} \rangle$ with the topology defined by the norm $|\cdot|_r$. By Lemma 3.1.5(iii), $R_0^{\dagger,r}\langle \underline{X} \rangle$ and $R^{\dagger,r}\langle \underline{X} \rangle$ are complete. By Lemma 3.1.5(ii), $R_0^{\dagger,r}\langle \underline{X} \rangle$ can be regarded as the (p, S)-adic Hausdorff completion of $R_0^{\dagger,r}[\underline{X}]$, hence, $R_0^{\dagger,r}\langle \underline{X} \rangle$ and $R^{\dagger,r}\langle \underline{X} \rangle = R_0^{\dagger,r}\langle \underline{X} \rangle[S^{-1}]$ are Noetherian integral domains by Lemma 3.1.5(iv). Also, we may view $R^+\langle \underline{X} \rangle$ as a subring of $R_0^{\dagger,r}\langle \underline{X} \rangle$.

The following lemma seems to be used implicitly in [Xiao 2010, §1].

Lemma 3.1.7. *The canonical map $R^+\langle \underline{X} \rangle \to R^{\dagger,r}\langle \underline{X} \rangle$ is flat.*

Proof (due to Liang Xiao). We may regard $R_0^{\dagger,r}\langle \underline{X} \rangle$ as the (p, S)-adic Hausdorff completion of $R^+\langle \underline{X} \rangle \otimes_{R^+} R_0^{\dagger,r}$. Since $\mathcal{R}_0^{\dagger,r}$ is dense in $R_0^{\dagger,r}$ by Lemma 3.1.5(iii), $R_0^{\dagger,r}\langle \underline{X} \rangle$ can be viewed as the (p, S)-adic Hausdorff completion of $R^+\langle \underline{X} \rangle \otimes_{R^+} \mathcal{R}_0^{\dagger,r}$, which is Noetherian by Lemma 3.1.5(i). Hence, the canonical map

$$\alpha : R^+\langle \underline{X} \rangle \otimes_{R^+} \mathcal{R}_0^{\dagger,r} \to R_0^{\dagger,r}\langle \underline{X} \rangle$$

is flat. Since $\mathcal{R}_0^{\dagger,r}[S^{-1}] = R$ and $R_0^{\dagger,r}\langle \underline{X} \rangle[S^{-1}] = R^{\dagger,r}\langle \underline{X} \rangle$, the canonical map $\alpha[S^{-1}]$ is also flat, which implies the assertion. □

Next, we consider prime ideals corresponding to good "points" of the open unit disc $R^+ = \mathcal{O}[\![S]\!]$.

Definition 3.1.8. An Eisenstein polynomial in R^+ is a polynomial in $\mathcal{O}[S]$ of the form $P(S) = S^e + a_{e-1}S^{e-1} + \cdots + a_0$ with $a_i \in \mathcal{O}$ such that $p \mid a_i$ for all i and $p^2 \nmid a_0$. We call $\mathfrak{p} \in \mathrm{Spec}(R^+)$ an Eisenstein prime ideal if $\mathfrak{p}$ is generated by an Eisenstein polynomial $P(S)$. Then, we put $\deg(\mathfrak{p}) := e$ if $e \neq 0$ and $\deg(\mathfrak{p}) := \infty$ if $e = 0$. Note that we may regard $\kappa(\mathfrak{p}) := R/\mathfrak{p}R$ as a complete discrete valuation field with integer ring $R^+/\mathfrak{p}R^+$. We denote by $\pi_{\mathfrak{p}} \in \mathcal{O}_{\kappa(\mathfrak{p})}$ the image of S, which is a uniformizer of $\mathcal{O}_{\kappa(\mathfrak{p})}$. Note that $\deg(\mathfrak{p}) < \infty$ if and only if the characteristic of $R/\mathfrak{p}$ is zero. For simplicity, we write $\kappa(p)$ and S instead of $\kappa((p))$ and $\pi_{\kappa((p))}$.

Lemma 3.1.9. *Let* $\mathfrak{p}$ *and* $\mathfrak{q}$ *be Eisenstein prime ideals of* R^+*. If*

$$\inf(v_{\kappa(\mathfrak{p})}(x \bmod \mathfrak{p}), v_{\kappa(\mathfrak{q})}(x \bmod \mathfrak{q})) < \inf(\deg \mathfrak{p}, \deg \mathfrak{q}),$$

for $x \in R^+$*, then we have* $v_{\kappa(\mathfrak{p})}(x \bmod \mathfrak{p}) = v_{\kappa(\mathfrak{q})}(x \bmod \mathfrak{q})$.

Proof. Let $x \in R^+$ and $i \in \mathbb{N}$ such that $0 \leq i < \deg \mathfrak{p}$. Then, we have the following equivalences:

$$\begin{aligned} v_{\kappa(p)}(x \bmod p) = i &\iff x \in (p, S^i) \setminus (p, S^{i+1}) \\ &\iff x \in (\mathfrak{p}, S^i) \setminus (\mathfrak{p}, S^{i+1}) \iff v_{\kappa(\mathfrak{p})}(x \bmod \mathfrak{p}) = i, \end{aligned}$$

where the second equivalence follows from the fact $(\mathfrak{p}, S^i) = (p, S^i)$, and the other equivalences follow from the definitions. By replacing $\mathfrak{q}$ by $\mathfrak{p}$, we obtain similar equivalences. As a result, $v_{\kappa(\mathfrak{p})}(x \bmod \mathfrak{p}) = i \Leftrightarrow v_{\kappa(\mathfrak{q})}(x \bmod \mathfrak{q}) = i$ for $x \in R^+$ and $i < \inf(\deg(\mathfrak{p}), \deg(\mathfrak{q}))$, which implies the assertion. □

The ring $R^{\dagger,r}\langle \underline{X} \rangle$ can be considered as a family of Tate algebras:

Lemma 3.1.10. *Let* $\mathfrak{p}$ *be an Eisenstein prime ideal of* R^+ *with* $e = \deg(\mathfrak{p})$*. Let* $r \in \mathbb{Q}_{>0}$ *satisfy* $1/e \leq r$*. Then, there exists a canonical isomorphism*

$$R^{\dagger,r}\langle \underline{X} \rangle / \mathfrak{p} R^{\dagger,r}\langle \underline{X} \rangle \xrightarrow{\sim} \kappa(\mathfrak{p})\langle \underline{X} \rangle.$$

In particular, $\mathfrak{p}R^{\dagger,r} \neq R^{\dagger,r}$.

Proof. We will briefly recall a result in [Lazard 1962]. Let F be a complete discrete valuation field of mixed characteristic $(0, p)$. Recall that $L_F[0, r]$ is the ring of Laurent series with variable S and coefficients in F, which converge in the annulus $|p|^r \leq |S| < 1$, see [Lazard 1962, §1.3]. For $r' \in \mathbb{Q}_{>0}$, a polynomial $P \in F[S]$ is said to be r'-extremal if all zeroes x of P in F^{alg} satisfy $v(x) = r'$, see [Lazard 1962, §2.7]. Let $r' \leq r$ be a positive rational number and $P \in F[S]$ an r'-extremal polynomial. Then, for $f \in L_F[0, r]$, there exist a unique $g \in L_F[0, r]$ and a unique polynomial $Q \in F[S]$ of degree less than $\deg P$ such that $f = Pg + Q$, which is a special case of [Lazard 1962, Lemme 2]. Note that if $f \in F[S]$ with $\deg(f) < \deg(P)$, then we have $g = 0$ and $Q = f$ by the uniqueness. In particular, the canonical map $\delta : F[S]/P \cdot F[S] \to L_F[0, r]/P \cdot L_F[0, r]$ is an isomorphism.

We prove the assertion. We can easily reduce to the case $\underline{X} = \phi$. That is, we only have to prove that the canonical map

$$R^{\dagger,r}/\mathfrak{p}R^{\dagger,r} \to \kappa(\mathfrak{p})$$

is an isomorphism. The assertion is trivial when $\mathfrak{p} = (p)$. Hence, we may assume $\mathfrak{p} \neq (p)$. Since p is invertible in $\kappa(\mathfrak{p})$, p is also invertible in $R^{\dagger,r}/\mathfrak{p}R^{\dagger,r}$. Hence, we have $R^{\dagger,r}/\mathfrak{p}R^{\dagger,r} = R^{\dagger,r}[1/p]/\mathfrak{p}R^{\dagger,r}[1/p]$. Note that $R^{\dagger,r}[1/p]$ coincides, by definition, with $L_F[0, r]$ with $F := \mathrm{Frac}(\mathcal{O})$. Let $P \in \mathcal{O}[S]$ be an Eisenstein polynomial which generates $\mathfrak{p}$. Then, P is $1/e$-extremal by a property of Eisenstein polynomials. Hence, the assertion follows from the isomorphisms

$$\begin{aligned} L_F[0,r]/\mathfrak{p}L_F[0,r] &\cong F[S]/P\cdot F[S] \\ &\cong (\mathcal{O}[S]/P\cdot\mathcal{O}[S])[1/p] \cong (R^+/\mathfrak{p})[1/p] = \kappa(\mathfrak{p}). \end{aligned}$$

Here, the first isomorphism is Lazard's δ, with $r' = 1/e$. □

3.2. ***Gröbner basis argument over complete regular local rings.*** In this subsection, we will develop a basic theory of Gröbner bases over complete regular local rings R, which generalizing that over fields. This is done in [Xiao 2010, §1.1], when R is a 1-dimensional complete regular local ring of characteristic p. We assume knowledge of the classical theory of Gröbner bases over fields; our basic reference is [Cox et al. 1997].

Recall that the classical theory of Gröbner bases on $F[\underline{X}]$ for a field F can be regarded as a multi-variable version of the Euclidean division algorithm of the 1-variable polynomial ring $F[X]$. To obtain an appropriate division algorithm in $F[\underline{X}]$, we need to fix a "monomial order" on $F[\underline{X}]$ in order to define a leading term, which is the analogue of the naïve degree function in the 1-variable case. Hence, we should first define a notion of leading terms over the ring of convergent power series.

Definition 3.2.1. A monomial order $\succeq$ on a commutative monoid $(M,+)$ is an well-order such that if $\alpha\succeq\beta$, then $\alpha+\gamma\succeq\beta+\gamma$. When $\alpha\succeq\beta$ and $\alpha\neq\beta$, we write $\alpha\succ\beta$.

In the following, we restrict to the case where M is isomorphic to $\mathbb{N}^l$. Moreover, the reader may assume that $\succ$ is a lexicographic order; the lexicographic order $\succeq_{\text{lex}}$ on $\mathbb{N}^l$ is defined by $(a_1,\dots,a_l)\succ_{\text{lex}}(a'_1,\dots,a'_l)$ if $a_1=a'_1,\dots,a_i=a'_i, a_{i+1}>a'_{i+1}$. A lexicographic order is a monomial order, see [Cox et al. 1997, §2.2, Proposition 4].

For convenience, we define a monoid $M\cup\{\infty\}$ by $\alpha+\infty=\infty$ for any $\alpha\in M\cup\{\infty\}$. We extend any monomial order $\succeq$ on M to $M\cup\{\infty\}$ by $\infty\succ\alpha$ for any $\alpha\in M$.

Construction 3.2.2. Let R be a complete regular local ring of Krull dimension d with fixed regular system of parameters $\{s_1,\dots,s_d\}$. We put $R_i := R/(s_1,\dots,s_i)R$, which is also a regular local ring. We denote the image of $s_{i+1},\dots,s_d$ in R_i by $s_{i+1},\dots,s_d$ again and we regard these as a fixed regular system of parameters. Let $v_{s_i}: R_i \twoheadrightarrow \mathbb{N}\cup\{\infty\}$ be the multiplicative valuation associated to the divisor $s_i=0$. For a nonzero $f\in R$ and $0\leq i\leq d$, we define a nonzero $f^{(i)}\in R_i$ inductively as follows. We put $f^{(0)} := f$, and define $f^{(i+1)}$ as the image of $f^{(i)}/s_{i+1}^{v_{s_{i+1}}(f^{(i)})}$ in R_{i+1}, which is nonzero by definition. We put $\underline{v}_R(f) := (v_{s_1}(f^{(0)}), v_{s_2}(f^{(1)}),\dots,v_{s_d}(f^{(d-1)}))\in\mathbb{N}^d$ and $\underline{v}_R(0) := \infty$. Thus, we obtain a map $\underline{v}_R: R\to\mathbb{N}^d\cup\{\infty\}$. We also apply this construction to each R_i. Note that we have a formula

$$\underline{v}_R(f) = \big(v_{s_1}(f), \underline{v}_{R_1}(f^{(1)})\big). \tag{1}$$

Also, note that $\underline{v}_R$ is multiplicative, i.e., $\underline{v}_R(fg) = \underline{v}_R(f) + \underline{v}_R(g)$, which follows by induction on d and by using the formula.

Let $R\langle \underline{X}\rangle$ be the $\mathfrak{m}_R$-adic Hausdorff completion of $R[\underline{X}]$. We fix a monomial order $\succeq$ on $\underline{X}^{\mathbb{N}} \cong \mathbb{N}^l$. For any nonzero $f = \sum_{\underline{n}} a_{\underline{n}} \underline{X}^{\underline{n}} \in R\langle \underline{X}\rangle$ with $a_{\underline{n}} \in R$, we define $\underline{v}_R(f) := \inf_{\succeq_{\mathrm{lex}}} \underline{v}_R(a_{\underline{n}})$, where $\succeq_{\mathrm{lex}}$ is the lexicographic order on $\mathbb{N}^d$, and $\underline{\deg}_R(f) := \inf_{\succeq}\{\underline{n} \in \mathbb{N}^l;\ \underline{v}_R(a_{\underline{n}}) = \underline{v}_R(f)\}$. We put $\underline{\deg}_R(0) := \infty$. Note that when $f \neq 0$, we have a formula

$$\underline{\deg}_R(f) = \underline{\deg}_R(f^{(0)}) = \underline{\deg}_R(f^{(1)}) = \cdots = \underline{\deg}_R(f^{(d)}), \tag{2}$$

which follows from (1). Also, note that $\underline{\deg}_R$ is multiplicative. Indeed, formula (2) allows us to reduce to the case where R is a field; here $\underline{\deg}_R$ is multiplicative by [Cox et al. 1997, Chapter 2, Lemma 8]. Thus, we obtain a multiplicative map

$$\underline{v}_R \times \underline{\deg}_R \colon R\langle \underline{X}\rangle \to (\mathbb{N}^d \times \mathbb{N}^l) \cup \{\infty\},$$

where ∞ in the RHS denotes (∞, ∞). We endow $\mathbb{N}^d \times \mathbb{N}^l$ with a total order $\succeq$ by

$$(\underline{a}, \underline{n}) \succeq (\underline{a}', \underline{n}') \text{ if } \underline{a} \preceq_{\mathrm{lex}} \underline{a}' \text{ or } \underline{a} = \underline{a}' \text{ and } \underline{n} \succeq \underline{n}'$$

and extend it to $(\mathbb{N}^d \times \mathbb{N}^l) \cup \{\infty\}$ as in Definition 3.2.1. Note that this order is an extension of the fixed order on $\mathbb{N}^l = \{0\} \times \ldots \{0\} \times \mathbb{N}^l$. As in the classical notation, we also define

$$\mathrm{LT}_R(f) := \underline{s}^{\underline{v}_R(f)} \underline{X}^{\underline{\deg}_R(f)} \quad \text{for } f \neq 0, \mathrm{LT}_R(0) := 0,$$

where $\underline{s} = (s_1, \ldots, s_d)$. Note that LT_R is also multiplicative by the multiplicativities of $\underline{v}_R$ and $\underline{\deg}_R$. We also have the formula

$$\mathrm{LT}_R(f) \equiv \mathrm{LT}_{R_i}(f \bmod (s_1, \ldots, s_i)) \bmod (s_1, \ldots, s_i),\ \forall f \in R\langle \underline{X}\rangle. \tag{3}$$

Indeed, if $s_i \mid f^{(i-1)}$ for some i, then both sides are zero. If $s_i \nmid f^{(i-1)}$ for all i, then the formula follows from (1) and (2). The map LT_R takes values in the subset $\underline{s}^{\mathbb{N}} \underline{X}^{\mathbb{N}} \cup \{0\}$ of $R\langle \underline{X}\rangle$. We identify $\underline{s}^{\mathbb{N}} \underline{X}^{\mathbb{N}} \cup \{0\}$ with $(\mathbb{N}^d \times \mathbb{N}^l) \cup \{\infty\}$ as a monoid and consider the total order $\succeq$ on $\underline{s}^{\mathbb{N}} \underline{X}^{\mathbb{N}} \cup \{0\}$.

When R is a field, the above definition coincides with the classical definition as in [Cox et al. 1997, §2].

Remark 3.2.3. LT stands for "leading term" with respect to a given monomial order in the classical case $d = 0$. To define an appropriate LT in the case $d > 0$, we should consider a suitable order on the coefficient ring R, which is defined by using an ordered regular system of parameters as above. Our definition is compatible with dévissage, namely, compatible with parameter-reducing maps $R \to R_1 \to \cdots \to R_d$. This property enables us to reduce everything about Gröbner bases to the classical case by assuming a certain "flatness" as we will see below.

In the rest of this subsection, let the notation be as in Construction 3.2.2. In particular, we fix a monomial order $\succeq$ on $\underline{X}^{\mathbb{N}}$.

Definition 3.2.4. For I an ideal of $R\langle\underline{X}\rangle$, we denote by $\mathrm{LT}_R(I)$ the ideal of $R\langle\underline{X}\rangle$ generated by $\{\mathrm{LT}_R(f);\ f \in I\}$. Assume that $R\langle\underline{X}\rangle/I$ is R-flat. We say that $f_1, \dots, f_s \in I$ form a Gröbner basis if $(\mathrm{LT}_R(f_1), \dots, \mathrm{LT}_R(f_s)) = \mathrm{LT}_R(I)$. Note that a Gröbner basis always exists since $R\langle\underline{X}\rangle$ is Noetherian.

Note that for monomials $f, f_1, \dots, f_s \in R\langle\underline{X}\rangle$, we have $f \in (f_1, \dots, f_s)$ if and only if f is divisible by some f_i. Indeed, any term of $g \in (f_1, \dots, f_s)$ is divisible by some f_i, which implies the necessity.

Notation 3.2.5. Let I be an ideal of $R\langle\underline{X}\rangle$ such that $R\langle\underline{X}\rangle/I$ is R-flat. We write $I_i := I/(s_1, \dots, s_i)I$. We may identify $R\langle\underline{X}\rangle \otimes_R R_i$ and $I \otimes_R R_i$ with $R_i\langle\underline{X}\rangle$ and I_i, respectively. Note that $R_i\langle\underline{X}\rangle/I_i$ is R_i-flat.

Lemma 3.2.6. *Let I be an ideal of $R\langle\underline{X}\rangle$ such that $R\langle\underline{X}\rangle/I$ is R-flat. The following are equivalent for $f_1, \dots, f_s \in I$:*

(i) *$f_1, \dots, f_s$ form a Gröbner basis of I.*

(ii) *The images of $f_1, \dots, f_s$ form a Gröbner basis of $I_i \subset R_i\langle\underline{X}\rangle$ for some i.*

Moreover, when $f_1, \dots, f_s$ is a Gröbner basis of I, $f_1, \dots, f_s$ generate I.

Proof. We prove the first assertion by induction on $d = \dim R$. When $d = 0$, there is nothing to prove. Assume the assertion is true for dimension $< d$. By the induction hypothesis, we only have to prove the equivalence between (i) and (ii) with $i = 1$.

We first prove (i) $\Rightarrow$ (ii). Let $\bar{f} \in I_1$ be a nonzero element and $f \in I$ a lift of $\bar{f}$. By assumption, we have $\mathrm{LT}_R(f_j) \mid \mathrm{LT}_R(f)$ for some j. Then, $\mathrm{LT}_{R_1}(f_j \bmod s_1)$ divides $\mathrm{LT}_{R_1}(\bar{f})$ by formula (3).

We prove (ii) $\Rightarrow$ (i). Let $f \in I$ be a nonzero element. By Lemma 3.1.3, we have $f^{(1)} = f/s_1^{v_{s_1}(f)} \in I$. By assumption, we have $\mathrm{LT}_{R_1}(f_j \bmod s_1) \mid \mathrm{LT}_{R_1}(f^{(1)} \bmod s_1)$ for some j. Since $\mathrm{LT}_{R_1}(f^{(1)} \bmod s_1) \neq 0$, s_1 does not divides f_j, i.e., $v_{s_1}(f_j) = 0$. By formulas (1) and (2), $\mathrm{LT}_R(f_j)$ divides $\mathrm{LT}_R(f^{(1)})$, and hence divides $\mathrm{LT}_R(f)$, which implies the assertion.

We prove the last assertion. By Nakayama's lemma and (ii) with $i = d$, the assertion is reduced to the case where R is a field. In this case, the assertion follows from [Cox et al. 1997, §2.5, Corollary 6]. □

Remark 3.2.7. By Lemma 3.2.6, $f_1, \dots, f_s$ is a Gröbner basis of I if and only if $f_1 \bmod \mathfrak{m}_R, \dots, f_s \bmod \mathfrak{m}_R$ is a Gröbner basis of $I/\mathfrak{m}_R I$. In particular, the definition of Gröbner basis does not depend on the choice of a regular system of parameters $\{s_1, \dots, s_d\}$.

We can generalize the classical division algorithm, which is a basic tool in many Gröbner basis arguments.

Proposition 3.2.8 (division algorithm). *Let I be an ideal of $R\langle \underline{X} \rangle$ such that $R\langle \underline{X} \rangle / I$ is R-flat. Let $f_1, \dots, f_s \in I$ be a Gröbner basis of I. Then, for any nonzero $f \in R\langle \underline{X} \rangle$, there exist $a_i, r \in R\langle \underline{X} \rangle$ for all i such that*

$$f = \sum_{1 \le i \le s} a_i f_i + r,$$

with $\mathrm{LT}_R(f) \succeq \mathrm{LT}_R(a_i f_i)$ if $a_i f_i \neq 0$, and any nonzero term of r is not divisible by any $\underline{X}^{\underline{\deg}_R(f_i)}$. Moreover, such r is uniquely determined (but the a_i's are not), and $f \in I$ if and only if $r = 0$.

Proof. When $d = 0$, i.e, R is a field, the assertion is well known (see [Cox et al. 1997, §2.6, Proposition 1] for example). We prove the first assertion by induction on $d = \dim R$. Assume that the assertion is true for dimension $< d$. We may assume $s_1 \nmid f_i$ for all i. Indeed, by Lemma 3.2.6, the set $\{f_i;\ s_1 \nmid f_i\}$ forms a Gröbner basis of I. Moreover, any $\mathrm{LT}_R(f_j)$ is divisible by some $\mathrm{LT}_R(f_i)$ with $s_1 \nmid f_i$. Therefore, if we can write $f = \sum_{i : s_1 \nmid f_i} a_i f_i + r$ with respect to $\{f_i;\ s_1 \nmid f_i\}$, then we can write f in the same way with respect to $f_1, \dots, f_s$. First, we construct $g_n \in R\langle \underline{X} \rangle$ by induction on $n \in \mathbb{N}$. For $h \in R\langle \underline{X} \rangle$, let $\bar{h}$ be its image in $R_1\langle \underline{X} \rangle$. Put $g_0 := f$. Assume that g_n has been defined. Put $g_n' := g_n / s_1^{v_{s_1}(g_n)}$. By applying the induction hypothesis to $I_1 = (\bar{f}_1, \dots, \bar{f}_s)$, we have $\bar{a}_{i,n}, \bar{r}_n \in R_1\langle \underline{X} \rangle$ with

$$\bar{g}_n' = \sum_i \bar{a}_{i,n} \bar{f}_i + \bar{r}_n,$$

such that no nonzero terms of $\bar{r}_n$ are divisible by any $\underline{X}^{\underline{\deg}_{R_1}(\bar{f}_i)}$, and such that $\mathrm{LT}_{R_1}(\bar{g}_n') \succeq \mathrm{LT}_{R_1}(\bar{a}_{i,n} \bar{f}_i)$ if $\bar{a}_{i,n} \bar{f}_i \neq 0$. We choose lifts $a_{i,n}$ and r_n in $R\langle \underline{X} \rangle$ of $\bar{a}_{i,n}$ and $\bar{r}_n$, respectively, such that no nonzero terms of $a_{i,n}$ and r_n are divisible by s_1. Then, we put $g_{n+1} := g_n - s_1^{v_{s_1}(g_n)} \big(\sum_i a_{i,n} f_i + r_n \big)$. By construction, we have $v_{s_1}(g_{n+1}) > v_{s_1}(g_n)$, hence, $\{g_n\}$ converges s_1-adically to zero. Moreover, $a_i := \sum_n s_1^{v_{s_1}(g_n)} a_{i,n}$ and $r := \sum_n s_1^{v_{s_1}(g_n)} r_n$ converge s_1-adically and we have $f = \sum_i a_i f_i + r$. We will check that a_i and r satisfy the condition. Since $s_1 \nmid f_i$ and since no nonzero term of r_n is divisible by s_1, no nonzero term of r is divisible by $\underline{X}^{\underline{\deg}_R(f_i)}$ for all i. We have $v_{s_1}(f_i) = 0$ by assumption and $v_{s_1}(a_i) \geq v_{s_1}(f)$ by definition. If $v_{s_1}(a_i) > v_{s_1}(f)$, then we have $\underline{v}_R(f) \preceq_{\mathrm{lex}} \underline{v}_R(a_i f_i)$, hence, $\mathrm{LT}_R(f) \succeq \mathrm{LT}_R(a_i f_i)$. If $v_{s_1}(a_i) = v_{s_1}(f)$, then we have $a_i^{(0)} \equiv a_{i,0} \bmod s_1$, hence, $\underline{v}_R(f) \preceq \underline{v}_R(a_i f_i)$ by formulas (1), (2) and the choice of $\bar{a}_{i,0}$. In particular, $\mathrm{LT}_R(f) \succeq \mathrm{LT}_R(a_i f_i)$. Thus, we obtain the first assertion.

We prove the rest of the assertion. We first prove the uniqueness of r. Let $f = \sum a_i f_i + r = \sum a_i' f_i + r'$ be expressions satisfying the conditions. Then, we have $r-r' \in I$, hence, $\mathrm{LT}_R(r-r) \in \mathrm{LT}_R(I)$. Therefore, $r-r'$ is divisible by $\mathrm{LT}_R(f_i)$ for some i. Since no nonzero term of $r-r'$ is divisible by any $\mathrm{LT}_R(f_i)$, we must have $r=r'$. We prove the equivalence $r=0 \Leftrightarrow f \in I$. We only have to prove the necessity. Since $r \in I$, we have $\mathrm{LT}_R(r) \in \mathrm{LT}_R(I)$. Hence, $\mathrm{LT}_R(r)$ is divisible by $\mathrm{LT}_R(f_i)$ for some i. Since all nonzero terms of r are divisible by $\underline{X}^{\deg_R(f_i)}$, we must have $r=0$. □

Definition 3.2.9. We call the above expression $f=\sum a_i f_i+r$ a standard expression (of f) and call r the remainder of f (with respect to $f_1,\dots,f_s$). Note that standard expressions are additive and compatible with scalar multiplications, that is, if $f=\sum_i a_i f_i+r$ and $g=\sum_i a_i' f_i+r'$ are standard expressions, then $f+g=\sum_i(a_i+a_i')f_i+r+r'$ is also a standard expression of $f+g$, and $\lambda f=\sum_i \lambda a_i f_i+\lambda r$ is a standard expression of λf for $\lambda \in R$ by formulas (1) and (2). The remainder of f depends only on the class $f \bmod I$ by Proposition 3.2.8 and the above additive property. Therefore, we may call r the remainder of $f \bmod I$.

As in the classical case, we have the following.

Lemma 3.2.10. *Let I be an ideal of $R\langle\underline{X}\rangle$ such that $R\langle\underline{X}\rangle/I$ is R-flat. Let $f_1,\dots,f_s \in I$ be a Gröbner basis of I. Let $f \in R\langle\underline{X}\rangle$ be a nonzero element. For $r \in R\langle\underline{X}\rangle$, the following are equivalent*:

(i) *r is the remainder of f.*

(ii) *$f-r \in I$ and no nonzero term of r is divisible by $\underline{X}^{\deg(f_i)}$ for all i.*

Proof. Since the assertion (i) ⇒ (ii) is trivial, we prove the converse. By applying the division algorithm to $f-r$, we have $f-r=\sum a_i f_i$ such that $\mathrm{LT}_R(f) \succeq \mathrm{LT}_R(a_i f_i)$ if $a_i f_i \neq 0$. This means exactly that r is the remainder of f. □

Corollary 3.2.11. *Let the notation be as in Lemma 3.2.10. We regard $f_1 \bmod s_1,\dots,f_s \bmod s_1$ as a Gröbner basis of I_1. For $f \in R\langle\underline{X}\rangle$ with $s_1 \nmid f$, denote by r and r' the remainders of f and $f \bmod s_1$, respectively. Then, we have $r \bmod s_1 \equiv r'$.*

Finally, we give a concrete example of a Gröbner basis, which will appear in Section 3.5.

Proposition 3.2.12. *Let $I=(f_1,\dots,f_s) \subset R\langle\underline{X}\rangle$ be an ideal. Assume that there exists relatively prime monic monomials $T_1,\dots,T_s$ and units $u_1,\dots,u_s \in R^{\times}$ such that $\mathrm{LT}_R(f_i)=u_iT_i$ for $1 \le i \le s$. Then, we have the following*:

(i) *$R\langle\underline{X}\rangle/I$ is R-flat.*

(ii) *$f_1,\dots,f_s$ is a Gröbner basis of I.*

(iii) *$f_1,\dots,f_s$ is a regular sequence in $R\langle\underline{X}\rangle$.*

Proof. We may assume that $\mathrm{LT}_R(f_1), \ldots, \mathrm{LT}_R(f_s)$ are relatively prime monic monomials by replacing f_i by f_i/u_i. We first note that in the case of $d = 0$, the assertion is basic, since condition (i) is automatically satisfied. Condition (ii) directly follows from [Cox et al. 1997, §2.9, Theorem 3 and Proposition 4]. Condition (iii) follows from [Eisenbud 1995, Proposition 15.15] with $F = S = R[\underline{X}]$ and $M = 0$, $h_j = f_j$, where F, S and M, h_j's are as in the reference. We prove the assertion by induction on s. In the case of $s = 1$, we have only to prove condition (i). We proceed by induction on d. By the local criteria of flatness and the induction hypothesis, we only have to prove that the multiplication by s_1 on $R\langle\underline{X}\rangle/I$ is injective. Let $f \in R\langle\underline{X}\rangle$ such that $s_1 f \in I$. Write $s_1 f = f_1 h$ for some $h \in R\langle\underline{X}\rangle$. By taking v_{s_1}, we have $s_1 \mid h$ since $s_1 \nmid f_1$. This implies $f_1 \mid f$, i.e., $f \in I$. This finishes the case $s = 1$. We assume that the assertion is true when the cardinality of f_i's is $< s$. We proceed by induction on d. The case $d = 0$ can be done as above. Assume that the assertion is true for dimension $< d$. For $h \in R\langle X\rangle$, denote by $\bar{h}$ its image in $R_1\langle\underline{X}\rangle$. By assumption, $s_1 \nmid f_i$ for all i, hence, we can apply the induction hypothesis to $\bar{f}_1, \ldots, \bar{f}_s \in I_1 := (\bar{f}_1, \ldots, \bar{f}_s) \subset R\langle\underline{X}\rangle$ by formula (3). Hence, $R_1\langle\underline{X}\rangle/I_1$ is R_1-flat, $\bar{f}_1, \ldots, \bar{f}_s$ are a Gröbner basis of I_1, and $\bar{f}_1, \ldots, \bar{f}_s$ is a regular sequence in $R_1\langle\underline{X}\rangle$. Condition (ii) follows from Lemma 3.2.6. Next, we check condition (i). By the local criteria of flatness, we only have to prove that multiplication by s_1 on $R\langle\underline{X}\rangle/I$ is injective. It suffices to prove $I \cap s_1 \cdot R\langle\underline{X}\rangle \subset s_1 I$. Denote by $C_\bullet$ and $\bar{C}_\bullet$ Koszul complexes for $\{f_1, \ldots, f_s\}$ and $\{\bar{f}_1, \ldots, \bar{f}_s\}$ [Matsumura 1980, 18.D]. Then, we have $\bar{C}_i = C_i/s_1 C_i$ for $i \geq 1$ by definition, and $\bar{C}_\bullet$ is exact since $\bar{f}_1, \ldots, \bar{f}_s$ is a regular sequence. We also have a morphism of complexes $C_\bullet \to \bar{C}_\bullet$, whose first few terms are

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & C_2 & \xrightarrow{d_2} & C_1 & \xrightarrow{d_1} & I & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & \bar{C}_2 & \xrightarrow{\bar{d}_2} & \bar{C}_1 & \xrightarrow{\bar{d}_1} & I_1 & \longrightarrow & 0 \end{array}$$

Let $f \in I \cap s_1 \cdot R\langle\underline{X}\rangle$. Then, there exists $a \in C_1$ such that $d_1(a) = f$. Since $\bar{d}_1(\bar{a}) \equiv 0 \bmod s_1$, there exists $\bar{b} \in C_2$ with $\bar{d}_2(\bar{b}) = \bar{a}$. Let $b \in C_2$ be a lift of $\bar{b}$. Then, there exists $a' \in C_1$ such that $a - d_2(b) = s_1 a'$. Therefore, we have $f = d_1(a - d_2(b)) = s_1 d_1(a') \in s_1 I$. Thus, condition (i) is proved. Finally, we check condition (iii). We only have to prove that if $f_i f \in (f_1, \ldots, f_{i-1})$ for some $f \in R\langle\underline{X}\rangle$ and $1 \leq i \leq s$, then we have $f \in (f_1, \ldots, f_{i-1})$. Note that $f_1, \ldots, f_{i-1}$ is a Gröbner basis of $(f_1, \ldots, f_{i-1})$ by the induction hypothesis. Let $f = \sum_{1\leq j<i} a_j f_j + r$ be a standard expression of f with respect to $f_1, \ldots, f_{i-1}$. It suffices to prove that $r = 0$. We suppose the contrary and deduce a contradiction. No nonzero term of r is divisible by $\mathrm{LT}_R(f_j)$ for any $1 \leq j < i$; in particular, we have $\mathrm{LT}_R(f_j) \nmid \mathrm{LT}_R(r)$. By assumption, $f_i f = f_i\big(\sum_{1\leq j<i} a_j f_j\big) + f_i r \in (f_1, \ldots, f_{i-1})$. We therefore have

$f_i r \in (f_1, \dots, f_{i-1})$. In particular, there exists $1 \le j < i$ with $\mathrm{LT}_R(f_j) \mid \mathrm{LT}_R(f_i r)$. Since $\mathrm{LT}_R(f_i)$ and $\mathrm{LT}_R(f_j)$ are relatively prime, we have $\mathrm{LT}_R(f_j) \mid \mathrm{LT}_R(r)$, which is a contradiction. Thus, we obtain assertion (iii). □

A remarkable feature of the remainder is the compatibility with quotient norms:

Lemma 3.2.13. *Let I be an ideal of $R\langle \underline{X}\rangle$ such that $R\langle \underline{X}\rangle/I$ is R-flat. Let $f_1, \dots, f_s \in I$ be a Gröbner basis of I. Let $|\cdot| : R \to \mathbb{R}_{\ge 0}$ be any nonarchimedean norm satisfying $|R| \le 1$ and $|\mathfrak{m}_R| < 1$. We extend $|\cdot|$ to a norm on $R\langle \underline{X}\rangle$ by $|\sum_{\underline{n}} a_{\underline{n}} \underline{X}^{\underline{n}}| := \sup_{\underline{n}} |a_{\underline{n}}| < \infty$. If we denote by $|\cdot|_{\mathrm{qt}} : R\langle \underline{X}\rangle/I \to \mathbb{R}_{\ge 0}$ the quotient norm of $|\cdot|$, then the remainder r of $f \in R\langle \underline{X}\rangle$ achieves the quotient norm of f mod I, i.e.,*

$$|r| = |f \bmod I|_{\mathrm{qt}}.$$

Proof. Let $f = \sum \lambda_{\underline{n}} \underline{X}^{\underline{n}}$ with $\lambda_{\underline{n}} \in R$. Let $\underline{X}^{\underline{n}} = \sum a_{\underline{n},i} f_i + r_{\underline{n}}$ be a standard expression of $\underline{X}^{\underline{n}}$. Let $a_i := \sum_{\underline{n}} \lambda_{\underline{n}} a_{\underline{n},i}$ and $r := \sum_{\underline{n}} \lambda_{\underline{n}} r_{\underline{n}}$, which converge since $\lambda_{\underline{n}} \to 0$ as $|\underline{n}| \to \infty$. Then, $f = \sum a_i f_i + r$ is a standard expression of f by Lemma 3.2.10. We have $|a_i f_i| \le |a_i| \le \sup_{\underline{n}} |\lambda_{\underline{n}} a_{\underline{n},i}| \le \sup_{\underline{n}} |\lambda_{\underline{n}}| = |f|$. Hence, we have $|r| \le |f|$. Since the remainder depends only on the class f mod I, we have

$$|f \bmod I|_{\mathrm{qt}} = \inf_{g \in I} |f + g| \ge |r| \ge |f \bmod I|_{\mathrm{qt}},$$

which implies the assertion. □

3.3. ***Gröbner basis argument over annuli.*** In this subsection, we will give an analogue of a Gröbner basis argument over rings of overconvergent power series. We use the notations of Section 3.1 and 3.2 and further use the following notation.

Notation 3.3.1. Let $\mathcal{O}$, R^+, and R be as in Notation 3.1.4. Fix $\{p, S\}$ as a regular system of parameters of R^+. Let $I \subset R^+\langle \underline{X}\rangle$ be an ideal such that $R^+\langle \underline{X}\rangle/I$ is R^+-flat. For $r \in \mathbb{Q}_{>0}$, we give $R^{\dagger,r}$ the topology defined by the norm $|\cdot|_r$, and write

$$A := R^+\langle \underline{X}\rangle/I, \quad I^{\dagger,r} := I \otimes_{R^+\langle \underline{X}\rangle} R^{\dagger,r}\langle \underline{X}\rangle, \quad A^{\dagger,r} := A \otimes_{R\langle \underline{X}\rangle} R^{\dagger,r}\langle \underline{X}\rangle.$$

(When $I = 0$, $R^{\dagger,r}\langle \underline{X}\rangle$ is denoted by $R\langle \underline{X}\rangle^{\dagger,r}$ in this notation. However, we use this notation for simplicity.) Since $R^+\langle \underline{X}\rangle \to R^{\dagger,r}\langle \underline{X}\rangle$ is flat (Lemma 3.1.7), we may identify $I^{\dagger,r}$ and $A^{\dagger,r}$ with $I \cdot R^{\dagger,r}\langle \underline{X}\rangle$ and $R^{\dagger,r}\langle \underline{X}\rangle/I^{\dagger,r}$. Since R^+ is an integral domain, A and hence, $A^{\dagger,r}$ are R^+-torsion free by flatness.

Let $|\cdot|_{r,\mathrm{qt}} : A^{\dagger,r} \to \mathbb{R}_{\ge 0}$ be the quotient norm of $|\cdot|_r$. Note that $A^{\dagger,r}$ is complete with respect to $|\cdot|_{r,\mathrm{qt}}$ by [Bosch et al. 1984, Section 1.1.7, Proposition 3].

Lemma 3.3.2 (cf. [Xiao 2010, Lemma 1.1.22]). *Let $f_1, \dots, f_s \in I$ be a Gröbner basis of I. For $f \in R^{\dagger,r}\langle \underline{X}\rangle$, there exists a unique $\mathfrak{r} \in R^{\dagger,r}\langle \underline{X}\rangle$ such that $f - \mathfrak{r} \in I^{\dagger,r}$ and no nonzero term of $\mathfrak{r}$ is divisible by $\underline{X}^{\deg_R(f_i)}$. Moreover, we have $|\mathfrak{r}|_{r'} = |f|_{r',\mathrm{qt}}$ for $r' \in \mathbb{Q} \cap (0, r]$, and $\mathfrak{r} = 0$ if and only if $f \in I^{\dagger,r}$. We call $\mathfrak{r}$ the remainder of f (with respect to $f_1, \dots, f_s$).*

Proof. We first construct $\mathfrak{r}$. Let $f=\sum_{\underline{n}}\lambda_{\underline{n}}\underline{X}^{\underline{n}}\in R^{\dagger,r}\langle\underline{X}\rangle$ with $\lambda_{\underline{n}}\in R^{\dagger,r}$. Let

$$\underline{X}^{\underline{n}}=\sum_i a_{\underline{n},i}f_i+r_{\underline{n}}$$

be the standard expression of $\underline{X}^{\underline{n}}$ in $R^+\langle\underline{X}\rangle$ with respect to $f_1,\dots,f_s$. Since $\lambda_{\underline{n}}\to 0$ as $|\underline{n}|\to\infty$, the series

$$a_i:=\sum_{\underline{n}}\lambda_{\underline{n}}a_{\underline{n},i},\qquad \mathfrak{r}:=\sum_{\underline{n}}\lambda_{\underline{n}}r_{\underline{n}}$$

converge in $R^{\dagger,r}\langle\underline{X}\rangle$ with respect to the topology defined by $|\cdot|_r$. Then, we have

$$|\mathfrak{r}|_{r'}\leq\sup_{\underline{n}}|\lambda_{\underline{n}}r_{\underline{n}}|_{r'}\leq\sup_{\underline{n}}|\lambda_{\underline{n}}|_{r'}=|f|_{r'}. \tag{4}$$

Obviously, no nonzero term of $\mathfrak{r}$ is divisible by any $\underline{X}^{\deg_R(f_i)}$ and we have $f-\mathfrak{r}=\sum_i a_i f_i\in I^{\dagger,r}$.

We prove the uniqueness of $\mathfrak{r}$. We suppose the contrary and deduce a contradiction. Let $\mathfrak{r}'\in R^{\dagger,r}\langle\underline{X}\rangle$ be an element such that $f-\mathfrak{r}'\in I^{\dagger,r}$ and such that no nonzero term of $\mathfrak{r}'$ is divisible by any $\underline{X}^{\deg_R(f_i)}$. We choose $m\in\mathbb{N}$ such that $\delta:=S^m(\mathfrak{r}-\mathfrak{r}')$ belongs to $I_0^{\dagger,r}:=I\otimes_{R^+\langle\underline{X}\rangle}R_0^{\dagger,r}\langle\underline{X}\rangle$. If we write $\delta=p^n\delta'$ such that $\delta'\in R_0^{\dagger,r}\langle\underline{X}\rangle$ is not divisible by p in $R_0^{\dagger,r}\langle\underline{X}\rangle$, then we have $\delta'\in I_0^{\dagger,r}$ by Lemma 3.1.3. We may identify $I_0^{\dagger,r}/pI_0^{\dagger,r}$ with I/pI by Lemma 3.1.10. We write $\bar{\delta}':=\delta'\bmod pI_0^{\dagger,r}\in I/pI$. We also write $R_1^+:=R^+/pR^+$, which is a complete discrete valuation ring with uniformizer S. Then, no nonzero term of $\bar{\delta}'$ is divisible by $\underline{X}^{\deg_{R_1^+}(f_i \bmod p)}$. Hence, $\bar{\delta}'$ is the remainder of 0 with respect to $f_1\bmod p,\dots,f_s\bmod p$ in $R_1\langle\underline{X}\rangle$. By Lemma 3.2.10, $\bar{\delta}'=0$, i.e., $\delta'\in\operatorname{mod}pI_0^{\dagger,r}$, contradicting $p\nmid\delta'$.

We prove $f=I^{\dagger,r}\Leftrightarrow\mathfrak{r}=0$. If $f\in I^{\dagger,r}$, then 0 satisfies the required property for the remainder, and hence $\mathfrak{r}=0$ by uniqueness. If $\mathfrak{r}=0$, then $f\in I^{\dagger,r}$ by definition.

We prove $|\mathfrak{r}|_{r'}=|f\bmod I^{\dagger,r}|_{r',\mathrm{qt}}$. Let $\alpha\in I^{\dagger,r}$. Since $\mathfrak{r}$ satisfies the required condition for the remainder of $f+\alpha$, the remainder of $f+\alpha$ is equal to $\mathfrak{r}$ by uniqueness. In particular, the remainder depends only on the of class $f\bmod I^{\dagger,r}$. Hence, the assertion follows from

$$|f\bmod I^{\dagger,r}|_{r',\mathrm{qt}}=\inf_{\alpha\in I^{\dagger,r}}|\mathfrak{r}+\alpha|_{r'}\geq|\mathfrak{r}|_{r'}\geq|f\bmod I^{\dagger,r}|_{r',\mathrm{qt}},$$

where the first equality follows from (4) and the second inequality follows by definition. □

The following is an immediate consequence of the above lemma.

Lemma 3.3.3. *Let $f_1,\dots,f_s$ be a Gröbner basis of I. Let $f,g\in R^{\dagger,r}\langle\underline{X}\rangle$ and let $\mathfrak{r},\mathfrak{r}'$ be their remainders with respect to $f_1,\dots,f_s$. Then, we have the following*:

(i) *The remainder of $f+g$ is equal to $\mathfrak{r}+\mathfrak{r}'$.*

(ii) *The remainder* $\mathfrak{r}$ *depends only on* f mod $I^{\dagger,r}$. *One may call the remainder of* f *the remainder of* f mod $I^{\dagger,r}$.

(iii) *For* $\lambda \in R^{\dagger,r}$, *the remainder of* λf *is equal to* $\lambda\mathfrak{r}$. *Moreover, if* f mod $I^{\dagger,r}$ *is divisible by* $\lambda \in R^{\dagger,r}$, *then* $\mathfrak{r}$ *is also divisible by* λ.

Corollary 3.3.4. *Let* $\mathfrak{a} \subsetneq R^{\dagger,r}$ *be a principal ideal. Then, we have* $\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n \cdot A^{\dagger,r} = 0$.

Proof. Fix a Gröbner basis $f_1, \dots, f_s$ of I. Let $f \in \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n \cdot A^{\dagger,r}$ and let $\mathfrak{r}$ be the remainder of f with respect to $f_1, \dots, f_s$. By Lemma 3.3.3(iii) and the assumption, we have $\mathfrak{r} \in \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = 0$. □

Remark 3.3.5. Using [Kedlaya 2005, Proposition 2.6.5], one can prove that $R^{\dagger,r}$ is a principal ideal domain. We do not use this fact in this paper.

3.4. ***Continuity of connected components for families of affinoids.*** In this subsection, we will apply the previous results to prove a continuity of connected components of fibers of families of affinoids.

Lemma 3.4.1. *Let* $f : R \to S$ *be a morphism of Noetherian rings and let* $\mathrm{Idem}(T)$ *denote the set of idempotents of a ring* T. *If the canonical map* $f_* : \mathrm{Idem}(R) \to \mathrm{Idem}(S)$ *is surjective and* $f_*^{-1}(\{0\}) = \{0\}$, *then* $f^* : \pi_0^{\mathrm{Zar}}(S) \to \pi_0^{\mathrm{Zar}}(R)$ *is bijective.*

Proof. We first recall a basic fact on commutative algebras. For a ring A, finite partitions of $\mathrm{Spec}(A)$ into nonempty open subspaces as a topological space correspond to finite sets of nonzero idempotents $e_1, \dots, e_n$ of A such that $\sum_i e_i = 1$ and $e_i e_j = 0$ for all $i \neq j$. Precisely, $e_1, \dots, e_n$ correspond to $\mathrm{Spec}(Ae_1) \sqcup \cdots \sqcup \mathrm{Spec}(Ae_n)$ (for details, see [Bourbaki 1998, Proposition 15, II, §4, no 3]).

Decompose $\mathrm{Spec}(R)$ into connected components and choose the corresponding idempotents $e_1, \dots, e_n$ as above. Since the nonzero idempotents $f(e_1), \dots, f(e_n)$ satisfy $\sum_{1\leq i\leq n} f(e_i) = 1$ and $f(e_i)f(e_j) = 0$ for $i \neq j$, we obtain a finite partition $\mathrm{Spec}(S) = \mathrm{Spec}(Sf(e_1)) \sqcup \cdots \sqcup \mathrm{Spec}(Sf(e_n))$. Hence, we only have to prove that $\mathrm{Spec}(Sf(e_i))$ is connected for all $1 \leq i \leq n$. Let $e' \in \mathrm{Idem}(Sf(e_i))$. By regarding e' as an element of $\mathrm{Idem}(S)$, we obtain an $x \in \mathrm{Idem}(R)$ such that $e' = f(x)$. Since $xe_i \in \mathrm{Idem}(Re_i)$ and $\mathrm{Spec}(Re_i)$ is connected by definition, we either have $xe_i = 0$ or $xe_i = e_i$. Since we have $e' = e'f(e_i) = f(x)f(e_i) = f(xe_i)$, we either have $e' = 0$ or $e' = f(e_i)$. Hence, $Sf(e_i)$ has only trivial idempotents, which implies the assertion. □

Notation 3.4.2. In the remainder of this subsection, we let the notation be as in Notation 3.3.1 and Definition 3.1.8, unless otherwise stated. For an Eisenstein prime ideal $\mathfrak{p}$ of R^+, we fix a norm $|\cdot|_{\mathfrak{p}}$ of the complete discrete valuation field $\kappa(\mathfrak{p})$ and write

$$A_{\kappa(\mathfrak{p})} := (A/\mathfrak{p}A)[S^{-1}].$$

We identify $R^+\langle\underline{X}\rangle/\mathfrak{p}R^+\langle\underline{X}\rangle$ with $\mathcal{O}_{\kappa(\mathfrak{p})}\langle\underline{X}\rangle$, and denote the Gauss norm on $\kappa(\mathfrak{p})\langle\underline{X}\rangle$ by $|\cdot|_{\mathfrak{p}}$. We also denote the quotient (resp. spectral) norm of $|\cdot|_{\mathfrak{p}}$ on $A/\mathfrak{p}A$ and $A_{\kappa(\mathfrak{p})}$ by $|\cdot|_{\mathfrak{p},\mathrm{qt}}$ (resp. $|\cdot|_{\mathfrak{p},\mathrm{sp}}$). For simplicity, we also write $|f \bmod I/\mathfrak{p}I|_{\mathfrak{p},\mathrm{qt}}$ (resp. $|f \bmod I/\mathfrak{p}I|_{\mathfrak{p},\mathrm{qt}}$) by $|f|_{\mathfrak{p},\mathrm{qt}}$ (resp. $|f|_{\mathfrak{p},\mathrm{qt}}$) for $f\in\kappa(\mathfrak{p})\langle\underline{X}\rangle$.

For $f=\sum_{\underline{n}} a_{\underline{n}}\underline{X}^{\underline{n}}\in\mathcal{O}_{\kappa(\mathfrak{p})}\langle\underline{X}\rangle$ with nonzero $a_{\underline{n}}\in\mathcal{O}_{\kappa(\mathfrak{p})}$, let $\tilde{a}_{\underline{n}}\in R^+$ be a lift of $a_{\underline{n}}$. Then, $\tilde{f}:=\sum_{\underline{n}}\tilde{a}_{\underline{n}}\underline{X}^{\underline{n}}\in R^+\langle\underline{X}\rangle$ is called a minimal lift of f.

We may apply Construction 3.2.2 to $R=\mathcal{O}_{\kappa(\mathfrak{p})}$ and $s_1=\pi_{\mathfrak{p}}$ with the same monomial order $\succeq$ for $\mathcal{O}[\![S]\!]$. Let $f_1,\dots,f_s$ be a Gröbner basis of I. Then, the images of f_i's in $R^+/\mathfrak{m}_{R^+}[\underline{X}]$ form a Gröbner basis by Lemma 3.2.6. Hence, the images of f_i's in $\mathcal{O}_{\kappa(\mathfrak{p})}\langle\underline{X}\rangle$ form a Gröbner basis of $I/\mathfrak{p}I$ by Lemma 3.2.6 again. In particular, if $\mathfrak{r}$ is the remainder of $f\in R^+\langle\underline{X}\rangle$ with respect to $f_1,\dots,f_s$, then the image of $\mathfrak{r}$ in $\mathcal{O}_{\kappa(\mathfrak{p})}\langle\underline{X}\rangle$ is the remainder of $f \bmod \mathfrak{p}$ with respect to $f_1 \bmod \mathfrak{p},\dots,f_s \bmod \mathfrak{p}$.

By using our Gröbner basis argument, Lemma 3.1.9 can be converted into the following form:

Lemma 3.4.3. *Let $c\in\mathbb{N}$ and let $\mathfrak{p},\mathfrak{q}$ be Eisenstein prime ideals of R^+ such that $c<\inf(\deg\mathfrak{p},\deg\mathfrak{q})$. Assume that for $n\in\mathbb{N}$, we have*

$$|f^n|_{\mathfrak{p},\mathrm{qt}}\geq|\pi_{\mathfrak{p}}|_{\mathfrak{p}}^c|f|_{\mathfrak{p},\mathrm{qt}}^n,\quad\forall f\in A_{\kappa(\mathfrak{p})}.$$

Then, we have

$$|f^n|_{\mathfrak{q},\mathrm{qt}}\geq|\pi_{\mathfrak{q}}|_{\mathfrak{q}}^c|f|_{\mathfrak{q},\mathrm{qt}}^n,\quad\forall f\in A_{\kappa(\mathfrak{q})}.$$

Proof. We fix a Gröbner basis $f_1,\dots,f_s$ of I. We may regard the $f_i \bmod \mathfrak{p}$'s (resp. $f_i \bmod \mathfrak{q}$'s) as a Gröbner basis of $I/\mathfrak{p}I$ (resp. $I/\mathfrak{q}I$). To prove the assertion, we may assume that $f\in A/\mathfrak{q}A$. Let $\mathfrak{r}\in\mathcal{O}_{\kappa(\mathfrak{q})}\langle\underline{X}\rangle$ be the remainder of f. We have $|f|_{\mathfrak{q},\mathrm{qt}}=|\mathfrak{r}|_{\mathfrak{q}}=|\pi_{\mathfrak{q}}|_{\mathfrak{q}}^m$ for some $m\in\mathbb{N}$. To prove the assertion, we may assume $|f|_{\mathfrak{q},\mathrm{qt}}=|\mathfrak{r}|_{\mathfrak{q}}=1$ by replacing $f,\mathfrak{r}$ by $f/\pi_{\mathfrak{q}}^m,\mathfrak{r}/\pi_{\mathfrak{q}}^m$.

Let $\tilde{\mathfrak{r}}\in R^+\langle\underline{X}\rangle$ be a minimal lift of $\mathfrak{r}$ and let $\tilde{f}\in A$ denote the image of $\tilde{\mathfrak{r}}$. Denote by $\mathfrak{r}_n\in R^+\langle\underline{X}\rangle$ the remainder of $\tilde{f}^n$. Then, we have

$$|\mathfrak{r}_n \bmod \mathfrak{p}|_{\mathfrak{p}}=|\tilde{f}^n \bmod \mathfrak{p}|_{\mathfrak{p},\mathrm{qt}}\geq|\pi_{\mathfrak{p}}|_{\mathfrak{p}}^c|\tilde{f} \bmod \mathfrak{p}|_{\mathfrak{p},\mathrm{qt}}^n$$

by Lemma 3.2.13 and by assumption. Since $|\mathfrak{r}|_{\mathfrak{q}}=1$, the coefficient of some $\underline{X}^{\underline{n}}$ in $\mathfrak{r}$ belongs to $\mathcal{O}_{\kappa(\mathfrak{p})}^{\times}$. Therefore, the coefficient of $\underline{X}^{\underline{n}}$ in $\tilde{\mathfrak{r}}$, hence, in $\tilde{\mathfrak{r}} \bmod \mathfrak{p}$ is a unit. Therefore, we have

$$|\tilde{f} \bmod \mathfrak{p}|_{\mathfrak{p},\mathrm{qt}}=|\tilde{\mathfrak{r}} \bmod \mathfrak{p}|_{\mathfrak{p}}=1,$$

hence, $|\mathfrak{r}_n \bmod \mathfrak{p}|_{\mathfrak{p}}\geq|\pi_{\mathfrak{p}}|_{\mathfrak{p}}^c$. By applying Lemma 3.1.9 to the coefficient λ of $\mathfrak{r}_n$ that satisfies $|\lambda \bmod \mathfrak{p}|_{\mathfrak{p}}\geq|\pi_{\mathfrak{p}}|^c$, we obtain $|\mathfrak{r}_n \bmod \mathfrak{q}|_{\mathfrak{q}}\geq|\pi_{\mathfrak{q}}|_{\mathfrak{q}}^c$. Since $\mathfrak{r}_n \bmod \mathfrak{q}$ is the remainder of f^n, we have $|f^n|_{\mathfrak{q},\mathrm{qt}}=|\mathfrak{r}_n \bmod \mathfrak{q}|_{\mathfrak{q}}\geq|\pi_{\mathfrak{q}}|_{\mathfrak{q}}^c$ by Lemma 3.2.13, which implies the assertion. □

The following lemma can be considered as an analogue of Hensel's lemma.

Lemma 3.4.4 (cf. [Xiao 2010, Theorem 1.2.11]). *Assume that there exists $c \in \mathbb{R}_{\geq 0}$ such that*

$$|\cdot|_{\mathfrak{p},\mathrm{sp}} \geq |\pi_{\mathfrak{p}}|^c |\cdot|_{\mathfrak{p},\mathrm{qt}} \ \text{ on } A_{\kappa(\mathfrak{p})}.$$

Then, for all $\mathfrak{r} \in \mathbb{Q}_{>0} \cap [1/\deg \mathfrak{p}, 1/2c)$, *there exists a canonical bijection*

$$\pi_0^{\mathrm{Zar}}(A_{\kappa(\mathfrak{p})}) \to \pi_0^{\mathrm{Zar}}(A^{\dagger,r}).$$

Proof. Replacing c by $\lfloor c \rfloor$, we may assume $c \in \mathbb{N}$. Denote by α the canonical map $\mathrm{Idem}(A^{\dagger,r}) \to \mathrm{Idem}(A_{\kappa(\mathfrak{p})})$. By Lemma 3.4.1, we only have to prove that we have $\alpha^{-1}(\{0\}) = \{0\}$ and that α is surjective. Let $e \in \mathrm{Idem}(A^{\dagger,r})$ satisfy $\alpha(e) = 0$. Then, we have $e \in \mathfrak{p} \cdot A^{\dagger,r}$. Since $e = e^n$, we have $e \in \bigcap_{n\in\mathbb{N}} \mathfrak{p}^n \cdot A^{\dagger,r} = 0$ by Corollary 3.3.4, which implies the first assertion. We will prove the surjectivity of α. Let $e \in \mathrm{Idem}(A_{\kappa(\mathfrak{p})})$. Since $|e|_{\mathfrak{p},\mathrm{sp}} = 1 \geq |\pi_{\mathfrak{p}}|_{\mathfrak{p}}^c |e|_{\mathfrak{p},\mathrm{qt}}$ by assumption, we have $e \in \pi_{\mathfrak{p}}^{-c} A/\mathfrak{p}A$. Hence, we can choose $e' \in A$ such that $e \equiv S^{-c}e' \bmod \mathfrak{p}$. Put $h_0 := S^{-2c}(e'^2 - S^c e') \in A[S^{-1}]$. Since

$$e'^2 - S^c e' \equiv (S^c e)^2 - S^c \cdot S^c e \equiv S^{2c}(e^2 - e) \equiv 0 \bmod \mathfrak{p},$$

we have $h_0 \in \mathfrak{p}S^{-2c} \cdot A$. Since $\mathfrak{p} \subset (p, S^e)R^+$, we obtain

$$|h_0|_{r,\mathrm{qt}} \leq \sup(|S|^e, |p|)|S|^{-2c} = |p^{1-2cr}| < 1.$$

We define sequences $\{f_n\}$ and $\{h_n\}$ in $A[S^{-1}]$ inductively as follows. Put $f_0 := S^{-c}e'$ and let h_0 be as above. For $n \geq 0$, we put

$$f_{n+1} := f_n + h_n - 2h_n f_n, \quad h_{n+1} := f_{n+1}^2 - f_{n+1} \in A[S^{-1}].$$

Note that for $n \in \mathbb{N}$, we have

$$f_{n+1} = -f_n^2(2f_n - 3), \quad f_{n+1} - 1 = -(f_n - 1)^2(2f_n + 1),$$

hence, $h_{n+1} = f_n^2(f_n - 1)^2(4f_n^2 - 4h_n - 3) = h_n^2(4h_n - 3)$. Then, we have

$$|h_{n+1}|_{r,\mathrm{qt}} \leq |h_n|_{r,\mathrm{qt}}^2 \sup(|h_n|_{r,\mathrm{qt}}, 1).$$

Therefore, by induction on n, we have $|h_n|_r < 1$, hence, $|h_{n+1}|_r \leq |h_n|_r^3$. In particular, we have $|h_n|_r \to 0$ for $n \to \infty$. We also have

$$\sup(|f_{n+1}|_{r,\mathrm{qt}}, 1) \leq \sup(|f_n|_{r,\mathrm{qt}}, |h_n|_{r,\mathrm{qt}}, |h_n|_{r,\mathrm{qt}}|f_n|_{r,\mathrm{qt}}, 1) = \sup(|f_n|_{r,\mathrm{qt}}, 1),$$

hence, $\sup(|f_n|_{r,\mathrm{qt}}, 1) \leq \sup(|f_0|_{r,\mathrm{qt}}, 1)$. Therefore, we have

$$|f_{n+1} - f_n|_{r,\mathrm{qt}} = |h_n(1-2f_n)|_{r,\mathrm{qt}} \leq |h_n|_{r,\mathrm{qt}} \sup(|f_n|_{r,\mathrm{qt}}, 1) \leq |h_n|_{r,\mathrm{qt}} \sup(|f_0|_{r,\mathrm{qt}}, 1).$$

In particular, $\{f_n\}_n$ is a Cauchy sequence in $A^{\dagger,r}$ with respect to $|\cdot|_{r,\mathrm{qt}}$. The element $f := \lim_{n\to\infty} f_n$ satisfies $f^2 - f = \lim_{n\to\infty} h_n = 0$ and is an idempotent of $A^{\dagger,r}$. Since we have $h_n \in \mathfrak{p} \cdot A^{\dagger,r}$ by induction on n, $f \equiv f_0 \equiv e \bmod \mathfrak{p}$, i.e., $\alpha(f) = e$. □

Proposition 3.4.5 (Continuity of connected components). *Let $A_{\kappa(p)}$ be reduced.*

(i) *There exists $c \in \mathbb{R}_{\geq 0}$ such that*

$$|\cdot|_{(p),\mathrm{sp}} \geq |S|_{(p)}^{c}\, |\cdot|_{(p),\mathrm{qt}}$$

on $A_{\kappa(p)}$. We fix such c in the following.

(ii) *Let $n \in \mathbb{N}_{\geq 2}$ and $\mathfrak{p}$ an Eisenstein prime ideal of R^+ with* $\deg \mathfrak{p} > nc$. *Then*:

$$|\cdot|_{\mathfrak{p},\mathrm{sp}} \geq |\pi_{\mathfrak{p}}|_{\mathfrak{p}}^{\frac{nc}{n-1}}\, |\cdot|_{\mathfrak{p},\mathrm{qt}} \quad \text{on } A_{\kappa(\mathfrak{p})}.$$

(iii) *Let $\mathfrak{p}$ be an Eisenstein prime ideal of R^+ such that* $\deg \mathfrak{p} > 3c$. *Then*, *for $r \in \mathbb{Q}_{>0} \cap [1/\deg \mathfrak{p}, \frac{1}{2}c)$*, *there exists a canonical bijection*

$$\pi_0^{\mathrm{Zar}}(A_{\kappa(\mathfrak{p})}) \to \pi_0^{\mathrm{Zar}}(A^{\dagger,r}).$$

In particular, *we have*

$$\#\pi_0(A_{\kappa(\mathfrak{p})}) = \#\pi_0(A_{\kappa(p)}) = \#\pi_0^{\mathrm{Zar}}(A^{\dagger,r}).$$

Proof.

(i) By assumption, $|\cdot|_{(p),\mathrm{sp}}$ is equivalent to $|\cdot|_{(p),\mathrm{qt}}$ on $A_{\kappa(p)}$. Hence, there exists $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_{\mathrm{sp}} \geq \lambda |\cdot|_{\mathrm{qt}}$. From $|1|_{\mathrm{sp}} = |1|_{\mathrm{qt}} = 1$, we deduce $\lambda \leq 1$. Hence, $c = \log_{|S|} \lambda \geq 0$ satisfies the condition.

(ii) By (i), we have

$$|f^n|_{(p),\mathrm{qt}} \geq |f^n|_{(p),\mathrm{sp}} = |f|_{(p),\mathrm{sp}}^{n} \geq |S|_{(p)}^{nc}\, |f|_{(p),\mathrm{qt}}^{n}, \quad \forall f \in A_{\kappa(p)}.$$

From Lemma 3.4.3, we obtain

$$|f^n|_{\mathfrak{p},\mathrm{qt}} \geq |\pi_{\mathfrak{p}}|_{\mathfrak{p}}^{nc}\, |f|_{\mathfrak{p},\mathrm{qt}}^{n}, \quad \forall f \in A_{\kappa(\mathfrak{p})}.$$

By using this inequality iteratively, we obtain

$$|f^{n^i}|_{\mathfrak{p},\mathrm{qt}} \geq |\pi_{\mathfrak{p}}|_{\mathfrak{p}}^{nc+n^2c+\cdots+n^ic}\, |f|_{\mathfrak{p},\mathrm{qt}}^{n^i} = |\pi_{\mathfrak{p}}|_{\mathfrak{p}}^{\frac{nc(n^i-1)}{n-1}}\, |f|_{\mathfrak{p},\mathrm{qt}}^{n^i}, \quad \forall f \in A_{\kappa(\mathfrak{p})}.$$

Hence, for all $f \in A_{\kappa(\mathfrak{p})}$, we have $|f|_{\mathfrak{p},\mathrm{sp}} = \inf_{i\in\mathbb{N}} |f^{n^i}|_{\mathfrak{p},\mathrm{qt}}^{1/n^i} \geq |\pi_{\mathfrak{p}}|_{\mathfrak{p}}^{nc/(n-1)}\, |f|_{\mathfrak{p},\mathrm{qt}}$.

(iii) When $\mathfrak{p} = (p)$, the assertion follows from (i) and Lemma 3.4.4. We consider the case $\mathfrak{p} \neq (p)$. By applying Lemma 3.4.4 to the inequality in (ii) with $n = 3$, we obtain the assertion for $r \in \mathbb{Q} \cap [1/\deg \mathfrak{p}, \frac{1}{3}c)$. For general $r \in \mathbb{Q} \cap [1/\deg \mathfrak{p}, \frac{1}{2}c)$, the assertion is reduced to the previous case by taking π_0^{Zar} of the commutative diagram

$$\begin{array}{ccccc}
A_{\kappa(p)} & \xleftarrow{\text{can.}} & A^{\dagger,r} & \xrightarrow{\text{can.}} & A_{\kappa(\mathfrak{p})} \\
\Big\| \text{id} & & \Big\downarrow \text{can.} & & \Big\| \text{id} \\
A_{\kappa(p)} & \xleftarrow{\text{can.}} & A^{\dagger,\frac{1}{\deg \mathfrak{p}}} & \xrightarrow{\text{can.}} & A_{\kappa(\mathfrak{p})}
\end{array}$$

□

Remark 3.4.6. In Theorem 1.2.11 of [Xiao 2010], Xiao proves $\#\pi_0(A_{\kappa(p)}) = \#\pi_0^{\mathrm{Zar}}(A^{\dagger,r})$ under the slightly mild Hypothesis 1.1.10 on A by a similar idea. To generalize Xiao's result for Eisenstein prime ideals, it seems needed to assume that A is flat over R.

To obtain a geometric version of this proposition, we need the following lifting lemma.

Lemma 3.4.7. *Let $\mathfrak{p}$ be an Eisenstein prime ideal of R^+ and $L/\kappa(\mathfrak{p})$ a finite extension. Let $\mathcal{O}'$ be a Cohen ring of k_L and put $R' := \mathcal{O}'[[T]]$. Then, there exists a finite flat morphism $\alpha : R^+ \to R'$ and an isomorphism $R'/\mathfrak{p}R' \cong \mathcal{O}_L$ of $R^+/\mathfrak{p}$-algebras. Moreover, for any Eisenstein prime $\mathfrak{q}$ of R^+, $\mathfrak{q}R'$ is again an Eisenstein prime ideal with degree $e_{L/\kappa(\mathfrak{p})}\deg(\mathfrak{q})$.*

Proof. We can define α similar to the definition of the homomorphism β in Construction 1.6.3: we fix an $\mathcal{O}'$-algebra structure on $\mathcal{O}_L$, and let $f : R' \to \mathcal{O}_L$ be the local $\mathcal{O}'$-algebra homomorphism, which maps T to a uniformizer π_L of L. Write $\pi_{\mathfrak{p}} = \pi_L^{e_{L/\kappa(\mathfrak{p})}}\bar{u}$ with $u \in \mathcal{O}_L^{\times}$. Since f is surjective by Nakayama's lemma, we can choose a lift $u \in (R')^{\times}$ of $\bar{u}$. Since R^+ is p-adically formally smooth over $\mathbb{Z}[S]$, we can define a morphism $\alpha : R^+ \to R'$, which maps S to $T^{e_{L/\kappa(\mathfrak{p})}}u$, by the lifting property.

We claim that $\mathfrak{p}R'$ is an Eisenstein prime. Let P be an Eisenstein polynomial of $\mathcal{O}[S]$ that generates $\mathfrak{p}$. We have $P \equiv T^{\deg(\mathfrak{p})e_{L/\kappa(\mathfrak{p})}}u \bmod pR'$ for some unit $u \in R'$. By the Weierstrass preparation theorem, there exists a distinguished polynomial $Q(T)$ of degree $\deg(\mathfrak{p})e_{L/\kappa(\mathfrak{p})}$ and a unit $U(T) \in R'$ such that $P = Q(T)U(T)$. By evaluating at $T = 0$, we see that $Q(0)$ is equal to p times a unit of $\mathcal{O}'$, which implies the claim. In particular, $R'/\mathfrak{p}R'$ is a discrete valuation ring. Hence, the canonical surjection $R'/\mathfrak{p}R' \to \mathcal{O}_L$ induced by f is an isomorphism. By Nakayama's lemma and the local criteria of flatness, α is finite flat. The second assertion also follows from the Weierstrass preparation theorem. □

The following is our main result of this subsection:

Proposition 3.4.8 (continuity of geometric connected components). *Assume that $A_{\kappa(p)}$ is geometrically reduced.*

(i) *If all connected components of $A_{\kappa(p)}$ are geometrically connected, then all connected components of $A_{\kappa(\mathfrak{p})}$ are also geometrically connected for all Eisenstein prime ideals $\mathfrak{p}$ of R^+ with* $\deg\mathfrak{p} \gg 0$.

(ii) *For all Eisenstein prime ideals $\mathfrak{p}$ of R^+ with* $\deg\mathfrak{p} \gg 0$, *we have*

$$\#\pi_0^{\mathrm{geom}}(A_{\kappa(\mathfrak{p})}) = \#\pi_0^{\mathrm{geom}}(A_{\kappa(p)}).$$

Proof.

(i) By assumption, there exists $c \in \mathbb{R}_{\geq 0}$ such that $|\cdot|_{(p),\mathrm{sp}} \geq |S|^c_{(p)} |\cdot|_{(p),\mathrm{qt}}$ on $A_{\kappa(p)} \otimes_{\kappa(p)} \kappa(p)^{\mathrm{alg}}$. We prove that all Eisenstein prime ideals $\mathfrak{p}$ of R^+ with $\deg(\mathfrak{p}) > 3c$ satisfy the condition. Let $L/\kappa(\mathfrak{p})$ be a finite extension. Let R' be as in Lemma 3.4.7. Since R' is finite flat over R^+, we have $R^+\langle \underline{X}\rangle \otimes_{R^+} R' \cong R'\langle \underline{X}\rangle$ and $I' := I \otimes_{R^+\langle \underline{X}\rangle} R'\langle \underline{X}\rangle \cong I \cdot R'\langle \underline{X}\rangle$. Hence, we can apply Proposition 3.4.5 to $R^+ = R'$, $I = I'$ and $A = A' := A \otimes_{R^+} R' \cong R'\langle \underline{X}\rangle / I'$. Note that $ce_{L/\kappa(\mathfrak{p})}$ can be taken as c in Proposition 3.4.5(i). Therefore, Proposition 3.4.5(iii) yields

$$\begin{aligned}\#\pi_0^{\mathrm{Zar}}(A_{\kappa(\mathfrak{p})} \otimes_{\kappa(\mathfrak{p})} L) = \#\pi_0^{\mathrm{Zar}}(A'_{\kappa(\mathfrak{p}R')}) = \pi_0^{\mathrm{Zar}}(A'_{\kappa(p)}) \\ = \#\pi_0^{\mathrm{Zar}}(A_{\kappa(p)}) = \#\pi_0^{\mathrm{Zar}}(A_{\kappa(\mathfrak{p})}),\end{aligned}$$

where the third equality follows from the assumption. Therefore, we have $\#\pi_0^{\mathrm{geom}}(A_{\kappa(\mathfrak{p})}) = \#\pi_0(A_{\kappa(\mathfrak{p})})$, which implies the assertion.

(ii) Let $L/\kappa(p)$ be a finite extension such that all connected components of $A_{\kappa(p)} \otimes_{\kappa(p)} L$ are geometrically connected. Let R' be a lifting of $\mathcal{O}_L$ as in Lemma 3.4.7 and A' as in the proof of (i). Part (i) and Proposition 3.4.5(iii) give the assertion. □

3.5. ***Application: Ramification compatibility of fields of norms.*** In this subsection, we prove Theorem 3.5.3, which is the ramification compatibility of Scholl's equivalence in Theorem 1.8.3, as an application of our Gröbner basis argument.

We first construct a characteristic zero lift of the Abbes–Saito space in characteristic p.

Lemma 3.5.1. *Let F/E be a finite extension of complete discrete valuation fields of characteristic p. Assume that the residue field extension k_F/k_E is either trivial or purely inseparable. For $m \in \mathbb{N}$, we put $\underline{X} := (X_0, \dots, X_m)$ and $\underline{Y} := (Y_0, \dots, Y_m)$.*

(i) [*Xiao 2010, Notation* 3.3.8] *For some $m \in \mathbb{N}$, there exist a set of generators $\{z_0, \dots, z_m\}$ of $\mathcal{O}_F$ as an $\mathcal{O}_E$-algebra, with z_0 a uniformizer of F, and a set of generators $\{p_0, \dots, p_m\}$ of the kernel of the $\mathcal{O}_E$-algebra homomorphism $\mathcal{O}_E\langle \underline{X}\rangle \twoheadrightarrow \mathcal{O}_F$ defined by $X_j \mapsto z_j$ such that*

$$\begin{aligned}p_0 &= X_0^{e_{F/E}} + \pi_E \eta_0, \\ p_j &= X_j^{f_j} - \varepsilon_j + X_0 \delta_j + \pi_E \eta_j \quad \text{for } 1 \leq j \leq m,\end{aligned}$$

where $\delta_j, \eta_j \in \mathcal{O}_E\langle \underline{X}\rangle$, $\varepsilon_j \in \mathcal{O}_E\langle X_0, \dots, X_{j-1}\rangle$ and $f_j \in \mathbb{N}$.

(ii) *Let $\succeq$ be the lexicographic order on $\mathcal{O}_E\langle \underline{X}\rangle$ defined by $X_m \succ \cdots \succ X_0$. We view π_E as a regular system of parameters of $\mathcal{O}_E$ and apply Construction 3.2.2. Then, we have $\mathrm{LT}_{\mathcal{O}_E}(p_0^n) = X_0^{ne_{F/E}}$ for all $n \in \mathbb{N}$. Let $l, n \in \mathbb{N}_{>0}$ satisfy*

$p^l n \geq e_{F/E}$. Then, for $1 \leq j \leq m$, there exists $\theta_{j,l,n} \in \mathcal{O}_E\langle \underline{X} \rangle$ such that $\mathrm{LT}_{\mathcal{O}_E}(p_j^{p^l n} - p_0^{\lfloor p^l n/e_{F/E} \rfloor}\theta_{j,l,n}) = uX_j^{f_j p^l n}$ for some unit $u \in 1 + \pi_E\mathcal{O}_E$.

(iii) (*cf.* [*Xiao 2010, Example* 1.3.4.]). *Fix an isomorphism $E \cong k_E((S))$. Let $\mathcal{O}$ be a Cohen ring of k_E and let $R := \mathcal{O}[\![S]\!]$ with canonical projection $R \to \mathcal{O}_E$. Fix a lift $P_j \in R\langle \underline{X} \rangle$ of p_j for all j. Let $\underline{\alpha} \in \mathbb{N}^{m+1}$, $\underline{\beta} \in \mathbb{N}_{>0}^{m+1}$. Assume that $\lfloor \beta_j/e_{F/E} \rfloor \geq \beta_0$ for all $1 \leq j \leq m$, and assume that there exists $l \in \mathbb{N}_{>0}$ such that $p^l \mid \beta_j$ for all $1 \leq j \leq m$. Then, the R-algebra*

$$A_{\underline{\alpha},\underline{\beta}} := R\langle \underline{X}, \underline{Y} \rangle / (S^{\alpha_j} Y_j - P_j^{\beta_j},\ 0 \leq j \leq m).$$

is R-flat. Moreover, the fiber of $A_{\underline{\alpha},\underline{\beta}}$ at any Eisenstein prime $\mathfrak{p}$ of R is an affinoid variety, which gives rise to the following affinoid subdomain of $D^{m+1}_{\kappa(\mathfrak{p})}$:

$$D^{m+1}(|\pi_{\mathfrak{p}}|^{-\alpha_j/\beta_j}(P_j \bmod \mathfrak{p}),\ 0 \leq j \leq m).$$

Proof.

(i) See [Xiao 2010, Construction 3.3.5] for details.

(ii) Since the coefficient of $X_0^{ne_{F/E}}$ in p_0^n is equal to 1, the first assertion follows from $p_0^n \equiv X_0^{ne_{F/E}} \bmod \pi_E$. For the second, we put $\theta_{j,l,n} := X_0^{p^l n - e_{F/E}\lfloor p^l n/e_{F/E} \rfloor}\delta_j^{p^l n}$. Since

$$p_j^{p^l n} \equiv X_j^{p^l n f_j} - \varepsilon_j^{p^l n} + X_0^{p^l n}\delta_j^{p^l n} \equiv X_j^{p^l n f_j} - \varepsilon_j^{p^l n} + p_0^{\lfloor p^l n/e_{F/E} \rfloor}\theta_{j,l,n} \bmod \pi_E,$$

we have $\mathrm{LT}_{k_E}(p_j^{p^l n} - p_0^{\lfloor p^l n/e_{F/E} \rfloor}\theta_{j,l,n} \bmod \pi_E) = \mathrm{LT}_{k_E}(X_j^{p^l n f_j} - \varepsilon_j^{p^l n} \bmod \pi_E) = X_j^{f_j p^l n}$, which implies the assertion.

(iii) The last assertion is trivial. We prove the first assertion. Let $\succeq$ be the lexicographic order on $\mathcal{O}_E\langle \underline{X}, \underline{Y} \rangle$ defined by $X_m \succ \cdots \succ X_0 \succ Y_m \succ \cdots \succ Y_0$. We view $\{p, S\}$ as a regular system of parameters of R and apply Construction 3.2.2. For $1 \leq j \leq m$, we choose a lift of $\theta_{j,l,\beta_j/p^l}$ and denote it by Θ_j for simplicity. Then, the ideal $(S^{\alpha_j} Y_j - P_j^{\beta_j},\ 0 \leq j \leq m)$ is generated by $Q_0 := S^{\alpha_0} Y_0 - P_0^{\beta_0}$ and

$$Q_j := S^{\alpha_j} Y_j - P_j^{\beta_j} - (S^{\alpha_0} Y_0 - P_0^{\beta_0}) P_0^{\lfloor \beta_j/e_{F/E} \rfloor - \beta_0}\Theta_j$$

for $1 \leq j \leq m$. It follows from Proposition 3.2.12 that we only have to prove that $\mathrm{LT}_{R/\mathfrak{m}_R}(-Q_j \bmod \mathfrak{m}_R)$ are relatively prime monic monomials. We have $\mathrm{LT}_{R/\mathfrak{m}_R}(Q_0 \bmod \mathfrak{m}_R) = -\mathrm{LT}_{R/\mathfrak{m}_R}(p_0^{\beta_0}) = -X_0^{e_{F/E}\beta_0}$. Since

$$Q_j \equiv -p_j^{\beta_j} + p_0^{\lfloor \beta_j/e_{F/E} \rfloor}\theta_{j,l,\beta_j/p^l} \bmod \mathfrak{m}_R,$$

we have $\mathrm{LT}_{R/\mathfrak{m}_R}(Q_j \bmod \mathfrak{m}_R) = -X_j^{f_j\beta_j}$ by (ii), which yields the assertion. □

In the rest of this subsection, let the notation be as in Definition 1.8.1.

Lemma 3.5.2. *Fix an isomorphism $X_{\mathfrak{K}} \cong k_{\mathfrak{K}}((\Pi))$, let $\mathcal{O}$ be a Cohen ring of $k_{\mathfrak{K}}$ and put $R := \mathcal{O}[[\Pi]]$.*

(i) *There exists a surjective local ring homomorphism $\phi_n : R \to \mathcal{O}_{K_n}$ for all sufficiently large n such that diagram*

$$\begin{array}{ccc} R & \xrightarrow{\text{can.}} & X_{\mathfrak{K}}^{+} \\ \downarrow \phi_n & & \downarrow \mathrm{pr}_n \\ \mathcal{O}_{K_n} & \xrightarrow{\text{can.}} & \mathcal{O}_{K_n}/\xi\mathcal{O}_{K_n} \end{array}$$

commutes, and $\ker(\phi_n)$ *is an Eisenstein prime ideal of R. We fix ϕ_n in the following and put $\mathfrak{p}_n := \ker(\phi_n)$.*

(ii) *Let $r \in \mathbb{Q}_{>0}$ and let L_∞/K_∞ be a finite extension and $\mathfrak{L} = \{L_n\}_{n>0}$ a corresponding strictly deeply ramified tower. Assume that the residue field extension of $X_{\mathfrak{L}}/X_{\mathfrak{K}}$ is either trivial or purely inseparable. Then, there exists a flat R-algebra AS^r (resp. $AS^r_{\log}$) of the form $R\langle \underline{X}\rangle/I$ for an ideal $I \subset R\langle \underline{X}\rangle$, whose fibers at (p) and $\mathfrak{p}_n$ are isomorphic to the Abbes–Saito spaces $as^r_{X_{\mathfrak{L}}/X_{\mathfrak{K}},\bullet}$ and $as^r_{L_n/K_n,\bullet}$ (resp. $as^r_{X_{\mathfrak{L}}/X_{\mathfrak{K}},\bullet,\bullet}$ and $as^r_{L_n/K_n,\bullet,\bullet}$) for all sufficiently large n.*

(iii) *With the notation and assumption of (ii), we have for all sufficiently large n:*

$$\#\mathcal{F}^r(X_{\mathfrak{L}}) = \#\mathcal{F}^r(L_n), \quad \#\mathcal{F}^r_{\log}(X_{\mathfrak{L}}) = \#\mathcal{F}^r_{\log}(L_n).$$

Proof. Put $E := X_{\mathfrak{K}}$ and $F := X_{\mathfrak{L}}$.

(i) For all sufficiently large n, the projection $\mathrm{pr}_n : \mathcal{O}_E \to \mathcal{O}_{K_n}/\xi\mathcal{O}_{K_n}$ induces an isomorphism $\Phi_n : k_{\mathfrak{K}} \to k_{K_n}$ of the residue fields. Hence, we can choose an embedding $\mathcal{O} \to \mathcal{O}_{K_n}$ that lifts Φ_n. Let π_{K_n} be a uniformizer of $\mathcal{O}_{K_n}$, which is a lift of $\mathrm{pr}_n(\Pi) \in \mathcal{O}_{K_n}/\xi\mathcal{O}_{K_n}$. Since the $\mathcal{O}$-algebra homomorphism $\mathcal{O}[\Pi] \to R$; $\Pi \mapsto \Pi$ is formally étale, we have a map ϕ_n sending Π to π_{K_n}. Since $\mathcal{O}_{K_n}/\mathcal{O}$ is totally ramified, the kernel of ϕ_n is generated by an Eisenstein polynomial.

(ii) Fix $\xi' \in \mathcal{O}_{K_\infty}$ such that $0 < v_p(\xi') < v_p(\xi)$ and such that $\{L_n\}_{n>0}$ is strictly deeply ramified with respect to ξ'. We denote the composite $\mathrm{can} \circ \mathrm{pr}_n : \mathcal{O}_E \to \mathcal{O}_{K_n}/\xi\mathcal{O}_{K_n} \to \mathcal{O}_{K_n}/\xi'\mathcal{O}_{K_n}$ by pr_n again, and fix an expression $r = a/b$ with $a, b \in \mathbb{N}$ and $b > 0$. Also, fix $l \in \mathbb{N}$ with $p^l \geq e_{F/E}$. Define $\underline{\alpha}, \underline{\alpha}_{\log}, \underline{\beta}, \underline{\beta}_{\log} \in \mathbb{N}^l$ via $\alpha_0 := a$, $\alpha_{\log,0} := a + b$, $\beta_0 := \beta_{\log,0} := b$, and $\alpha_j = \alpha_{\log,j} = ap^l$, $\beta_j = \beta_{\log,j} := bp^l$ for $1 \leq j \leq m$. Then, we can apply Lemma 3.5.1 to the finite extension F/E. In the following, we use the notation as of that lemma. We will prove that $A_{\underline{\alpha},\underline{\beta}}$ (resp. $A_{\underline{\alpha}_{\log},\underline{\beta}_{\log}}$) satisfies the desired condition. We first consider the nonlog case. By Lemma 3.5.1(iii), the fiber of $A_{\underline{\alpha},\underline{\beta}}$ at (p) is isomorphic to

$as^r_{F/E,Z}$, where $Z = \{z_0, \ldots, z_m\}$. Recall that we have a canonical surjection $\mathrm{pr}_n : \mathcal{O}_F \to \mathcal{O}_{L_n}/\xi'\mathcal{O}_{L_n}$ for all sufficiently large n. We choose a lift $z_j^{(n)} \in \mathcal{O}_{L_n}$ of $\mathrm{pr}_n(z_j) \in \mathcal{O}_{L_n}/\xi'\mathcal{O}_{L_n}$. Then, the $z_j^{(n)}$'s are generators of $\mathcal{O}_{L_n}$ as an $\mathcal{O}_{K_n}$-algebra by Nakayama's lemma and, by lemma Lemma 3.5.1(i), $z_j^{(0)}$ is a uniformizer of $\mathcal{O}_{L_n}$. We consider the surjection $\varphi_n : \mathcal{O}_{K_n}\langle \underline{X}\rangle \to \mathcal{O}_{L_n}$; $X_j \mapsto z_j^{(n)}$ and choose a lift $p_j^{(n)} \in \ker(\varphi_n)$ of $\mathrm{pr}_n(p_j) \in \mathcal{O}_{K_n}/\xi'\mathcal{O}_{K_n}[\underline{X}]$:

$$\begin{array}{ccc}
\mathcal{O}_E\langle \underline{X}\rangle & \xrightarrow{X_j \mapsto z_j} & \mathcal{O}_F \\
\downarrow{\scriptstyle \mathrm{pr}_n} & & \downarrow{\scriptstyle \mathrm{pr}_n} \\
\mathcal{O}_{K_n}/\xi'\mathcal{O}_{K_n}[\underline{X}] & \xrightarrow{X_j \mapsto \mathrm{pr}_n(z_j)} & \mathcal{O}_{L_n}/\xi'\mathcal{O}_{L_n} \\
\uparrow{\scriptstyle \mathrm{can.}} & & \uparrow{\scriptstyle \mathrm{can.}} \\
\mathcal{O}_{K_n}\langle \underline{X}\rangle & \xrightarrow{\varphi_n;\, X_j \mapsto z_j^{(n)}} & \mathcal{O}_{L_n}.
\end{array}$$

By Nakayama's lemma, the $p_j^{(n)}$'s are generators of $\ker(\varphi_n)$. We may assume $v_{K_n}(\xi') \geq r$ by choosing n sufficiently large. Since $\phi_n(P_j) \equiv p_j^{(n)} \bmod (\xi')$, we have $|\phi_n(P_j)(x)| \leq |\pi_{K_n}|^r$ if and only if $|p_j^{(n)}(x)| \leq |\pi_{K_n}|^r$ for any $x \in \mathcal{O}_{\overline{K}}^{m+1}$. This implies that the fiber of AS^r at $\mathfrak{p}_n$ is isomorphic to $as^r_{L_n/K_n,Z^{(n)}}$, where $Z^{(n)} = \{z_0^{(n)}, \ldots, z_m^{(n)}\}$, which implies the assertion. In the log case, a similar proof works if we choose n sufficiently large such that $v_{K_n}(\xi') \geq r+1$.

(iii) This follows from applying Proposition 3.4.8 to AS^r and $AS^r_{\log}$. □

The following is the main theorem in this subsection. See [Hattori 2014, §6] for an alternative proof.

Theorem 3.5.3. *Let L_∞/K_∞ be a finite separable extension and $\mathfrak{L} = \{L_n\}_{n>0}$ a corresponding strictly deeply ramified tower. Then, the sequence $\{b(L_n/K_n)\}_{n>0}$ (resp. $\{b_{\log}(L_n/K_n)\}_{n>0}$) converges to $b(X_{\mathfrak{L}}/X_{\mathfrak{K}})$ (resp. $b_{\log}(X_{\mathfrak{L}}/X_{\mathfrak{K}})$).*

Proof. Since the nonlog and log ramification filtrations are invariant under base change, so are the nonlog and log ramification breaks. Hence, we may assume that the residue field extension of $X_{\mathfrak{L}}/X_{\mathfrak{K}}$ is either trivial or purely inseparable by replacing K_∞ and L_∞ by their maximal unramified extensions. We first prove the nonlog case. Recall that we have $[X_{\mathfrak{L}} : X_{\mathfrak{K}}] = [L_n : K_n]$ for all sufficiently large n by Theorem 1.8.3. For $r \in \mathbb{Q}_{>0}$ with $b(X_{\mathfrak{L}}/X_{\mathfrak{K}}) < r$, we have $\#\mathcal{F}^r(L_n) = \#\mathcal{F}^r(X_{\mathfrak{L}}) = [L_n : K_n]$ for all sufficiently large n by Lemma 3.5.2. Hence, we have $\limsup_n b(L_n/K_n) \leq b(X_{\mathfrak{L}}/X_{\mathfrak{K}})$. For $r \in \mathbb{Q}_{>0}$ with $b(X_{\mathfrak{L}}/X_{\mathfrak{K}}) > r$, we have $\#\mathcal{F}^r(L_n) = \#\mathcal{F}^r(X_{\mathfrak{L}}) < [L_n : K_n]$ for all sufficiently large n by Lemma 3.5.2 and the definition of $\mathcal{F}^r$. Hence, we have $\liminf_n b(L_n/K_n) \geq b(X_{\mathfrak{L}}/X_{\mathfrak{K}})$. Therefore, we have $b(X_{\mathfrak{L}}/X_{\mathfrak{K}}) \leq \liminf_n b(L_n/K_n) \leq \limsup_n b(L_n/K_n) \leq b(X_{\mathfrak{L}}/X_{\mathfrak{K}})$, which implies the assertion. In the log case, the same argument with b and $\mathcal{F}^r$ replaced by $b_{\log}$ and $\mathcal{F}^r_{\log}$ works. $\square$

The following representation version of Theorem 3.5.3 will be used in the proof of Theorem 4.7.1.

Lemma 3.5.4. *Let $F/\mathbb{Q}_p$ be a finite extension and let $V \in \mathrm{Rep}^f_F(G_{K_n})$ a finite F-representation for some n. We identify $G_{X_{\mathfrak{K}}}$ with G_{K_∞} via the equivalence in Theorem 1.8.3.*

(i) *For $m \geq n$, let L_m (resp. L_∞, X') be the finite Galois extension corresponding to the kernel of the action of G_{K_m} (resp. G_{K_∞}, $G_{X_{\mathfrak{K}}}$) on V. Then, L_∞ corresponds to X' under the equivalence in Theorem 1.8.3 and $\{L_m\}_{m\geq n}$ is a strictly deeply ramified tower corresponding to L_∞.*

(ii) *The sequences $\left\{\mathrm{Art}^{\mathrm{AS}}(V|_{K_m})\right\}_{m\geq n}$ and $\left\{\mathrm{Swan}^{\mathrm{AS}}(V|_{K_m})\right\}_{m\geq n}$ are eventually stationary and their limits are equal to $\mathrm{Art}^{\mathrm{AS}}(V|_{X_{\mathfrak{K}}})$ and $\mathrm{Swan}^{\mathrm{AS}}(V|_{X_{\mathfrak{K}}})$.*

Proof.

(i) The first assertion is trivial. We prove the second assertion. Since $G_{L_n} \cap G_{K_m} = G_{L_m}$ for all $m \geq n$, we have $L_m = L_n K_m$. Therefore, $\{L_m\}$ is a strictly deeply ramified tower corresponding to $L'_\infty := \bigcup_m L_m$. Hence, we only have to prove that $L_\infty = L'_\infty$. Let $\rho : G_{K_n} \to \mathrm{GL}(V)$ be a matrix presentation of V. By the commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & G_{L_\infty} & \xrightarrow{\text{inc.}} & G_{K_\infty} & \xrightarrow{\rho} & \mathrm{GL}(V) \\ & & & & \Big\downarrow{\scriptstyle \text{can.}} & & \Big\downarrow{\scriptstyle \text{id}} \\ 1 & \longrightarrow & G_{L_m} & \xrightarrow{\text{inc.}} & G_{K_m} & \xrightarrow{\rho|_{G_{K_m}}} & \mathrm{GL}(V), \end{array}$$

where the horizontal sequences are exact, we obtain a canonical injection $G_{L_\infty} \hookrightarrow G_{L_m}$. Therefore, we have $L_m \subset L_\infty$, hence, $L'_\infty \subset L_\infty$. To prove the converse, we only have to prove $[L_\infty : K_\infty] \leq [L'_\infty : K_\infty]$. Since $(K_\infty \cap L_n)/K_n$ is finite, we have $K_\infty \cap L_n = K_m \cap L_n$ for sufficiently large m. In particular,

$$\begin{aligned} [L'_\infty : K_\infty] &= [L_n K_\infty : K_\infty] = [L_n : K_\infty \cap L_n] \\ &= [L_n : K_m \cap L_n] = [L_n K_m : K_m] = [L_m : K_m]. \end{aligned}$$

Then, the assertion follows from

$$[L_\infty : K_\infty] = \#\rho(G_{K_\infty}) \leq \#\rho(G_{K_m}) = [L_m : K_m].$$

(ii) By Maschke's theorem, there exists an irreducible decomposition $V|_{X_{\mathfrak{K}}} = \bigoplus_\lambda V^\lambda$ with $V^\lambda \in \mathrm{Rep}^f_F(G_{X_{\mathfrak{K}}})$. We choose $m_0 \in \mathbb{N}$ such that the canonical map $G_{L_\infty/K_\infty} \to G_{L_m/K_m}$ is an isomorphism for all $m \ge m_0$. Then, V^λ is G_{K_m}-stable for all $m \ge m_0$. Moreover, $V^\lambda|_{K_m} \in \mathrm{Rep}_F^f(G_{K_m})$ is irreducible. For $m \ge m_0$, let L_m^λ/K_m be the finite Galois extension corresponding to the kernel of the action of G_{K_m} on V^λ. By (i), $\mathfrak{L}^\lambda = \{L_m^\lambda\}_{m \ge m_0}$ is a strictly deeply ramified tower and $X_{\mathfrak{L}^\lambda}$ corresponds to the kernel of the action of $G_{X_{\mathfrak{K}}}$ on V^λ. By the irreducibility of the action of G_{K_m} (resp. $G_{X_{\mathfrak{K}}}$) on V^λ, we have

$$\mathrm{Art}^{\mathrm{AS}}(V^\lambda|_{K_m}) = b(L_m^\lambda/K_m)\dim_F(V),$$
$$\mathrm{Art}^{\mathrm{AS}}(V^\lambda|_{X_{\mathfrak{K}}}) = b(X_{\mathfrak{L}^\lambda}/X_{\mathfrak{K}})\dim_F(V)$$

for $m \ge m_0$. We apply Theorem 3.5.3 to each $\mathfrak{L}^\lambda$, to get $\lim_{m\to\infty}\mathrm{Art}(V|_{K_m}) = \mathrm{Art}(V|_{X_{\mathfrak{K}}})$. Note that K_m is not absolutely unramified for sufficiently large m. Indeed, the definition of strictly deeply ramified implies that K_{m+1}/K_m is not unramified. By Theorem 1.5.1, the convergence of $\{\mathrm{Art}(V|_{K_m})\}$ implies that $\{\mathrm{Art}(V|_{K_m})\}$ is eventually stationary, which implies the assertion for the Artin conductor. The assertion for the Swan conductor follows from the same argument by replacing Art and b by Swan and $b_{\log}$. □

Remark 3.5.5 (a Hasse–Arf property). Let the notation be as in Lemma 3.5.4 and let $p = 2$. By Theorem 1.7.10 and Lemma 3.5.4(ii), $\mathrm{Swan}(V|_{K_m})$ is an integer for all sufficiently large m (cf. Theorem 1.5.1).

4. Differential modules associated to de Rham representations

In this section, we first construct $\mathbb{N}_{\mathrm{dR}}(V)$ as a (φ, Γ_K)-module for de Rham representations $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G_K)$, see Section 4.2. Then, we prove that $\mathbb{N}_{\mathrm{dR}}(V)$ can be endowed with a (φ, ∇)-module structure (Section 4.4). Then, we define Swan conductors of de Rham representations (Section 4.6) and we prove that the differential Swan conductor of $\mathbb{N}_{\mathrm{dR}}(V)$ and Swan conductor of V are compatible (Section 4.7).

Throughout this section, let K be a complete discrete valuation field of mixed characteristic $(0, p)$. Except for Section 4.6, we assume that K satisfies Assumption 1.9.1, and we use the notation of Section 1.3.

4.1. ***Calculation of horizontal sections.*** For perfect k_K, $\mathbb{N}_{\mathrm{dR}}(V)$ is constructed by gluing a certain family of vector bundles over $K_n[\![t]\!]$ for $n \gg 0$, see [Berger 2008b, Section II.1]. When k_K is not perfect, $K_n[\![t]\!]$ should be replaced by the ring of horizontal sections of $K_n[\![u, t_1, \ldots, t_d]\!]$ with respect to the connection ∇^{geom}, which will be studied in this subsection.

Definition 4.1.1. (i) We have a canonical K_n-algebra injection

$$K_n[\![t, u_1, \ldots, u_d]\!] \to \mathbb{B}_{\mathrm{dR}}^+$$

since $\mathbb{B}_{\mathrm{dR}}^{+}$ is a complete local K^{alg}-algebra. The topology of $K_n[\![t, u_1, \dots, u_d]\!]$ as a subring of $\mathbb{B}_{\mathrm{dR}}^{+}$ (endowed with the canonical topology) is called the canonical topology. Note that $K_n[\![t, u_1, \dots, u_d]\!]$ is stable under the G_K-action, and that the G_K-action factors through Γ_K.

(ii) Let F be a complete valuation field. The Fréchet topology on

$$F[\![X_1, \dots, X_n]\!] \cong \varprojlim_m F[X_1, \dots, X_n]/(X_1, \dots, X_n)^m$$

is the inverse limit topology, where $F[X_1, \dots, X_n]/(X_1, \dots, X_n)^m$ is endowed with a (unique) topological F-vector space structure. Note that $F[\![X_1, \dots, X_n]\!]$ is a Fréchet space, and that the $(X_1, \dots, X_n)$-adic topology of $F[\![X_1, \dots, X_n]\!]$ is finer than the Fréchet topology.

Lemma 4.1.2. *The canonical topology of $K_n[\![t, u_1, \dots, u_d]\!]$ and the Fréchet topology are equivalent. In particular, $K_n[\![t, u_1, \dots, u_d]\!]$ is a closed subring of $\mathbb{B}_{\mathrm{dR}}^{+}$.*

Proof. Put $V_m := K_n[t, u_1, \dots, u_d]/(t, u_1, \dots, u_d)^m$ and identify $K_n[\![t, u_1, \dots, u_d]\!]$ with $\varprojlim_m V_m$. If we endow V_m with a (unique) topological K_n-vector space structure, then the resulting inverse limit topology is the Fréchet topology. We have a canonical injection $V_m \to \mathbb{B}_{\mathrm{dR}}^{+}/(t, u_1, \dots, u_d)^m$. If we endow V_m with the subspace topology as a subset of $\mathbb{B}_{\mathrm{dR}}^{+}/(t, u_1, \dots, u_d)^m$, which is endowed with the canonical topology, then the resulting inverse limit topology is the canonical topology. Since $\mathbb{B}_{\mathrm{dR}}^{+}/(t, u_1, \dots, u_d)^m$ is K_n-Banach space by definition, V_m endowed with this topology is a topological K_n-vector space. This implies the assertion. □

Notation 4.1.3. The subring $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla^{\mathrm{geom}}=0} = \mathbb{B}_{\mathrm{dR}}^{\nabla+} \cap K_n[\![t, u_1, \dots, u_d]\!]$ of $\mathbb{B}_{\mathrm{dR}}^{\nabla+}$ is denoted by $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ for $n \in \mathbb{N}$. We call the subspace topology of $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ as a subring of $\mathbb{B}_{\mathrm{dR}}^{+}$ (endowed with the canonical topology) the canonical topology. Note that $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ is a closed subring of $\mathbb{B}_{\mathrm{dR}}^{\nabla+}$ since the connection $\nabla^{\mathrm{geom}} : \mathbb{B}_{\mathrm{dR}}^{+} \to \mathbb{B}_{\mathrm{dR}}^{+} \otimes_K \widehat{\Omega}_K^1$ is continuous and $\mathbb{B}_{\mathrm{dR}}^{\nabla+}$ is closed in $\mathbb{B}_{\mathrm{dR}}^{+}$.

Lemma 4.1.4. *The ring $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ is a complete discrete valuation ring with residue field K_n and uniformizer t.*

Proof. We define a map

$$f : K_n[t, u_1, \dots, u_d] \to K_n[\![t, u_1, \dots, u_d]\!]$$
$$x \mapsto \sum_{(n_1,\dots,n_d)\in\mathbb{N}^d} \frac{(-1)^{n_1+\cdots+n_d}}{n_1! \dots n_d!} u_1^{n_1} \dots u_d^{n_d}\, \partial_1^{n_1} \circ \cdots \circ \partial_d^{n_d}(x).$$

It is easy to check that this is an abstract ring homomorphism such that $\mathrm{Im}(f) \subset K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$, $f(tx) = tf(x)$ for all $x \in K_n[t, u_1, \dots, u_d]$ and $f(u_j) = 0$ for all j. In particular, f is $(t, u_1, \dots, u_d)$-adically continuous. Passing to the completion, we obtain a ring homomorphism $f : K_n[\![t, u_1, \dots, u_d]\!] \to K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$. Since f is identity on $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$, f is surjective and f induces a surjection

$$\bar{f} : K_n[\![t]\!] \cong K_n[\![t, u_1, \dots, u_d]\!]/(u_1, \dots, u_d) \to K_n[\![t, u_1, \dots, u_d]\!]^{\nabla},$$

where the first isomorphism is induced by the inclusion $K_n[\![t]\!] \subset K_n[\![t, u_1, \dots, u_d]\!]$. Since $\bar{f}(t) = t$ is nonzero, $\bar{f}$ is an isomorphism, which implies the assertion. □

Lemma 4.1.5. *The t-adic topology on $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ is finer than the canonical topology.*

Proof. Denote $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ by R and identify R with $\varprojlim_m R/t^m R$. If we endow $R/t^m R$ with the discrete topology, then the resulting inverse limit topology is the t-adic topology. By Lemma 4.1.4 and dévissage, the canonical map $R/t^m R \to K_n[t, u_1, \dots, u_d]/(t, u_1, \dots, u_d)^m$ is injective. If we endow $R/t^m R$ with the subspace topology as a subset of $K_n[t, u_1, \dots, u_d]/(t, u_1, \dots, u_d)^m$, endowed with a (unique) topological K_n-vector space structure, then the resulting inverse limit topology is the canonical topology. Since the discrete topology is the finest topology, we obtain the assertion. □

The map f defined in the proof of Lemma 4.1.4 is continuous when $K = \widetilde{K}$:

Lemma 4.1.6. *Let $\varphi : \mathcal{O}_{\widetilde{K}} \to \mathcal{O}_{\widetilde{K}}$ be the unique Frobenius lift, characterized by $\varphi(t_j) = t_j^p$ for all $1 \le j \le d$. Then, the map $f : \widetilde{K}_n[\![t, u_1, \dots, u_d]\!] \to \widetilde{K}_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ defined in the proof of Lemma 4.1.4 is continuous with respect to the Fréchet topologies.*

Proof. By the definition of f, we only have to prove the following claim: for all $m \in \mathbb{N}$ and $1 \le j \le d$, we have

$$\partial_j^m(\mathcal{O}_{\widetilde{K}}) \subset m!\, \mathcal{O}_{\widetilde{K}}.$$

We first note since $d : \mathcal{O}_{\widetilde{K}} \to \widehat{\Omega}^1_{\mathcal{O}_{\widetilde{K}}}$ and $\varphi_* : \widehat{\Omega}^1_{\mathcal{O}_{\widetilde{K}}} \to \widehat{\Omega}^1_{\mathcal{O}_{\widetilde{K}}}$ commute, we have

$$\partial_j \circ \varphi^i = p^i t_j^{p^i - 1} \varphi^i \circ \partial_j \tag{5}$$

for all $i \in \mathbb{N}$ and $1 \le j \le d$. We prove the claim. Fix m and choose $i \in \mathbb{N}$ such that $v_p(m!) \le i$. Since $k_{\widetilde{K}} = k_{\widetilde{K}}^{p^i}[\bar{t}_1, \dots, \bar{t}_d]$, we have $\mathcal{O}_{\widetilde{K}} = \varphi^i(\mathcal{O}_{\widetilde{K}})[t_1, \dots, t_d]$ by Nakayama's lemma. By Leibniz's rule, we have

$$\partial_j^m(\varphi^i(\lambda) t_1^{a_1} \dots t_d^{a_d}) = \sum_{0 \le m_0 \le m} \binom{m}{m_0} \partial_j^{m_0}(\varphi^i(\lambda)) t_1^{a_1} \dots \partial_j^{m-m_0}(t_j^{a_j}) \dots t_d^{a_d} \tag{6}$$

for $\lambda \in \mathcal{O}_{\widetilde{K}}$ and $a_1, \dots, a_d \in \mathbb{N}$. We have $\partial_j^{m_0}(\varphi^i(\lambda)) \in p^i \mathcal{O}_{\widetilde{K}} \subset m! \mathcal{O}_{\widetilde{K}}$, unless $m_0 = 0$, by (5), and $\partial_j^m(t_j^{a_j}) \in m!\, \mathcal{O}_{\widetilde{K}}$. Hence, the RHS of (6) belongs to $m!\, \mathcal{O}_{\widetilde{K}}$, which implies the claim. □

4.2. ***Construction of*** $\mathbb{N}_{\mathbf{dR}}$. In this subsection, we construct $\mathbb{N}_{\mathrm{dR}}(V)$ as a (φ, Γ_K)-module for de Rham representations V. The idea is similar to [Berger 2008b, §II], i.e., gluing a compatible family of vector bundles over $K_n[\![t, u_1, \dots, u_d]\!]^{\nabla}$ to obtain vector bundles over $\mathbb{B}^{\dagger,r}_{\mathrm{rig}}$.

Notation 4.2.1. For $n \in \mathbb{N}$, put $r(n) := 1/p^{n-1}(p-1)$. For $r \in \mathbb{Q}_{>0}$, let $n(r) \in \mathbb{N}$ be the smallest integer n with $r \geq r(n)$.

For each K, we fix r_0 such that $\mathbb{A}_K$ has enough r_0-units (Construction 1.6.1) and $\mathbb{A}^{\dagger,r}_K \cong \mathcal{O}'((\pi'))^{\dagger,r/e_{K/\tilde{K}}}$ for all $r \in \mathbb{Q}_{>0} \cap (0, r_0)$ (Lemma 1.10.2), where $\mathcal{O}'$ is a Cohen ring of $k_{\mathbb{E}_K}$. In the rest of this section, let $r \in \mathbb{Q}_{>0}$, and when we consider $\mathbb{A}^{\dagger,r}_K$, $\mathbb{B}^{\dagger,r}_K$ and $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$, we tacitly assume $r \in \mathbb{Q}_{>0} \cap (0, r_0)$ unless otherwise stated. Moreover, for $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G_K)$, we further choose r_0 sufficiently small (dependent on V though) such that $\mathbb{D}^{\dagger,r}(V)$ admits a $\mathbb{B}^{\dagger,r}_K$-basis for all $r \in (0, r_0)$. Note that $\mathbb{A}^{\dagger,r}_K$, $\mathbb{B}^{\dagger,r}_K$ are PID's and that $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ is a Bézout integral domain.

Definition 4.2.2. Let $r > 0$ and $n \in \mathbb{N}$ with $n \geq n(r)$. For $x = \sum_{k \gg -\infty} p^k [x_k] \in \widetilde{\mathbb{B}}^{\dagger,r}$, the sequence $\{\sum_{k \leq N} p^k [x_k^{p^{-n}}]\}_{N \in \mathbb{Z}}$ converges in $\mathbb{B}^{\nabla+}_{\mathrm{dR}}$. Moreover, if we put

$$\iota_n : \widetilde{\mathbb{B}}^{\dagger,r} \to \mathbb{B}^{\nabla+}_{\mathrm{dR}}$$
$$x \mapsto \sum_{k \gg -\infty} p^k [x_k^{p^{-n}}],$$

then ι_n is a continuous ring homomorphism (see the proof of [Andreatta and Brinon 2010, Lemme 7.2] for details). Since $\mathbb{B}^{\nabla+}_{\mathrm{dR}}$ is Fréchet complete, ι_n extends to a continuous ring homomorphism

$$\iota_n : \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \to \mathbb{B}^{\nabla+}_{\mathrm{dR}}.$$

We also denote by ι_n the restriction of ι_n to $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}$ or $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. Unless otherwise stated, we also denote by ι_n the composite of ι_n and the inclusion $\mathbb{B}^{\nabla+}_{\mathrm{dR}} \subset \mathbb{B}^{+}_{\mathrm{dR}}$.

Lemma 4.2.3. *For $x \in \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$, we have*

$$x \in (\mathbb{B}^{\dagger,r}_K)^{\times} \Leftrightarrow x \in (\mathbb{B}^{\dagger,r}_{\mathrm{rig},K})^{\times} \Leftrightarrow x \text{ has no slopes} \Leftrightarrow x \in (\widetilde{\mathbb{B}}^{\dagger,r}_K)^{\times} \Leftrightarrow x \in (\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K})^{\times}.$$

Proof. Note that the slopes of x as an element of $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ or $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}$ are the same by definition (see Section 2). Therefore, the assertion follows from [Kedlaya 2005, Corollary 2.5.12]. □

Lemma 4.2.4. *For $B = \mathbb{B}^{\dagger,r}_K, \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}, \widetilde{\mathbb{B}}^{\dagger,r}_K, \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}$, we have*

$$\ker(\theta \circ \iota_n : B \to \mathbb{C}_p) = \varphi^{n-1}(q)B$$

for $n \geq n(r)$.

Proof. Note that since $\widetilde{\mathbb{E}}_K$ and $\widetilde{\mathbb{E}}_{K\widetilde{K}^{\mathrm{pf}}}$ are isomorphic, the associated analytic rings $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}$ and $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K\widetilde{K}^{\mathrm{pf}}}$ are isomorphic. Hence, in the case of $B=\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}$, the claim follows from [Berger 2008b, Proposition 4.8]. By regarding $\mathbb{C}_p$ as the completion of an algebraic closure of $\widetilde{K}^{\mathrm{pf}}$ and applying [Berger 2008b, Remarque 2.14], we have $\ker(\theta\circ\iota_n:\widetilde{\mathbb{B}}^{\dagger,r}\to\mathbb{C}_p)=\varphi^{n-1}(q)\widetilde{\mathbb{B}}^{\dagger,r}$. Since $(\widetilde{\mathbb{B}}^{\dagger,r})^{H_K}=\widetilde{\mathbb{B}}^{\dagger,r}_K$ and $\varphi^{n-1}(q)\in\widetilde{\mathbb{B}}^{\dagger,r}_K$, we obtain the assertion for $B=\widetilde{\mathbb{B}}^{\dagger,r}_K$. We will prove the assertion for $B=\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. Let $x\in\ker(\theta\circ\iota_n:\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}\to\mathbb{C}_p)$. Since $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ is a Bézout integral domain, we have $(x,\varphi^{n-1}(q))=(y)$ for some $y\in\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. Let $y'\in\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ such that $\varphi^{n-1}(q)=yy'$. Since $y\in\ker(\theta\circ\iota_n:\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}\to\mathbb{C}_p)=\varphi^{n-1}(q)\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}$, we have $y=\varphi^{n-1}(q)y''$ for some $y''\in\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},K}$, hence, $y'y''=1$. By Lemma 4.2.3, y' is a unit in $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. Hence, we have $x\in\varphi^{n-1}(q)\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ for any $x\in\ker(\theta\circ\iota_n:\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}\to\mathbb{C}_p)$, which implies the assertion. For $B=\mathbb{B}^{\dagger,r}_K$, a similar proof works since $\mathbb{B}^{\dagger,r}_K$ is a PID, hence, a Bézout integral domain. □

Lemma 4.2.5. *The image of $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ under ι_n is contained in $K_n[\![t,u_1,\dots,u_d]\!]$ for $n\geq n(r)$. In particular, ι_n induces a morphism $\iota_n:\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}\to K_n[\![t,u_1,\dots,u_d]\!]^{\nabla}$ for $n\geq n(r)$.*

Proof. Since $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}\subset\mathbb{B}^{\dagger,r(n)}_{\mathrm{rig},K}$, we may assume $r=r(n)$. By [Andreatta and Brinon 2010, Lemme 8.5], there exists a subring $\mathcal{A}_{R,(1,(p-1)p^{n-1})}$ of $\widetilde{\mathbb{A}}$ such that $\mathbb{A}^{\dagger,r(n)}_K=\mathcal{A}_{R,(1,(p-1)p^{n-1})}[[\bar{\pi}]^{-1}]$. The inclusion $\iota_n(\mathbb{B}^{\dagger,r}_K)\subset K_n[\![t,u_1,\dots,u_d]\!]$ is proved in Proposition 8.6 of the same paper. Since $K_n[\![r,u_1,\dots,u_d]\!]$ is closed in $\mathbb{B}^+_{\mathrm{dR}}$, we obtain the assertion. □

Lemma 4.2.6. *For $h\in\mathbb{N}$ and $n\geq n(r)$, the morphism*

$$\mathrm{pr}_h\circ\iota_n:\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}\to K_n[\![t,u_1,\dots,u_d]\!]^{\nabla}/t^hK_n[\![t,u_1,\dots,u_d]\!]^{\nabla}$$

is surjective.

Proof. Since $t\in\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ we may assume $h=1$ by Lemma 4.1.4. Put $\theta_n:=\theta\circ\iota_n$. Let $\mathbb{A}^+_K\subset\mathbb{A}^{\dagger,r}_K$ be as in [Andreatta and Brinon 2008, Proposition 4.42]. By the proof of [Andreatta and Brinon 2010, Lemme 8.2], $\theta_n:\mathbb{A}^+_K\to\mathcal{O}_{K_n}$ is surjective after taking the reduction modulo some power of p. Since $\mathbb{A}^+_K$ is Noetherian and $(p/\pi^a,p)$-adically Hausdorff complete, $\mathbb{A}^+_K$ is p-adically Hausdorff complete, which implies the surjectivity of $\theta_n:\mathbb{A}^+_K\to\mathcal{O}_{K_n}$ by Nakayama's lemma. □

Lemma 4.2.7. *The image of $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ under ι_n is dense in $K_n[\![t,u_1,\dots,u_d]\!]^{\nabla}$ with respect to the canonical topology for $n\geq n(r)$.*

Proof. By Lemma 4.1.5, the assertion follows from Lemma 4.2.6. □

Lemma 4.2.8 ([Kedlaya 2005, Corollary 2.8.5, Definition 2.9.5], see also [Berger 2008a, Proposition 1.1.1]). *For* $B = \widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}, \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}, \mathbb{B}^{\dagger}_{\mathrm{rig},K}, \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ *and a* B*-submodule* M *of a finite free* B*-module*, *the following are equivalent*:

(i) M *is finite free.*

(ii) M *is closed.*

(iii) M *is finitely generated.*

Lemma 4.2.9. *Let* B *be either* $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$ *or* $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. *If* I *is a principal ideal of* B *which divides* (t^h) *for some* $h \in \mathbb{N}$, *then* I *is generated by an element of the form* $\prod_{n\geq n(r)}(\varphi^{n-1}(q)/p)^{j_n}$ *with* $j_n \leq h$.

Proof. Note that we have a slope factorization $t = \pi \prod_{n\geq 1}(\varphi^{n-1}(q)/p)$ in $\mathbb{B}^{\dagger,r}_{\mathrm{rig},\mathbb{Q}_p}$ (see the proof of [Berger 2008b, Proposition I. 2.2]). For $n < n(r)$, $\varphi^{n-1}(q)/p$ is a unit in $\mathbb{B}^{\dagger,r}_{\mathrm{rig},\mathbb{Q}_p}$ and for $n \geq n(r)$, $\varphi^{n-1}(q)/p$ generates a prime ideal of B by Lemma 4.2.4. Hence, the assertion follows from the uniqueness of slope factorizations, see Lemma 2.0.5. □

Lemma 4.2.10 (The existence of a partition of unity). *Let* $n \in \mathbb{N}$ *and* $r > 0$ *satisfy* $n \geq n(r)$. *For* $w \in \mathbb{N}_{>0}$, *there exists* $t_{n,w} \in \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ *such that* $\iota_n(t_{n,w}) = 1 \bmod t^w K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla}$ *and* $\iota_m(t_{n,w}) \in t^w K_m[\![t, u_1, \ldots, u_d]\!]^{\nabla}$ *if* $m \neq n$ *and* $m \geq n(r)$.

Proof. Since $\mathbb{B}^{\dagger,r}_{\mathrm{rig},\mathbb{Q}_p} \subset \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ and $\mathbb{Q}_p(\zeta_{p^m})[\![t]\!] \subset K_m[\![t, u_1, \ldots, u_d]\!]^{\nabla}$, we may assume $K = \mathbb{Q}_p$. The assertion then follows from [Berger 2008b, Lemma I.2.1]. □

Lemma 4.2.11. *Let* B *be either* $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$ *or* $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. *For* $n \geq n(r)$, *write* $\iota_n : B := \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \to B_n := \mathbb{B}^{\nabla+}_{\mathrm{dR}}$ *in the first case and* $\iota_n : B := \mathbb{B}^{\dagger,r}_{\mathrm{rig},K} \to B_n := K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla}$ *in the second case. Let* D *be a* φ*-module over* B *of rank* d' *and* $D^{(1)}$ *and* $D^{(2)}$ *two* B*-submodules of rank* d' *stable by* φ *on* $D[1/t] = B[1/t] \otimes_B D$ *such that*

(i) $D^{(1)}[1/t] = D^{(2)}[1/t] = D[1/t]$;

(ii) $B_n \otimes_{\iota_n,B} D^{(1)} = B_n \otimes_{\iota_n,B} D^{(2)}$ *for all* $n \geq n(r)$.

Then, *we have* $D^{(1)} = D^{(2)}$.

Proof. Since $D^{(1)} + D^{(2)}$ is finite free by Lemma 4.2.8 and satisfies the same condition as $D^{(2)}$, we may assume that $D^{(1)} \subset D^{(2)}$ by replacing $D^{(2)}$ by $D^{(1)} + D^{(2)}$. Then, the proof of [Berger 2008b, Proposition I.3.4] works by using the ingredients Lemma 2.0.6 and Lemma 4.2.9 instead of [Berger 2008b, Proposition I.2.2]. □

Proposition 4.2.12 (cf. [Berger 2008b, Théorème II.1.2]). *Let* $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$ *be a de Rham representation with negative Hodge–Tate weights. Let* B *be either* $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$ *or* $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. *Let* B_n *and* $\iota_n : B \to B_n$ *be as in Lemma 4.2.11. In the first case, let* $D_n := (\mathbb{B}^{+}_{\mathrm{dR}} \otimes_K \mathbb{D}_{\mathrm{dR}}(V))^{\nabla^{\mathrm{geom}}=0}$, *and let* $D_n := (K_n[\![t, u_1, \ldots, u_d]\!] \otimes_K \mathbb{D}_{\mathrm{dR}}(V))^{\nabla^{\mathrm{geom}}=0}$ *in* *the second case. Put* $D := \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V$ *in the first case and* $D := \mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V)$ *in the second case. Then, the following holds.*

(i) *There exists* $h \in \mathbb{N}$ *such that*

$$t^h B_n \otimes_{\iota_n, B} D \subset D_n \subset B_n \otimes_{\iota_n, B} D$$

for all $n \geq n(r)$.

(ii) *Let* $\iota_n : D \to B_n \otimes_{\iota_n, B} D$ *be given by* $x \mapsto 1 \otimes x$ *and put*

$$\mathcal{N} := \{x \in D;\ \iota_n(x) \in D_n \ \text{for all } n \geq n(r)\}.$$

Then, $\mathcal{N}$ *is a finite free* B*-submodule of* D, *whose rank is equal to* $\dim_{\mathbb{Q}_p} V$. *Moreover, there exists a canonical isomorphism*

$$B_n \otimes_{\iota_n, B} \mathcal{N} \to D_n$$

for all $n \geq n(r)$.

Proof.

(i) Since the inclusion $B_n \subset \mathbb{B}^+_{\mathrm{dR}}$ is faithfully flat by Lemma 4.1.4, we only have to prove the assertion after tensoring $\mathbb{B}^+_{\mathrm{dR}}$ over B_n. We have the following isomorphisms:

$$\begin{aligned} \mathbb{B}^+_{\mathrm{dR}} \otimes_{B_n} B_n \otimes_{\iota_n, B} D &\cong \mathbb{B}^+_{\mathrm{dR}} \otimes_{\iota_n, \mathbb{B}^{\dagger,r}} \mathbb{B}^{\dagger,r} \otimes_{\mathbb{B}^{\dagger,r}} D^{\dagger,r} \\ &\cong \mathbb{B}^+_{\mathrm{dR}} \otimes_{\iota_n, \mathbb{B}^{\dagger,r}} \mathbb{B}^{\dagger,r} \otimes_{\mathbb{Q}_p} V = \mathbb{B}^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V, \end{aligned}$$

where $D^{\dagger,r} := \widetilde{\mathbb{B}}^{\dagger,r} \otimes_{\mathbb{Q}_p} V$ in the first case and $D^{\dagger,r} := \mathbb{D}^{\dagger,r}(V)$ in the second case. Since $\mathbb{B}^+_{\mathrm{dR}} \otimes_{B_n} D_n \subset \mathbb{B}^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$ by assumption and $\mathbb{B}^+_{\mathrm{dR}} \otimes_{B_n} D_n[1/t] \cong \mathbb{B}^+_{\mathrm{dR}} \otimes_K \mathbb{D}_{\mathrm{dR}}(V)[1/t] = \mathbb{B}_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$, there exists $h \in \mathbb{N}$ such that

$$t^h \mathbb{B}^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V \subset \mathbb{B}^+_{\mathrm{dR}} \otimes_{B_n} D_n \subset \mathbb{B}^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V,$$

which implies the assertion.

(ii) Since $\mathcal{N}$ is a closed B-submodule of D containing $t^h D$, $\mathcal{N}$ is free of rank $\dim_{\mathbb{Q}_p} V$ by Lemma 4.2.8. To prove the second assertion, we only have to prove that the canonical map $B_n \otimes_{\iota_n, B} \mathcal{N} \to D_n / t D_n$ is surjective for all $n \geq n(r)$ since B_n is a t-adically complete discrete valuation ring. Fix n and let $x \in D_n$. Note that $\mathrm{pr}_{h+1} \circ \iota_n : B \to B_n / t^{h+1} B_n$ is surjective. Indeed, when $B = \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$, this follows from Lemma 4.2.6. When $B = \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$, it is reduced to the case $h = 0$, and $\mathrm{pr}_1 \circ \iota_n = \theta \circ \iota_n : \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \to \mathbb{C}_p$ is surjective since $\widetilde{\mathbb{B}}^+ \subset \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$. Hence, there exists $y \in D$ such that $\iota_n(y) - x \in t^{h+1} B_n \otimes_{\iota_n, B} D \in t D_n$. We put

$z := t_{n,h+1}y \in D$, where $t_{n,h+1}$ is as in Lemma 4.2.10. By the property of $t_{\bullet,\bullet}$, we have

$$\iota_n(z) - x = \big(\iota_n(t_{n,h+1}) - 1\big)\iota_n(y) + \iota_n(y) - x \in tD_n$$

and for $m \neq n$,

$$\iota_m(z) \in t^{h+1}B_n \otimes_{\iota_n,B} D \subset tD_n.$$

These imply $z \in \mathcal{N}$; hence, we obtain the assertion. □

Definition 4.2.13. In the context of Proposition 4.2.12, we denote $\mathcal{N}$ by $\widetilde{\mathbb{N}}^{\dagger,r}_{\mathrm{rig}}(V)$ in the first case and by $\mathbb{N}_{\mathrm{dR},r}(V)$ in the second case. For a de Rham representation V with arbitrary Hodge–Tate weights, we put $\widetilde{\mathbb{N}}^{\dagger,r}_{\mathrm{rig}}(V) := \widetilde{\mathbb{N}}^{\dagger,r}_{\mathrm{rig}}(V(-n))(n)$ and $\mathbb{N}_{\mathrm{dR},r}(V) := \mathbb{N}_{\mathrm{dR},r}(V(-n))(n)$ for sufficiently large $n \in \mathbb{N}$. These definitions are independent of the choice of n. We also put $\widetilde{\mathbb{N}}^{\dagger}_{\mathrm{rig}}(V) := \bigcup_r \widetilde{\mathbb{N}}^{\dagger,r}_{\mathrm{rig}}(V)$ and $\mathbb{N}_{\mathrm{dR},r}(V) := \bigcup_r \mathbb{N}_{\mathrm{dR},r}(V)$. We note that for $0 < s \leq r$, the canonical map $\mathbb{B}^{\dagger,s}_{\mathrm{rig},K} \otimes_{\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}} \mathbb{N}_{\mathrm{dR},r}(V) \to \mathbb{N}_{\mathrm{dR},s}(V)$ is an isomorphism by Lemma 4.2.11 and Proposition 4.2.12. So, the canonical morphism $\mathbb{B}^{\dagger}_{\mathrm{rig},K} \otimes_{\mathbb{B}^{\dagger,r}_{\mathrm{rig}}} \mathbb{N}_{\mathrm{dR},r}(V) \to \mathbb{N}_{\mathrm{dR}}(V)$ is an isomorphism, and in particular, $\mathbb{N}_{\mathrm{dR}}(V)$ is a finite free $\mathbb{B}^{\dagger}_{\mathrm{rig},K}$-module of rank $\dim_{\mathbb{Q}_p} V$. Since the map $\varphi : \mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V) \to \mathbb{D}^{\dagger,r/p}_{\mathrm{rig}}(V)$ induces a map $\varphi : \mathbb{N}_{\mathrm{dR},r}(V) \to \mathbb{N}_{\mathrm{dR},r/p}(V)$ by the formula $\iota_{n+1} \circ \varphi = \iota_n$, $\mathbb{N}_{\mathrm{dR}}(V)$ is stable under the (φ, Γ_K)-action of $\mathbb{D}^{\dagger}_{\mathrm{rig}}(V)$. Similarly, $\widetilde{\mathbb{N}}^{\dagger}_{\mathrm{rig}}(V)$ is free of rank $\dim_{\mathbb{Q}_p} V$ and is stable under the (φ, G_K)-action of $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V$. Thus, we obtain a (φ, G_K)-module $\widetilde{\mathbb{N}}^{\dagger}_{\mathrm{rig}}(V)$ over $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}$ and a (φ, Γ_K)-module $\mathbb{N}_{\mathrm{dR}}(V)$ over $\mathbb{B}^{\dagger}_{\mathrm{rig},K}$.

4.3. ***Differential action of a p-adic Lie group.*** In this subsection, we recall basic facts on the differential action of a certain p-adic Lie group. Throughout this subsection, let $\mathcal{G}$ be a p-adic Lie group, which is isomorphic to an open subgroup of $(1 + 2p\mathbb{Z}_p) \ltimes \mathbb{Z}_p^d$ via a continuous group homomorphism $\eta : \mathcal{G} \hookrightarrow \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^d$. Denote $\eta(\gamma) = (\eta_0(\gamma), \dots, \eta_d(\gamma)) \in \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^d$ for $\gamma \in \mathcal{G}$. For $1 \leq j \leq d$, let

$$\mathcal{G}_0 := \{\gamma \in \mathcal{G};\ \eta_j(\gamma) = 0 \text{ for all } j > 0\},$$
$$\mathcal{G}_j := \{\gamma \in \mathcal{G};\ \eta_0(\gamma) = 1, \eta_i(\gamma) = 0 \text{ for all positive } i \neq j\}.$$

Notation 4.3.1. Let (R, v) be a $\mathbb{Q}_p$-Banach algebra and M a finite free R-module endowed with an R-valuation v. Assume that $\mathcal{G}$ acts on R and M such that:

(i) The $\mathcal{G}$-action on R is $\mathbb{Q}_p$-linear and the action of $\mathcal{G}$ on M is R-semilinear.

(ii) We have $v \circ \gamma(x) = v(x)$ for all $x \in R$ and $\gamma \in \mathcal{G}$.

(iii) There exists an open subgroup $\mathcal{G}_o \leq_o \mathcal{G}$ such that

$$v((\gamma - 1)x) \geq v(x) + v(p)$$

for all $\gamma \in \mathcal{G}_o$ and $x \in R$.

(iv) For any $x \in M$, there exists an open subgroup $\mathcal{G}_x \leq_o \mathcal{G}_o$ such that

$$v((\gamma - 1)x) \geq v(x) + v(p)$$

for all $\gamma \in \mathcal{G}_x$.

Construction 4.3.2. Let the notation be as in Notation 4.3.1. We extend the construction of the differential operator ∇_V in [Berger 2002, §5.1] to this setting. By assumption, there exists an open subgroup $\mathcal{G}_M \leq_o \mathcal{G}_o$ such that

$$v((\gamma - 1)x) \geq v(x) + v(p)$$

for all $x \in M$ and $\gamma \in \mathcal{G}_M$. Hence, we can apply Berger's argument to the 1-parameter subgroup $\gamma^{\mathbb{Z}_p}$ for $\gamma \in \mathcal{G}_M$. Thus, we can define a continuous $\mathbb{Q}_p$-linear map

$$\begin{aligned} \log(\gamma) : M &\to M \\ x &\mapsto \log(\gamma)(x) := \sum_{n \geq 1} (-1)^{n-1} \frac{(\gamma - 1)^n}{n} x \end{aligned}$$

for $\gamma \in \mathcal{G}_M$. Moreover, the operators

$$\nabla_0(x) := \frac{\log(\gamma)(x)}{\log(\eta_0(\gamma))} \quad \text{for } \gamma \in \mathcal{G}_M \cap \mathcal{G}_0,$$
$$\nabla_j(x) := \frac{\log(\gamma)(x)}{\eta_j(\gamma)} \quad \text{for } \gamma \in \mathcal{G}_M \cap \mathcal{G}_j$$

for $1 \leq j \leq d$ are independent of the choice of γ.

Assume that N satisfies the conditions of Notation 4.3.1. Then, $M \otimes_R N$ satisfies the conditions of Notation 4.3.1, and we have

$$\log(\gamma \otimes \gamma) = \log(\gamma) \otimes \mathrm{id}_N + \mathrm{id}_M \otimes \log(\gamma) \quad \text{for } \gamma \in \mathcal{G}_M \cap \mathcal{G}_N$$

in $\mathrm{End}_{\mathbb{Q}_p}(M \otimes_R N)$. With $(M, N) = (R, R)$ or (M, R), $\nabla_j : R \to R$ is a continuous derivation and $\nabla_j : M \to M$ is a continuous derivation, compatible with $\nabla_j : R \to R$, that is, $\nabla_j(\lambda x) = \nabla_j(\lambda)x + \lambda \nabla_j(x)$ for $\lambda \in R$ and $x \in M$.

Lemma 4.3.3. *Let the notation be as in Construction 4.3.2. In* $\mathrm{End}_{\mathbb{Q}_p}(M)$, *we have*

$$[\nabla_i, \nabla_j] = -[\nabla_j, \nabla_i] = \begin{cases} \nabla_j & \text{if } i = 0,\ 1 \leq j \leq d, \\ 0 & \text{if } 1 \leq i, j \leq d. \end{cases}$$

Proof. Since $\mathcal{G}_i$ and $\mathcal{G}_j$ are commutative for $1 \leq i, j \leq d$, the assertion in the second case is trivial. We prove the other case. Fix $x \in M$. We regard $\mathcal{G}$ as a subgroup of $\mathrm{GL}_{d+1}(\mathbb{Z}_p)$ as in Section 1.3. For sufficiently small $u_0, u_j \in \mathbb{Z}_p$, put $\gamma_0 := 1 + u_0 E_{1,0} \in \mathcal{G}_0 \cap \mathcal{G}_M$, $\gamma_j := 1 + u_j E_{1,j} \in \mathcal{G}_j \cap \mathcal{G}_M$, where $E_{1,j}$ is the

$(1, j+1)$-th elementary matrix in $M_{d+1}(\mathbb{Z}_p)$. Then, the assertion is equivalent to the equality

$$\log(\gamma_0)\circ\log(\gamma_j)(x)-\log(\gamma_j)\circ\log(\gamma_0)(x)=\log(1+u_0)\log(\gamma_j)x.$$

In the group ring $\mathbb{Q}_p[\mathcal{G}]$, we have

$$\sum_{1\le i\le n}\frac{(-1)^{n-1}}{n}u_0^n u_j E_{1,j}=\sum_{1\le i\le n}\frac{(-1)^{n-1}}{n}(u_0E_{1,1})^n\sum_{1\le i\le n}\frac{(-1)^{n-1}}{n}(u_jE_{1,j})^n$$
$$-\sum_{1\le i\le n}\frac{(-1)^{n-1}}{n}(u_jE_{1,j})^n\sum_{1\le i\le n}\frac{(-1)^{n-1}}{n}(u_0E_{1,1})^n.$$

After applying both sides to x, the LHS converges to $\log(1+u_0)\log(\gamma_j)(x)$ and the RHS converges to $\log(\gamma_0)\circ\log(\gamma_j)(x)-\log(\gamma_j)\circ\log(\gamma_0)(x)$, which implies the assertion. □

In the following, we will use the Fréchet version of Construction 4.3.2.

Construction 4.3.4. Let $(R, \{w_r\})$ be a Fréchet algebra and M a finite free R-module endowed with R-valuations $\{w_r\}$. Assume that $\mathcal{G}$ acts on R and M and assume that the $\mathcal{G}$-actions on $(\widehat{R}_r, w_r)$ and $(\widehat{M}_r, w_r)$ satisfy the conditions of Notation 4.3.1 for all r, where $\widehat{R}_r$ and $\widehat{M}_r$ are the completions of R and M with respect to w_r. By applying Construction 4.3.2 to each $\widehat{R}_r$ and $\widehat{M}_r$ and passing to the limits, we obtain continuous derivations $\nabla_j : R\to R$ and $\nabla_j : M\to M$ for $0\le j\le d$, which are compatible with $\nabla_j : R\to R$, that satisfy

$$[\nabla_0,\nabla_j]=\nabla_j\quad\text{for } 1\le j\le d,\qquad[\nabla_i,\nabla_j]=0\quad\text{for } 1\le i,j\le d.$$

Thus, the actions of $\nabla_0,\dots\nabla_d$ give rise to a differential action of the Lie algebra $\mathrm{Lie}(\mathcal{G})\cong\mathbb{Q}_p\ltimes\mathbb{Q}_p^d$.

4.4. *Differential action and differential conductor of* $\mathbb{N}_{\mathbf{dR}}$. In Section 4.2, we constructed $\mathbb{N}_{\mathrm{dR}}(V)$ for de Rham representations V as a (φ,Γ_K)-module. The aim of this subsection is to endow $\mathbb{N}_{\mathrm{dR}}(V)$ with the structure of (φ,∇)-module in the sense of Definition 1.7.5 by using the results in Section 4.3. As a consequence, we can define the differential Swan conductor of $\mathbb{N}_{\mathrm{dR}}(V)$ (Definition 4.4.9). Throughout this subsection, let V denote a p-adic representation of G_K.

Lemma 4.4.1. *There exists an open normal subgroup $\Gamma_K^o\le_o\Gamma_K$ and $r_K>0$ such that for all $0<r\le r_K$, there exists $c_r>0$ such that*

$$w_r((1-\gamma)x)\ge w_r(x)+c_r,\quad\forall x\in\mathbb{B}_K^{\dagger,r},\forall\gamma\in\Gamma_K^o.$$

Proof. We may assume $x\in\mathbb{A}_K^{\dagger,r}$. Recall that the ring $\Lambda_{m,\mathcal{O}_K}^{(i)}$ is a subring of $\widetilde{\mathbb{A}}_K^{\dagger,r}$ containing $\mathbb{A}_K^{\dagger,r}$ for $m\in\mathbb{N}$ by [Andreatta and Brinon 2008, page 82]. Hence, we only have to prove a similar assertion for $\Lambda^{(i)}_{m,\mathcal{O}_K}$. Then, the assertion follows from [Andreatta and Brinon 2008, Proposition 4.22] if we define Γ^o_K as the closed subgroup of Γ_K topologically generated by $\{\gamma_j^{p^m};\ 0\le j\le d\}$ for sufficiently large m. □

By shrinking Γ^o_K, if necessary, we may assume that Γ^o_K is an open subgroup of $(1+2p\mathbb{Z}_p)\ltimes\mathbb{Z}_p^d$ as in Section 1.3. In the rest of this paper, we assume that r_0 in Notation 4.2.1 is sufficiently small such that $r_0\le r_K$.

Lemma 4.4.2. *For $x\in\widetilde{\mathbb{B}}^{\dagger,r}$ and $c>0$, there exists an open subgroup $U_{x,c}\le_o G_K$ such that*

$$w_r((g-1)x)\ge c\quad \textit{for all } g\in U_{x,c}.$$

Proof. We may assume that x is of the form $[\bar{x}]$ with $\bar{x}\in\widetilde{\mathbb{E}}$. Indeed, if we write $x=\sum_{k\gg-\infty}p^k[x_k]$ with $x_k\in\widetilde{\mathbb{E}}$, then, by definition, there exists N such that $w_r(p^k[x_k])\ge c$ for all $k\ge N$. We choose $U_{x,c}$ such that $w_r((g-1)(p^k[x_k]))\ge c$ for all $k\le N$ and all $g\in U_{x,c}$. Then, $U_{x,c}$ satisfies the condition.

Let $x=[\bar{x}]$ with $\bar{x}\in\widetilde{\mathbb{E}}^{\times}$. Since the action of G_K on $\widetilde{\mathbb{E}}$ is continuous, there exists $U_{x,c}\le_o G_K$ such that $v_{\widetilde{\mathbb{E}}}((g-1)\bar{x})\ge p^{\lfloor c\rfloor}c/r$ (>0) for all $g\in U_{x,c}$. We prove that $U_{x,c}$ satisfies the desired condition. We can write

$$(g-1)[\bar{x}]=[(g-1)\bar{x}]+\sum_{k\ge1}p^k[x_k]$$

for some $x_k\in\widetilde{\mathbb{E}}$. Since

$$[\bar{x}]\big(\big[\frac{(g-1)\bar{x}}{\bar{x}}\big]+1\big)=(g(\bar{x}),-x_1^p,-x_2^{p^2},\dots),$$

$x_k^{p^k}/\bar{x}$ can be written as the value of a polynomial, with coefficients in $\mathbb{Z}$ with zero constant term, at $(g-1)\bar{x}/\bar{x}$. Indeed, let $S_m\in\mathbb{Z}[X_0,\dots,X_m,Y_0,\dots,Y_m]$ for $m\in\mathbb{N}$ be a family of polynomials defining the addition on the ring of Witt vectors, see [Bourbaki 2006, n°3, §1, IX]. Then, S_m is homogeneous of degree p^m, where $\deg(X_i)=\deg(Y_i)=p^i$. Since $S_0=X_0+Y_0$ and $\sum_{0\le i\le m}p^iS_i^{p^{m-i}}=\sum_{0\le i\le m}p^iX_i^{p^{m-i}}+\sum_{0\le i\le m}p^iY_i^{p^{m-i}}$ for $m\ge1$, the coefficients of both $X_0^{p^m}$, $Y_0^{p^m}\in S_m$ are equal to zero, which implies the assertion. Hence, for $n\in\mathbb{N}$, we have

$$\begin{aligned}v^{\le n}_{\widetilde{\mathbb{E}}}((g-1)[\bar{x}])&=\inf_{1\le k\le n}\big\{v_{\widetilde{\mathbb{E}}}((g-1)\bar{x}),\,v_{\widetilde{\mathbb{E}}}(x_k)\big\}\\&\ge\inf_{1\le k\le n}\Big\{v_{\widetilde{\mathbb{E}}}((g-1)\bar{x}),\,\frac{1}{p^k}v_{\widetilde{\mathbb{E}}}((g-1)\bar{x})\Big\}=\frac{1}{p^n}v_{\widetilde{\mathbb{E}}}((g-1)\bar{x}).\end{aligned}$$

Note that $v^{\le n}_{\widetilde{\mathbb{E}}}\big((g-1)[\bar{x}]\big)=\infty$ for $n\in\mathbb{Z}_{<0}$. Hence, we have $w_r((g-1)[\bar{x}])=\inf_{n\in\mathbb{N}}(rv^{\le n}_{\widetilde{\mathbb{E}}}((g-1)[\bar{x}])+n)\ge\inf(r\cdot\frac{1}{p^{\lfloor c\rfloor}}v_{\widetilde{\mathbb{E}}}((g-1)\bar{x}),\lfloor c\rfloor)\ge c$, which implies the assertion. □

Lemma 4.4.3. *Let $\{e_i\}$ be a $\mathbb{B}^{\dagger,r}_K$-basis of $\mathbb{D}^{\dagger,r}(V)$. We endow $\mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V)$ with valuations $\{w_s\}_{0<s\le r}$ that are compatible with the $\{w_s\}_{0<s\le r}$ associated to $\{e_i\}$. Then, the actions of Γ^o_K on $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ and $\mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V)$ satisfy the conditions of Notation 4.3.1.*

Proof. Conditions (i) and (ii) follow from the definition. Condition (iii) follows from the formula $\gamma^p - 1 = \sum_{1\le i\le p}\binom{p}{i}(\gamma-1)^i$ and Lemma 4.4.1. To prove condition (iv), we may assume $x \in \mathbb{D}^{\dagger,r}(V)$. We choose a lattice T of V stable under the G_K-action. Let $\{f_i\}$ be a basis of T and endow $\widetilde{\mathbb{B}}^{\dagger,r} \otimes_{\mathbb{Q}_p} V$ with the valuations $\{w'_s\}_{0<s\le r}$, compatible with the $\{w_s\}_{0<s\le r}$, associated to the $\widetilde{\mathbb{B}}^{\dagger,r}$-basis $\{1\otimes f_i\}$. By the canonical isomorphism $\mathbb{B}^{\dagger,r}\otimes_{\mathbb{B}^{\dagger,r}_K}\mathbb{D}^{\dagger,r}(V)\cong\mathbb{B}^{\dagger,r}\otimes_{\mathbb{Q}_p} V$ following from Theorem 1.10.5, we regard $\{1\otimes e_i\}$ as a $\mathbb{B}^{\dagger,r}$-basis of $\mathbb{B}^{\dagger,r}\otimes_{\mathbb{Q}_p} V$. Then, w_s is equivalent to w'_s; therefore, we only have to prove that for any $x \in \widetilde{\mathbb{B}}^{\dagger,r}\otimes_{\mathbb{Q}_p} V$ and $0 < s \le r$, there exists an open subgroup $G^o_{K,s,x} \le_o G_K$ such that $w'_s((g-1)x) \ge w'_s(x) + w'_s(p)$ for all $g \in G^o_{K,s,x}$. We may assume that x is of the form $\lambda\otimes v$ for $\lambda \in \widetilde{\mathbb{B}}^{\dagger,r}$ and $v \in T$. Since the action of G_K on T is continuous, there exists an open subgroup $U \le_o G_K$ such that U acts trivially on T/pT. We apply Lemma 4.4.2 after regarding $\lambda \in \widetilde{\mathbb{B}}^{\dagger,s}$, and get that there exists an open subgroup $U' \le_o G_K$ such that $w_s((g-1)\lambda) \ge w_s(\lambda) + w_s(p)$ for all $g \in U'$. If we put $G^o_{K,s,x} := U \cap U'$, then the assertion follows from

$$(g-1)(\lambda\otimes v) = (g-1)(\lambda)\otimes g(v) + \lambda\otimes(g-1)v. \qquad \square$$

Definition 4.4.4. By Lemma 4.4.3, we can apply Construction 4.3.4 to $\mathcal{G} = \Gamma_K$, $R = \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ and $M = \mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V)$. Thus, we obtain continuous differentials operators ∇_j on $\mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V)$ for $0 \le j \le d$. The operator ∇_j induces a continuous differential operator on $\mathbb{D}^{\dagger}_{\mathrm{rig}}(V)$, which is denoted by ∇_j again. Since the actions of Γ_K and φ commute, ∇_j commutes with φ by definition.

Until otherwise stated, let $V = \mathbb{Q}_p$ and regard $\mathbb{D}^{\dagger,r}_{\mathrm{rig}}(\mathbb{Q}_p)$ as $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. Then, ∇_j can be regarded as a continuous derivation on $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$. In the following, we will describe this derivation explicitly.

Construction 4.4.5. As in [Andreatta and Brinon 2010, Propostion 4.3], the action of Γ_K on $K_n[[t, u_1, \dots, u_d]]$ induces K_n-linear differentials

$$\widetilde{\nabla}_0 := \frac{\log(\gamma_0)}{\log(\eta_0(\gamma_0))} = t(1+\pi)\frac{\partial}{\partial\pi},$$
$$\widetilde{\nabla}_j := \frac{\log(\gamma_j)}{\eta_j(\gamma_j)} = -t[\tilde{t}_j]\frac{\partial}{\partial u_j} \quad \text{for } 1 \le j \le d$$

for all sufficiently small $\gamma_0 \in \Gamma_{K,0}$ and $\gamma_j \in \Gamma_{K,j}$. Note that these are continuous with respect to the canonical topology. Since the action of Γ_K commutes with ∇^{geom} by definition, $\widetilde{\nabla}_j$ acts on $K_n[[t, u_1, \dots, u_d]]^{\nabla}$.

We assume $K = \widetilde{K}$ until otherwise stated. By the isomorphism $\mathbb{A}_K^{\dagger,r} \cong \mathcal{O}((\pi))^{\dagger,r}$, we have derivations

$$\partial_0 := \frac{\partial}{\partial \pi},\ \partial_1 := \frac{\partial}{\partial[\tilde{t}_1]}, \ldots,\ \partial_d := \frac{\partial}{\partial[\tilde{t}_d]},$$

on $\mathbb{A}_K^{\dagger,r}$ (see Section 1.7), which are continuous with respect to the Fréchet topology defined by $\{w_s\}_{0<s\leq r}$. By passing to the completion, we obtain continuous derivations $\partial_j : \mathbb{B}^{\dagger,r}_{\mathrm{rig},K} \to \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ for $0 \leq j \leq d$. The derivation ∂_j also extends to a derivation $\partial_j : \mathbb{B}^{\dagger}_{\mathrm{rig},K} \to \mathbb{B}^{\dagger}_{\mathrm{rig},K}$. By Lemma 4.2.7, we may regard $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ as a dense subring of $K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla}$ via ι_n. Hence, we can extend any continuous derivation ∂ on $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ to a continuous derivation on $K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla}$, which is denoted by $\iota_n(\partial)$. Note that we have a formula

$$\iota_n(\partial)(\iota_n(x)) = \iota_n(\partial(x)) \text{ for } x \in \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}. \tag{7}$$

Lemma 4.4.6. *For $n \geq n(r)$, we have*

$$\iota_n(t(1+\pi)\partial_0) = \widetilde{\nabla}_0, \quad \iota_n(t[\tilde{t}_j]\partial_j) = \widetilde{\nabla}_j \ \textit{for } 1 \leq j \leq d.$$

Proof. Let $1 \leq j \leq d$ and put $\delta_0 := \iota_n(t(1+\pi)\partial_0) - \widetilde{\nabla}_0$ and $\delta_j := \iota_n(t[\tilde{t}_j]\partial_j) - \widetilde{\nabla}_j$. Let $f : K_n[\![t, u_1, \ldots, u_d]\!] \to K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla}$ be the map defined in the proof of Lemma 4.1.4, which is continuous by Lemma 4.1.6. Since f induces a surjection on the residue fields by definition, $f(K_n[t])$ is a dense subring of $K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla}$ by Lemmas 4.1.4 and 4.1.5. Hence, we only have to prove that $\delta_0 \circ f(K_n[t]) = \delta_j \circ f(K_n[t]) = 0$. We view $\delta_0 \circ f|_{K_n},\ \delta_j \circ f|_{K_n} \in \mathrm{Der}_{\mathrm{cont}}(K_n, K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla})$, which is isomorphic to $\mathrm{Hom}_{K_n}(\widehat{\Omega}^1_{K_n}, K_n[\![t, u_1, \ldots, u_d]\!]^{\nabla})$ by Lemma 1.2.3. Since $\widehat{\Omega}^1_{K_n} \cong K_n \otimes_K \widehat{\Omega}^1_K$ has a K_n-basis $\{dt_i;\ 1 \leq i \leq d\}$ and since we have $f(t) = t$ and $f(t_i) = [\tilde{t}_i]$ by definition, we only have to prove $\delta_0(t) = \delta_j(t) = 0$ and $\delta_0([\tilde{t}_i]) = \delta_j([\tilde{t}_i]) = 0$ for all $1 \leq i \leq d$. By using formula (7), we get

$$\iota_n(t(1+\pi)\partial_0)(t) = t = \widetilde{\nabla}_0(t), \quad \iota_n(t(1+\pi)\partial_0)[\tilde{t}_i] = 0,$$
$$\iota_n(t[\tilde{t}_j]\partial_j)(t) = 0 = \widetilde{\nabla}_j(t), \quad \iota_n(t[\tilde{t}_j]\partial_j)[\tilde{t}_i] = \delta_{ij} t[\tilde{t}_j]$$

for all $1 \leq i \leq d$. Since $(\partial/\partial u_j)[\tilde{t}_i] = -(\partial/\partial u_j)u_i = -\delta_{ij}$ for all $1 \leq i \leq d$, we obtain the assertion. □

For the rest of this section, we drop the assumptions $K = \widetilde{K}$ and $V = \mathbb{Q}_p$.

Corollary 4.4.7. *The derivation*

$$d' : \mathbb{B}^{\dagger}_{\mathrm{rig},K} \to \Omega^1_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}$$
$$x \mapsto \nabla_0(x)\frac{1}{t(1+\pi)}d\pi + \sum_{1\leq j\leq d} \nabla_j(x)\frac{1}{t}d[\tilde{t}_j]$$

coincides with the canonical derivation $d : \mathbb{B}^{\dagger}_{\mathrm{rig},K} \to \Omega^1_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}$.

Proof. Since the canonical map $\mathbb{B}^{\dagger}_{\mathrm{rig},\widetilde{K}} \to \mathbb{B}^{\dagger}_{\mathrm{rig},K}$ is finite étale by [Kedlaya 2005, Proposition 2.4.10], we can reduce to the case $K = \widetilde{K}$. Let the notation be as in Lemma 4.4.6. Obviously, ∇_j extends to $\widetilde{\nabla}_j$ by passing to the completion. Since ι_n is injective, we have

$$\nabla_0 = t(1+\pi)\partial_0, \quad \nabla_j = t[\tilde{t}_j]\partial_j \text{ for } 1 \le j \le d.$$

as derivations of $\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$ by Lemma 4.4.6, which implies the assertion. □

Lemma 4.4.8. *Let $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$.*

(i) *We have $\nabla_j(\mathbb{N}_{\mathrm{dR}}(V)) \subset t\mathbb{N}_{\mathrm{dR}}(V)$ for all $0 \le j \le d$. We put $\nabla'_j := 1/t\nabla_j$, which is a continuous differential operator on $\mathbb{N}_{\mathrm{dR}}(V)$.*

(ii) *For all $0 \le i, j \le d$, we have*

$$[\nabla'_i, \nabla'_j] = 0$$

(iii) *For all $0 \le i, j \le d$, we have*

$$\nabla'_j \circ \varphi = p\varphi \circ \nabla'_j$$

Proof.

(i) By Tate twist, we may assume that the Hodge–Tate weights of V are sufficiently small. Let the notation be as in Construction 4.4.5 and Proposition 4.2.12 (with $B = \mathbb{B}^{\dagger,r}_{\mathrm{rig},K}$). By viewing $t\mathbb{N}_{\mathrm{dR},r}(V)$ and $t\mathbb{D}_{\mathrm{dR}}(V)$ as $\mathbb{N}_{\mathrm{dR},r}(V(1))$ and $\mathbb{D}_{\mathrm{dR}}(V(1))$, respectively, we only have to prove that $\iota_n(\nabla_j(x)) \in tD_n$ for all $n \ge n(r)$ and $x \in \mathbb{N}_{\mathrm{dR},r}(V)$. For sufficiently small $\gamma_j \in \Gamma_{K,j}$, we have $\iota_n \circ \log(\gamma_j)(x) = \log(\gamma_j)(\iota_n(x))$ and $\iota_n(x) \in D_n \subset B_n \otimes_K \mathbb{D}_{\mathrm{dR}}(V)$. Since Γ_K acts trivially on $\mathbb{D}_{\mathrm{dR}}(V)$, $\log(\gamma_j)$ acts on $B_n \otimes_K \mathbb{D}_{\mathrm{dR}}(V)$ as $\log(\gamma_j) \otimes 1$. Since $\log(\gamma_j)(B_n) \subset tB_n$ (see Construction 4.4.5), we have $\iota_n \circ \log(\gamma_j)(x) \in (B_n \otimes_K \mathbb{D}_{\mathrm{dR}}(V(1)))^{\nabla^{\mathrm{geom}}=0} = tD_n$, which implies the assertion.

(ii) This follows from a straightforward calculation using Lemma 4.3.3, $\nabla_0(t) = t$, and $\nabla_i(t) = \nabla_j(t) = 0$.

(iii) Since ∇_j commutes with φ, we have $t\nabla'_j \circ \varphi = \nabla_j \circ \varphi = \varphi \circ \nabla_j = \varphi(t)\varphi \circ \nabla'_j = pt\varphi \circ \nabla'_j$. By dividing by t, we obtain the assertion since $\mathbb{N}_{\mathrm{dR}}(V)$ is torsion free. □

Definition 4.4.9. Let the notation be as in Lemma 4.4.8. For $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$, put

$$\nabla : \mathbb{N}_{\mathrm{dR}}(V) \to \mathbb{N}_{\mathrm{dR}}(V) \otimes_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}} \Omega^1_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}$$

$$x \mapsto \nabla'_0(x) \otimes \frac{1}{1+\pi} d\pi + \sum_{1 \le j \le d} \nabla'_j(x) \otimes d[\tilde{t}_j],$$

which defines a ∇-structure on $\mathbb{N}_{\mathrm{dR}}(V)$ by Corollary 4.4.7. Furthermore, this ∇-structure is compatible with the φ-structure on $\mathbb{N}_{\mathrm{dR}}(V)$ by Lemma 4.4.8(iii) and $\varphi((1+\pi)^{-1}d\pi) = p(1+\pi)^{-1}d\pi$ and $\varphi(d[\tilde{t}_j]) = pd[\tilde{t}_j]$. Thus, $\mathbb{N}_{\mathrm{dR}}(V)$ is endowed with a (φ, ∇)-module structure and we obtain the differential Swan conductor $\mathrm{Swan}^{\nabla}(\mathbb{N}_{\mathrm{dR}}(V))$ of $\mathbb{N}_{\mathrm{dR}}(V)$. The slope filtration of $\mathbb{N}_{\mathrm{dR}}(V)$ as a (φ, ∇)-module (Theorem 1.7.6) is Γ_K-stable by the commutativity of the Γ_K- and φ-actions, and the uniqueness of the slope filtration ([Kedlaya 2007, Theorem 6.4.1]).

4.5. ***Comparison of pure objects.*** In this subsection, we will study "pure" objects in various categories.

Notation 4.5.1. Let G be a topological group and R a topological ring on which G acts. Let $\phi : R \to R$ be a continuous ring homomorphism that commutes with the action of G. A (ϕ, G)-module over R is a finite free R-module with continuous and semilinear action of G and a semilinear endomorphism ϕ, both of which are commutative. We denote the category of (ϕ, G)-modules over R by $\mathrm{Mod}_R(\phi, G)$. The morphisms in $\mathrm{Mod}_R(\phi, G)$ consist of R-linear maps commuting with ϕ and G.

Definition 4.5.2 [Berger 2008a, Definition 3.2.1]. Let $h \geq 1$ and $a \in \mathbb{Z}$ be relatively prime. Let $\mathrm{Rep}_{a,h}(G_K)$ be the category with objects $V_{a,h} \in \mathrm{Rep}_{\mathbb{Q}_{p^h}}(G_K)$, endowed with a semilinear Frobenius action $\varphi : V_{a,h} \to V_{a,h}$ that commutes with the G_K-action such that $\varphi^h = p^a$. The morphisms of this category are $\mathbb{Q}_{p^h}$-linear maps that commute with (φ, G_K)-actions. When $h = 1$ and $a = 0$, $\mathrm{Rep}_{a,h}(G_K) = \mathrm{Rep}_{\mathbb{Q}_p}(G_K)$.

Let $s := a/h \in \mathbb{Q}$. We denote by $D_{[s]}$ the $\mathbb{Q}_p$-vector space $\bigoplus_{1 \leq i \leq h} \mathbb{Q}_p e_i$ endowed with a trivial G_K-action and with φ-actions via $\varphi(e_i) := e_{i+1}$ if $i \neq h$ and $\varphi(e_h) := p^a e_1$. Then, $\mathbb{Q}_{p^h} \otimes_{\mathbb{Q}_p} D_{[s]}$ belongs to $\mathrm{Rep}_{a,h}(G_K)$.

Definition 4.5.3. For $s \in \mathbb{Q}$, we define

$$\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^\dagger_{\mathrm{rig}}}(\varphi, G_K), \quad \mathrm{Mod}^s_{\mathbb{B}^\dagger_{\mathrm{rig},K}}(\varphi, \Gamma_K), \quad \mathrm{Mod}^s_{\widetilde{\mathbb{B}}^\dagger}(\varphi, G_K), \quad \mathrm{Mod}^s_{\mathbb{B}^\dagger_K}(\varphi, \Gamma_K)$$

to be the full subcategories of $\mathrm{Mod}_{\widetilde{\mathbb{B}}^\dagger_{\mathrm{rig}}}(\varphi, G_K)$, $\mathrm{Mod}_{\mathbb{B}^\dagger_{\mathrm{rig},K}}(\varphi, \Gamma_K)$, $\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^\dagger}(\varphi, G_K)$ and $\mathrm{Mod}^s_{\mathbb{B}^\dagger_K}(\varphi, \Gamma_K)$, whose objects are pure of slope s as φ-modules.

Lemma 4.5.4. (i) *For any $r > 0$, there exists a canonical injection*

$$\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \to \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}},$$

which is (φ, G_K)-equivariant. In the following, we regard $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$ as a subring of $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$ and we endow $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$ with a Fréchet topology induced by the family of valuations $\{w_r\}_{r>0}$.

(ii) *For $h \in \mathbb{N}_{>0}$,*

$$(\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}})^{\varphi^h=1} = (\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}})^{\varphi^h=1} = \mathbb{Q}_{p^h}.$$

Proof. By definition, $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$ and $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$ depend only on $\mathbb{C}_p$ and not on K. By regarding $\mathbb{C}_p$ as the p-adic completion of the algebraic closure of K^{pf}, we can reduce to the perfect residue field case. Assertion (i) follows from [Berger 2002, Exemple 2.8(2), Definition 2.16]. Assertion (ii) for $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$ is due to Colmez, see [Ohkubo 2013, Lemma 6.2], and (ii) for $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$ is a consequence of [Berger 2002, Proposition 3.2]. □

Definition 4.5.5. For $s\in\mathbb{Q}$, an object $M\in\mathrm{Mod}_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}}(\varphi,G_K)$ is said to be pure of slope s if M is isomorphic to $(\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}\otimes_{\mathbb{Q}_p}D_{[s]})^m$ as a φ-module for some $m\in\mathbb{N}$. Denote by $\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}}(\varphi,G_K)$ the category of (φ,G_K)-modules over $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$, which are pure of slope s.

Lemma 4.5.6. *Let the notation be as in Notation 1.6.2 and Definition 1.7.5. For $s\in\mathbb{Q}$, the forgetful functor*

$$\mathrm{Mod}^s_{\mathcal{R}}(\varphi,\nabla)\to\mathrm{Mod}^s_{\mathcal{R}}(\varphi).$$

is fully faithful.

Proof. We consider the following commutative diagram

$$\begin{array}{ccc}
\mathrm{Mod}^s_{\Gamma[1/p]}(\varphi,\nabla) & \xrightarrow{\alpha_1} & \mathrm{Mod}^s_{\Gamma[1/p]}(\varphi)\\
\beta_1\uparrow & & \uparrow\gamma_1\\
\mathrm{Mod}^s_{\Gamma^\dagger[1/p]}(\varphi,\nabla) & \xrightarrow{\alpha_2} & \mathrm{Mod}^s_{\Gamma^\dagger[1/p]}(\varphi)\\
\beta_2\downarrow & & \downarrow\gamma_2\\
\mathrm{Mod}^s_{\mathcal{R}}(\varphi,\nabla) & \xrightarrow{\alpha_3} & \mathrm{Mod}^s_{\mathcal{R}}(\varphi)
\end{array}$$

where $\alpha_\bullet$ is a forgetful functor, and $\beta_\bullet$ and $\gamma_\bullet$ are base change functors. We first note that γ_1 (resp. γ_2) is fully faithful (resp. an equivalence) by [Kedlaya 2005, Theorem 6.3.3(a)] (resp. [Kedlaya 2005, Theorem 6.3.3(b)]). Let $M,N\in\mathrm{Mod}^s_{\Gamma^\dagger[1/p]}(\varphi,\nabla)$ and let $\widehat{M},\widehat{N}$ be the base changes of M,N via the canonical map $\Gamma^\dagger[1/p]\to\Gamma[1/p]$. Then, we have

$$\begin{aligned}\mathrm{Hom}_{\mathrm{Mod}^s_{\Gamma^\dagger[1/p]}(\varphi,\nabla)}(M,N)&=\mathrm{Hom}_{\Gamma^\dagger[1/p]}(M,N)^{\varphi=1,\nabla=0}\\&=\mathrm{Hom}_{\Gamma[1/p]}(\widehat{M},\widehat{N})^{\varphi=1,\nabla=0},\end{aligned}$$

where the first equality follows by definition and the second equality follows because γ_1 is fully faithful. Therefore, β_1 is fully faithful. For the same reason, since γ_2 is fully faithful, so is β_2. Note that α_1 is an equivalence in the étale case, i.e., $s=0$ ([Kedlaya 2007, Proposition 3.2.8]). Let $M,N\in\mathrm{Mod}^s_{\Gamma[1/p]}(\varphi,\nabla)$. Since $\mathrm{Hom}_{\Gamma[1/p]}(M,N)\cong M^\vee\otimes_{\Gamma[1/p]}N$ can be regarded as an étale (φ,∇)-module over

$\Gamma[1/p]$, where $M^\vee$ denotes the dual of M, we have

$$\begin{aligned}\mathrm{Hom}_{\mathrm{Mod}^s_{\Gamma[1/p]}(\varphi,\nabla)}(M,N)&=\mathrm{Hom}_{\Gamma[1/p]}(M,N)^{\varphi=1,\nabla=0}=\mathrm{Hom}_{\Gamma[1/p]}(M,N)^{\varphi=1}\\&=\mathrm{Hom}_{\mathrm{Mod}^s_{\Gamma[1/p]}(\varphi)}(M,N),\end{aligned}$$

where the first and third equalities follow from the definition and the second equality follows since α_1 is fully faithful in the étale case. Therefore, α_1 is an equivalence. Since α_1, β_1 and γ_1 are fully faithful, so is α_2. Since α_2, β_2 and γ_2 are fully faithful, so is α_3. □

Lemma 4.5.7. *Let $s\in\mathbb{Q}$ and let $h\in\mathbb{N}_{\geq 1}$, $a\in\mathbb{Z}$ be relatively prime with $s=a/h$.*

(i) *There exist equivalences of categories*

$$\begin{aligned}
\widetilde{\mathbb{D}}^{\nabla+}_{\mathrm{rig}}&:\mathrm{Rep}_{a,h}(G_K)\to\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}}(\varphi,G_K);\quad V_{a,h}\mapsto\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}\otimes_{\mathbb{Q}_{p^h}}V_{a,h},\\
\widetilde{\mathbb{D}}^{\dagger}_{\mathrm{rig}}&:\mathrm{Rep}_{a,h}(G_K)\to\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}}(\varphi,G_K);\quad V_{a,h}\mapsto\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}\otimes_{\mathbb{Q}_{p^h}}V_{a,h},\\
\mathbb{D}^{\dagger}_{\mathrm{rig}}&:\mathrm{Rep}_{a,h}(G_K)\to\mathrm{Mod}^s_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}(\varphi,\Gamma_K);\quad V_{a,h}\mapsto\mathbb{B}^{\dagger}_{\mathrm{rig},K}\otimes_{\mathbb{B}^{\dagger}_K}(\mathbb{B}^{\dagger}\otimes_{\mathbb{Q}_{p^h}}V_{a,h})^{H_K},\\
\widetilde{\mathbb{D}}^{\dagger}&:\mathrm{Rep}_{a,h}(G_K)\to\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\dagger}}(\varphi,G_K);\quad V_{a,h}\mapsto\widetilde{\mathbb{B}}^{\dagger}\otimes_{\mathbb{Q}_{p^h}}V_{a,h},\\
\mathbb{D}^{\dagger}&:\mathrm{Rep}_{a,h}(G_K)\to\mathrm{Mod}^s_{\mathbb{B}^{\dagger}_K}(\varphi,\Gamma_K);\quad V_{a,h}\mapsto(\mathbb{B}^{\dagger}\otimes_{\mathbb{Q}_{p^h}}V_{a,h})^{H_K}.
\end{aligned}$$

More precisely, quasi-inverses of $\widetilde{\mathbb{D}}^{\nabla+}_{\mathrm{rig}}$, $\widetilde{\mathbb{D}}^{\dagger}_{\mathrm{rig}}$ and $\widetilde{\mathbb{D}}^{\dagger}$ are given by $M\mapsto M^{\varphi^h=p^a}$.

(ii) *We denote by α_i for $1\leq i\leq 5$ the following canonical morphisms of rings:*

$$\begin{array}{ccccc}
\mathbb{B}^{\dagger}_K & \xrightarrow{\alpha_1} & \mathbb{B}^{\dagger}_{\mathrm{rig},K} & & \\
\downarrow{\scriptstyle\alpha_2} & & \downarrow{\scriptstyle\alpha_4} & & \\
\mathbb{B}^{\dagger}_{\mathrm{rig}} & \xrightarrow{\alpha_3} & \widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} & \xleftarrow{\alpha_5} & \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}},
\end{array}$$

where the left square is commutative. Then, the α_i's induce the following base change functors $\alpha^*_\bullet$:

$$\begin{array}{ccccc}
\mathrm{Mod}^s_{\mathbb{B}^{\dagger}_K}(\varphi,\Gamma_K) & \xrightarrow{\alpha_1^*} & \mathrm{Mod}^s_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}(\varphi,\Gamma_K) & & \\
\downarrow{\scriptstyle\alpha_2^*} & & \downarrow{\scriptstyle\alpha_4^*} & & \\
\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\dagger}}(\varphi,G_K) & \xrightarrow{\alpha_3^*} & \mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}}(\varphi,G_K) & \xleftarrow{\alpha_5^*} & \mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}}(\varphi,G_K),
\end{array}$$

where the left square is commutative. Moreover, the functors $\alpha^*_\bullet$'s are compatible with the functor defined in (i), i.e., $\alpha_1^*\circ\mathbb{D}^{\dagger}=\mathbb{D}^{\dagger}_{\mathrm{rig}}$, etc. In particular, the $\alpha^*_\bullet$'s are equivalences.

Proof.

(i) We prove the assertion for $\widetilde{\mathbb{D}}^{\nabla+}_{\mathrm{rig}}$. Let $\mathcal{D} := \widetilde{\mathbb{D}}^{\nabla+}_{\mathrm{rig}}$ and let $\mathcal{V}$ be, as before, the functor in the other direction. Let $V \in \mathrm{Rep}_{a,h}(G_K)$. Then, there exists a functorial morphism $V \to \mathcal{V} \circ \mathcal{D}(V)$, which is bijective by Lemma 4.5.4(ii). Hence, we have a natural equivalence $\mathcal{V}\circ\mathcal{D} \simeq \mathrm{id}$. For $M \in \mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}}(\varphi, G_K)$, we get a functorial morphism $\mathcal{D} \circ \mathcal{V}(M) \to M$ that is bijective by the isomorphism $M \cong (\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} D_{[s]})^m$ of φ-modules and Lemma 4.5.4(ii). Hence, we have a natural equivalence $\mathcal{D} \circ \mathcal{V} \simeq \mathrm{id}$.

The assertions for $\widetilde{\mathbb{D}}^{\dagger}_{\mathrm{rig}}$ and $\widetilde{\mathbb{D}}^{\dagger}$ follow similarly: instead of using the isomorphism $M \cong (\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} D_{[s]})^m$, we use Kedlaya's Dieudonné–Manin decomposition theorems over $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}$ and $\widetilde{\mathbb{B}}^{\dagger}$, see Propositions 4.5.3 and 4.5.10 and Definition 4.6.1; Theorem 6.3.3(b) of [Kedlaya 2005], respectively. These assert that any object M in $\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}}(\varphi)$ or $\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\dagger}}(\varphi)$ is isomorphic to a direct sum of $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} D_{[s]}$ or of $\widetilde{\mathbb{B}}^{\dagger} \otimes_{\mathbb{Q}_p} D_{[s]}$, respectively.

We next prove the assertion for $\mathbb{D}^{\dagger}$. For $M \in \mathrm{Mod}^s_{\mathbb{B}^{\dagger}_K}(\varphi, \Gamma_K)$, let $\mathcal{V}(M) := (\mathbb{B}^{\dagger} \otimes_{\mathbb{B}^{\dagger}_K} M)^{\varphi^h = p^a}$. We will check that $\mathcal{V}$ gives a quasi-inverse of $\mathbb{D}^{\dagger}$. Let $V_{a,h} \in \mathrm{Rep}_{a,h}(G_K)$. By forgetting the action of φ on $V_{a,h}$ and applying Theorem 1.10.5 to $V = V_{a,h}$, we get a canonical bijection $\mathbb{B}^{\dagger} \otimes_{\mathbb{B}^{\dagger}_K} \mathbb{D}^{\dagger}(V_{a,h}) \to \mathbb{B}^{\dagger} \otimes_{\mathbb{Q}_{p^h}} V_{a,h}$. Since this map is φ-equivariant, we have canonical isomorphisms $\mathcal{V} \circ \mathbb{D}^{\dagger}(V_{a,h}) \cong (\mathbb{B}^{\dagger})^{\varphi^h=1} \otimes_{\mathbb{Q}_{p^h}} V_{a,h} \cong V_{a,h}$ by Lemma 4.5.4(ii). Thus, we obtain a natural equivalence $\mathcal{V} \circ \mathbb{D}^{\dagger} \simeq \mathrm{id}$. We prove $\mathbb{D}^{\dagger} \circ \mathcal{V} \simeq \mathrm{id}$. Let $M \in \mathrm{Mod}^s_{\mathbb{B}^{\dagger}_K}(\varphi, \Gamma_K)$. From [Kedlaya 2005, Proposition 6.3.5], we obtain the existence of an $\mathbb{A}^{\dagger}_K$-lattice N of M such that $p^{-a}\varphi^h$ maps some basis of N to another basis of N. Let M' denote M with the φ^h-action given by $x \mapsto p^{-a}\varphi^h(x)$ and with the same Γ_K-action as M. By the existence of the above lattice N, we have $M' \in \mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}^{\dagger}_K}(\varphi^h, \Gamma_K)$. Since we have G_K-equivariant isomorphisms $\mathcal{V}(M) = (\mathbb{B}^{\dagger} \otimes_{\mathbb{B}^{\dagger}_K} M)^{\varphi^h = p^a} \cong (\mathbb{B}^{\dagger} \otimes_{\mathbb{B}^{\dagger}_K} M')^{\varphi^h=1} = \mathbb{V}(M')$, the assertion follows from the étale case (Theorem 1.10.5).

Finally, we prove the assertion for $\mathbb{D}^{\dagger}_{\mathrm{rig}}$. By the base change equivalence

$$\alpha_1^* : \mathrm{Mod}^s_{\mathbb{B}^{\dagger}_K}(\varphi) \to \mathrm{Mod}^s_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}(\varphi),$$

see [Kedlaya 2005, Theorem 6.3.3(b)], we also have the base change equivalence $\alpha_1^* : \mathrm{Mod}^s_{\mathbb{B}^{\dagger}_K}(\varphi, \Gamma_K) \to \mathrm{Mod}^s_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}(\varphi, \Gamma_K)$. Hence, the assertion follows from the $\mathbb{D}^{\dagger}$-case.

(ii) To check that the $\alpha_{\bullet}^*$'s are well-defined, we have only to prove that pure objects are preserved by base change. For α_1 and α_3, this follows from [Kedlaya 2005, Theorem 6.3.3(b)]. For α_2, α_4, this follows from the definitions: $M \in \mathrm{Mod}_{\mathbb{B}^{\dagger}_K}(\varphi)$ and $\mathrm{Mod}_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}}(\varphi)$ are pure if $\widetilde{\mathbb{B}}^{\dagger} \otimes_{\mathbb{B}^{\dagger}_K} M$ and $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} \otimes_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}} M$, respectively, are pure by [Kedlaya 2005, Definitions 4.6.1 and 6.3.1] . For α_5, it follows from [Kedlaya 2005, Proposition 4.5.10 and Definition 4.6.1].

The commutativity of the diagram is trivial. The compatibility follows from the definition. □

4.6. ***Swan conductor for de Rham representations.*** In this subsection, we define Swan conductors of de Rham representations. In this subsection, Assumption 1.9.1 is not necessary since we do not use the results of [Andreatta and Brinon 2008].

We first recall the canonical slope filtration associated to a Dieudonné–Manin decomposition.

Definition 4.6.1 [Colmez 2008b, Remarque 3.3]. A φ-module M over $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$ is a finite free $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$-module together with a semilinear φ-action. A φ-module M over $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$ admits a Dieudonné–Manin decomposition if there exists an isomorphism $f : M \cong \bigoplus_{1\le i\le m} \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} D_{[s_i]}$ of φ-modules over $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$ with $s_1 \le \cdots \le s_m \in \mathbb{Q}$. We define the slope multiset of M as the multiset of cardinality $\mathrm{rank}(M)$, consisting of the s_i, together with its multiplicity $\dim_{\mathbb{Q}_p} D_{[s_i]}$. Let $s'_1 < \cdots < s'_{r'}$ be the distinct elements in the slope multiset of M. Then, we define $\mathrm{Fil}^0_f(M) := 0$ and $\mathrm{Fil}^i_f(M) := f^{-1}(\bigoplus_{j;s_j\le s'_i} \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} D_{[s_j]})$ for $1 \le i \le r'$. Note that the filtration and the slope multiset are independent of the choice of f above.

Definition 4.6.2. Let $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$. First, we assume that the Hodge–Tate weights of V are negative. By assumption, we have $\mathbb{D}_{\mathrm{dR}}(V) = (\mathbb{B}^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}$. As in [Ohkubo 2013, Proposition 5.3], we define

$$\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V) := \{x \in \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V;\ \iota_n(x) \in (\mathbb{B}^+_{\mathrm{dR}} \otimes_K \mathbb{D}_{\mathrm{dR}}(V))^{\nabla^{\mathrm{geom}}=0} \text{ for all } n \in \mathbb{Z}\},$$

where $\iota_n : \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V \to \mathbb{B}^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$ is defined by $x \otimes v \mapsto \varphi^{-n}(x) \otimes v$. Since $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)$ admits a Dieudonné–Manin decomposition due to Colmez ([Ohkubo 2013, Proposition 6.2]), $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)$ is endowed with a canonical slope filtration $\mathrm{Fil}^\bullet(\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V))$ of φ-modules by Definition 4.6.1. Let $s_1 < \cdots < s_r$ be the distinct elements in the slope multiset of $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)$. Write $s_i = a_i/h_i$ with $a_i \in \mathbb{Z}$, $h_i \in \mathbb{N}_{>0}$ relatively prime. By the uniqueness of slope filtrations, Fil^i is G_K-stable and the graded piece $\mathrm{gr}^i(\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V))$ lies in $\mathrm{Mod}^{s_i}_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}}(\varphi, G_K)$. Hence, by Lemma 4.5.7, there exists a unique $\mathcal{V}_i \in \mathrm{Rep}_{a_i,h_i}(G_K)$, up to isomorphism, such that $\mathrm{gr}^i(\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)) \cong \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_{p^{h_i}}} \mathcal{V}_i$. It is proved in Step 1 of the proof of the main theorem of [Ohkubo 2013] that the inertia I_K acts on $\mathcal{V}_i$ via a finite quotient, i.e., $\mathcal{V}_i \in \mathrm{Rep}^{f.g.}_{\mathbb{Q}_{p^{h_i}}}(G_K)$ (in the reference, Fil^i and $\mathcal{V}_i$ are denoted by $\mathcal{M}_i$ and W_i). Hence, we can define

$$\mathrm{Swan}(V) := \sum_i \mathrm{Swan}^{\mathrm{AS}}(\mathcal{V}_i).$$

In the general Hodge–Tate weights case, we define $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V) := \widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V(-n))(n)$ and $\mathrm{Swan}(V) := \mathrm{Swan}(V(-n))$ for sufficiently large n. The definition is independent of the choice of n since the above construction is compatible with Tate twist.

Remark 4.6.3. As in [Colmez 2008a], we should consider an appropriate contribution of "monodromy action" to define the Artin conductor. To avoid complication, we do not define Artin conductors for de Rham representations in this paper.

The lemma below easily follows from Hilbert 90.

Lemma 4.6.4. *Let* $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$.

(i) *If* L *is the* p*-adic completion of an unramified extension of* K, *then we have* $\mathrm{Swan}(V|_L) = \mathrm{Swan}(V)$.

(ii) *Assume* $V \in \mathrm{Rep}^f_{\mathbb{Q}_p}(G_K)$. *Then, we have* $\mathrm{Swan}(V) = \mathrm{Swan}^{\mathrm{AS}}(V)$.

Though the following result will not be used in the proof of the main theorem, we remark that when k_K is perfect, our definition is compatible with the classical definition.

Lemma 4.6.5 (Compatibility of usual Swan conductor in the perfect residue field case). *Assume that* k_K *is perfect. Then, we have* $\mathrm{Swan}(V) = \mathrm{Swan}(\mathbb{D}_{\mathrm{pst}}(V))$ *(see [Colmez 2008a, §0.4] for the definition of* $\mathbb{D}_{\mathrm{pst}}$*).*

Proof. Let the notation be as in Definition 4.6.2. By Tate twist, we may assume that all Hodge–Tate weights of V are negative. By $\mathrm{Swan}(\mathbb{D}_{\mathrm{pst}}(V)) = \mathrm{Swan}(\mathbb{D}_{\mathrm{pst}}(V|_{K^{\mathrm{ur}}}))$ and Lemma 4.6.4(i), we may assume that k_K is algebraically closed by replacing K by K^{ur}. Since $\mathbb{B}^+_{\mathrm{dR}} \otimes_K \mathbb{D}_{\mathrm{dR}}(V)$ is a lattice of $\mathbb{B}^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$, we may identify $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)[1/t]$ with $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V[1/t]$. By the p-adic monodromy theorem, there exists a finite Galois extension L/K such that $\mathbb{D}_{\mathrm{st},L}(V) := (\mathbb{B}_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_L}$ has dimension $\dim_{\mathbb{Q}_p} V$. Moreover, we may assume that G_L acts trivially on each $\mathcal{V}_i$. Put $D_i := (\mathbb{B}_{\mathrm{st}} \otimes_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}} \mathrm{Fil}^i(\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)))^{G_L}$. This forms an increasing filtration of $\mathbb{D}_{\mathrm{st},L}(V)$. Then, we have canonical morphisms

$$D_i/D_{i+1} \hookrightarrow (\mathbb{B}_{\mathrm{st}} \otimes_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}} \mathrm{gr}^i(\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)))^{G_L} \cong (\mathbb{B}_{\mathrm{st}} \otimes_{\mathbb{Q}_{p^{h_i}}} \mathcal{V}_i)^{G_L} \cong W(k_L)[1/p] \otimes_{\mathbb{Q}_{p^{h_i}}} \mathcal{V}_i,$$

where the first injection is an isomorphism by counting dimensions. By the additivity of Swan conductors, we have $\mathrm{Swan}(\mathbb{D}_{\mathrm{pst}}(V)) = \mathrm{Swan}(\mathbb{D}_{\mathrm{st},L}(V)) = \sum_i \mathrm{Swan}(D_i/D_{i+1}) = \sum_i \mathrm{Swan}(\mathcal{V}_i) = \mathrm{Swan}(V)$. □

4.7. *Main theorem.* The aim of this subsection is to prove the following theorem, which generalizes Marmora's formula in Remark 4.7.2:

Main Theorem 4.7.1. *Let* V *be a de Rham representation of* G_K. *Then, the sequence* $\{\mathrm{Swan}(V|_{K_n})\}_{n>0}$ *is eventually stationary and we have*

$$\mathrm{Swan}^{\nabla}(\mathbb{N}_{\mathrm{dR}}(V)) = \lim_n \mathrm{Swan}(V|_{K_n}).$$

Remark 4.7.2. When k_K is perfect, we explain that our formula coincides with the following formula from [Marmora 2004, Théorème 1.1]:

$$\mathrm{Irr}(\mathbb{N}_{\mathrm{dR}}(V)) = \lim_{n\to\infty} \mathrm{Swan}(\mathbb{D}_{\mathrm{pst}}(V|_{K_n})).$$

Here, the LHS means the irregularity of $\mathbb{N}_{\mathrm{dR}}(V)$ regarded as a p-adic differential equation. By Lemma 4.6.5, the RHS is equal to the RHS in Main Theorem 4.7.1. Therefore, we only have to prove $\mathrm{Irr}(D) = \mathrm{Swan}^{\nabla}(D)$ for a (φ, ∇)-module D over the Robba ring. Since D is endowed with a slope filtration and since both irregularity and the differential Swan conductor are additive, we may assume that D is étale by dévissage. Let V be the corresponding p-adic representation of finite local monodromy. Then, the differential Swan conductor $\mathrm{Swan}^{\nabla}(D)$ coincides with the usual Swan conductor of V ([Kedlaya 2007, Proposition 3.5.5]). On the other hand, $\mathrm{Irr}(D)$ coincides with the usual Swan conductor of V ([Tsuzuki 1998, Theorem 7.2.2]), which implies the assertion.

We will deduce Theorem 4.7.1 from Lemma 3.5.4(ii) by dévissage. In the following, we use the notation as in Definition 4.6.2.

Lemma 4.7.3. *Let V be a de Rham representation of G_K with nonpositive Hodge–Tate weights.*

(i) *The (φ, G_K)-modules*

$$\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} \otimes_{\mathbb{B}^{\dagger}_{\mathrm{rig},K}} \mathbb{N}_{\mathrm{dR}}(V), \quad \widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} \otimes_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}} \widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)$$

coincide with each other in $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V$. Moreover, the two filtrations induced by the slope filtrations of $\mathbb{N}_{\mathrm{dR}}(V)$ and $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)$ also coincide with each other.

(ii) *Let the notation be as in Construction 1.7.7. Then, there exists a canonical isomorphism*

$$\mathrm{gr}^i(\mathbb{N}_{\mathrm{dR}}(V)) \cong D^{\dagger}_{\mathrm{rig}}(\mathcal{V}_i|_{\mathbb{E}_K})$$

as (φ, ∇)-modules over $\mathbb{B}^{\dagger}_{\mathrm{rig},K}$.

Proof. (i) We prove the first assertion. By Lemma 4.2.11 (with $B = \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$), we only have to prove that $D^{(1)} := \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}} \mathbb{N}_{\mathrm{dR},r}(V)$, $D^{(2)} := \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}} \widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)$ and $D := \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V$ satisfy the conditions in the lemma. We have $\mathbb{N}_{\mathrm{dR},r}(V)[1/t] = \mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V)[1/t]$ by definition and

$$\begin{aligned}\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\mathbb{B}^{\dagger,r}_{\mathrm{rig},K}} \mathbb{D}^{\dagger,r}_{\mathrm{rig}}(V) &\cong \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\mathbb{B}^{\dagger,r}} \mathbb{B}^{\dagger,r} \otimes_{\mathbb{B}^{\dagger,r}} \mathbb{D}^{\dagger,r}(V)\\ &\cong \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\mathbb{B}^{\dagger,r}} \mathbb{B}^{\dagger,r} \otimes_{\mathbb{Q}_p} V \cong \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\mathbb{Q}_p} V.\end{aligned}$$

As we have $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)[1/t] = \widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}[1/t] \otimes_{\mathbb{Q}_p} V$ by definition, we obtain a canonical isomorphism $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}} \otimes_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}} \widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(V)[1/t] \cong \widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}[1/t] \otimes_{\mathbb{Q}_p} V$, which implies condition (i).

By Proposition 4.2.12(ii), we have a canonical isomorphism $\mathbb{B}_{\mathrm{dR}}^{+}\otimes_{\iota_n,\mathbb{B}_{\mathrm{rig},K}^{\dagger,r}}\mathbb{N}_{\mathrm{dR},r}(V)\cong\mathbb{B}_{\mathrm{dR}}^{+}\otimes_K\mathbb{D}_{\mathrm{dR}}(V)$. On the other hand, we have canonical isomorphisms

$$\mathbb{B}_{\mathrm{dR}}^{+}\otimes_{\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\nabla+}}\widetilde{\mathbb{N}}_{\mathrm{rig}}^{\nabla+}(V)\cong\mathbb{B}_{\mathrm{dR}}^{+}\otimes_{\mathbb{B}_{\mathrm{dR}}^{\nabla+}}(\mathbb{B}_{\mathrm{dR}}^{+}\otimes_K\mathbb{D}_{\mathrm{dR}}(V))^{\nabla^{\mathrm{geom}}=0}\cong\mathbb{B}_{\mathrm{dR}}^{+}\otimes_K\mathbb{D}_{\mathrm{dR}}(V),$$

where the first isomorphism follows from [Ohkubo 2013, Proposition 5.3(ii)] and the second isomorphism follows from [Ohkubo 2013, Proposition 5.4]. Since the canonical map $\mathbb{B}_{\mathrm{dR}}^{\nabla+}\to\mathbb{B}_{\mathrm{dR}}^{+}$ is faithfully flat, condition (ii) is verified. The second assertion follows from the uniqueness of the slope filtration [Kedlaya 2005, Theorem 6.4.1].

(ii) By (i), there exists canonical isomorphisms

$$\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\dagger}\otimes_{\mathbb{B}_{\mathrm{rig},K}^{\dagger}}\mathrm{gr}^i(\mathbb{N}_{\mathrm{dR}}(V))\cong\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\dagger}\otimes_{\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\nabla+}}\mathrm{gr}^i(\widetilde{\mathbb{N}}_{\mathrm{rig}}^{\nabla+}(V))\cong\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\dagger}\otimes_{\mathbb{Q}_{p^{h_i}}}\mathcal{V}_i$$

as (φ,G_K)-modules. By Lemma 4.5.7, we obtain a canonical isomorphism between $\mathrm{gr}^i(\mathbb{N}_{\mathrm{dR}}(V))$ and $\mathbb{D}_{\mathrm{rig}}^{\dagger}(\mathcal{V}_i)$ as (φ,Γ_K)-modules. Since $\mathcal{V}_i$ is of finite local monodromy, so is $\mathcal{V}_i|_{\mathbb{E}_K}$. So, $\dim_{\mathbb{B}_K^{\dagger}}D^{\dagger}(\mathcal{V}_i|_{\mathbb{E}_K})=\dim_{\mathbb{Q}_{p^h}}\mathcal{V}_i$; in particular, the canonical injection $D^{\dagger}(\mathcal{V}_i|_{\mathbb{E}_K})\hookrightarrow(\mathbb{B}^{\dagger}\otimes_{\mathbb{Q}_{p^{h_i}}}\mathcal{V}_i)^{H_K}$ is an isomorphism. Therefore, we have canonical isomorphisms $D_{\mathrm{rig}}^{\dagger}(\mathcal{V}_i|_{\mathbb{E}_K})\cong\mathbb{D}_{\mathrm{rig}}^{\dagger}(\mathcal{V}_i)\cong\mathrm{gr}^i(\mathbb{N}_{\mathrm{dR}}(V))$ as (pure) φ-modules over $\mathbb{B}_{\mathrm{rig},K}^{\dagger}$; hence, the assertion follows from Lemma 4.5.6. □

Remark 4.7.4. One can prove that there exist canonical isomorphisms

$$\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\dagger}\otimes_{\mathbb{B}_{\mathrm{rig},K}^{\dagger}}\mathbb{N}_{\mathrm{dR}}(V)\cong\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\dagger}\otimes_{\widetilde{\mathbb{B}}_{\mathrm{rig}}^{\nabla+}}\widetilde{\mathbb{N}}_{\mathrm{rig}}^{\nabla+}(V)\cong\mathbb{N}_{\mathrm{rig}}^{\dagger}(V).$$

Lemma 4.7.5. *We have*

$$\mathrm{Swan}^{\nabla}(\mathbb{N}_{\mathrm{dR}}(V))=\sum_{1\le i\le r}\mathrm{Swan}^{\mathrm{AS}}(\mathcal{V}_i|_{\mathbb{E}_K}).$$

Proof. We have

$$\begin{aligned}\mathrm{Swan}^{\nabla}(\mathbb{N}_{\mathrm{dR}}(V))&=\sum_{1\le i\le r}\mathrm{Swan}^{\nabla}\big(\mathrm{gr}^i(\mathbb{N}_{\mathrm{dR}}(V))\big)\\&=\sum_{1\le i\le r}\mathrm{Swan}^{\nabla}\big(D_{\mathrm{rig}}^{\dagger}(\mathcal{V}_i|_{\mathbb{E}_K})\big)=\sum_{1\le i\le r}\mathrm{Swan}^{\mathrm{AS}}(\mathcal{V}_i|_{\mathbb{E}_K}),\end{aligned}$$

where the first equality follows from the additivity of the differential Swan conductor (Lemma 1.7.9), the second one follows from Lemma 4.7.3(ii), and the third one follows from Xiao's comparison theorem (Theorem 1.7.10). □

Proof of Main Theorem 4.7.1. By Lemma 4.7.5 and the definition of the Swan conductor (Definition 4.6.2), we only have to prove $\mathrm{Swan}^{\mathrm{AS}}(\mathcal{V}_i|_{\mathbb{E}_K})=\mathrm{Swan}^{\mathrm{AS}}(\mathcal{V}_i|_{K_n})$ for all sufficiently large n. This follows from Lemma 3.5.4(ii). □

Appendix: list of notation

The following is a list of notation in order defined.

1.2: $\widehat{\Omega}^1_K$, ∂_j, $\partial/\partial t_j$.

1.3: $\widetilde{K}_n$, $\widetilde{K}_\infty$, $\Gamma_{\widetilde{K}}$, $H_{\widetilde{K}}$, γ_a, γ_b, $\eta = (\eta_0, \dots, \eta_d)$, $\mathfrak{g}$, L_n, L_∞, Γ_L, H_L, $\Gamma_{L,j}$.

1.4: $\widetilde{\mathbb{E}}^{(+)}$, $v_{\widetilde{\mathbb{E}}}$, $\widetilde{\mathbb{A}}^{(+)}$, $\widetilde{\mathbb{B}}^{(+)}$, ε, $\tilde{t}_j$, π, q, $\mathbb{A}_{\mathrm{inf}}$, $\mathbb{B}^{(+)}_{\mathrm{dR}}$, u_j, t, $\mathbb{D}_{\mathrm{dR}}(\cdot)$, ∇^{geom}, $\mathbb{B}^{\nabla(+)}_{\mathrm{dR}}$, $\mathbb{A}_{\mathrm{cris}}$, $\mathbb{B}_{\mathrm{cris}}$, $\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}$.

1.5: $as^a_{L/K,Z}$, $\mathcal{F}^a(L)$, $b(L/K)$, $as^a_{L/K,Z,P}$, $\mathcal{F}^a_{\log}(L)$, $b_{\log}(L/K)$, $\mathrm{Art}^{\mathrm{AS}}(\cdot)$, $\mathrm{Swan}^{\mathrm{AS}}(\cdot)$.

1.6: $v^{\leq n}$, w_r, $W(E)_r$, $W_{\mathrm{con}}(E)$, Γ_r, Γ_{con}, $\Gamma_{\mathrm{an},r}$, $\Gamma_{\mathrm{an,con}}$, $\mathcal{O}\{\{S\}\}$, $\mathcal{O}((S))^{\dagger,r}$, $\mathcal{O}((S))^{\dagger}$, $\mathcal{R}$, $\mathrm{Mod}_\bullet(\sigma)$, $\mathrm{Mod}^{\mathrm{et}}_\bullet(\sigma)$, $\mathrm{Mod}^s_\bullet(\sigma)$.

1.7: Ω^1_R, $\Omega^1_{\mathcal{R}}$, $d : \mathcal{R} \to \Omega^1_{\mathcal{R}}$, $\mathrm{Mod}^s_\bullet(\varphi^h, \nabla)$ D, $D^\dagger$, $\mathrm{Swan}^\nabla(\cdot)$.

1.8: $X^{(+)}_{\mathfrak{K}} = X^{(+)}(\mathfrak{K}, \xi, n_0)$.

1.9: $\mathbb{E}^{(+)}_L$, $\widetilde{\mathbb{E}}^{(+)}_K$, $\widetilde{\mathbb{A}}^{(+)}_L$, $\widetilde{\mathbb{B}}_L$, $\mathbb{A}$, $\mathbb{B}_L$, $\mathbb{B}$, $\mathrm{Mod}^{\mathrm{et}}_{\mathbb{B}_L}(\varphi^h, \Gamma_L)$, $\mathbb{D}(\cdot)$, $\mathbb{V}(\cdot)$.

1.10: $\widetilde{\mathbb{A}}^{\dagger,r}$, $\widetilde{\mathbb{A}}^{\dagger}$, $\widetilde{\mathbb{B}}^{\dagger,r}$, $\widetilde{\mathbb{B}}^{\dagger}$, $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig}}$, $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig}}$, $\mathbb{A}^{\dagger,r}$, $\mathbb{A}^{\dagger}$, $\mathbb{B}^{\dagger,r}$, $\mathbb{B}^{\dagger}$, $\mathbb{B}^{\dagger,r}_{\mathrm{rig}}$, $\mathbb{B}^{\dagger}_{\mathrm{rig}}$, $\widetilde{\mathbb{A}}^{\dagger,r}_L$, $\widetilde{\mathbb{A}}^{\dagger}_L$, $\widetilde{\mathbb{B}}^{\dagger,r}_L$, $\widetilde{\mathbb{B}}^{\dagger}_L$, $\widetilde{\mathbb{B}}^{\dagger,r}_{\mathrm{rig},L}$, $\widetilde{\mathbb{B}}^{\dagger}_{\mathrm{rig},L}$, $\mathbb{A}^{\dagger,r}_L$, $\mathbb{A}^{\dagger}_L$, $\mathbb{B}^{\dagger,r}_L$, $\mathbb{B}^{\dagger}_L$, $\mathbb{B}^{\dagger,r}_{\mathrm{rig},L}$, $\mathbb{B}^{\dagger}_{\mathrm{rig},L}$, $\mathbb{D}^{\dagger,r}(\cdot)$, $\mathbb{D}^{\dagger}(\cdot)$, $\mathbb{D}^{\dagger,r}_{\mathrm{rig}}(\cdot)$, $\mathbb{D}^{\dagger}_{\mathrm{rig}}(\cdot)$.

3.1: $R\langle \underline{X} \rangle$, $\mathcal{O}((S))^{\dagger,r}_0$, $|\cdot|_r$, $\mathcal{O}[\![S]\!]\langle \underline{X} \rangle$, $\mathcal{O}((S))^{\dagger,r}_0\langle \underline{X} \rangle$, $\mathcal{O}((S))^{\dagger,r}\langle \underline{X} \rangle$, $\deg(\mathfrak{p})$, $\kappa(\mathfrak{p})$, $\kappa(p)$, $\pi_{\mathfrak{p}}$.

3.2: $\succeq$, $\succ$, $\succeq_{\mathrm{lex}}$, $\underline{v}_R$, $\underline{\deg}_R$, $\mathrm{LT}_R(\cdot)$, $|\cdot|_{\mathrm{qt}}$.

3.3: A, $I^{\dagger,r}$, $A^{\dagger,r}$, $|\cdot|_{r,\mathrm{qt}}$.

3.4: $\mathrm{Idem}(\cdot)$, as $\cdot_{\mathfrak{p},\mathrm{qt}}$, $|\cdot|_{\mathfrak{p},\mathrm{sp}}$ $A_{\kappa(\mathfrak{p})}$.

3.5: AS^r, $AS^r_{\log}$.

4.1: $K_n[\![u_1, \dots, u_d]\!]^\nabla$.

4.2: ι_n, $t_{n,w}$, $\mathbb{N}_{\mathrm{dR},r}(\cdot)$, $\mathbb{N}_{\mathrm{dR}}(\cdot)$, $\widetilde{\mathbb{N}}^{\dagger,r}_{\mathrm{rig}}(\cdot)$, $\widetilde{\mathbb{N}}^{\dagger}_{\mathrm{rig}}(\cdot)$.

4.3: ∇_j.

4.4: $\widetilde{\nabla}_j$, ∇'_j.

4.5: $\mathrm{Rep}_{a,h}(G_K)$, $D_{[s]}$, $\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^\dagger_{\mathrm{rig}}}(\varphi, G_K)$, $\mathrm{Mod}^s_{\mathbb{B}^\dagger_{\mathrm{rig},K}}(\varphi, \Gamma_K)$, $\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^\dagger}(\varphi, G_K)$, $\mathrm{Mod}^s_{\mathbb{B}^\dagger_K}(\varphi, \Gamma_K)$, $\mathrm{Mod}^s_{\widetilde{\mathbb{B}}^{\nabla+}_{\mathrm{rig}}}(\varphi, G_K)$, $\widetilde{\mathbb{D}}^{\nabla+}_{\mathrm{rig}}(\cdot)$, $\widetilde{\mathbb{D}}^{+}_{\mathrm{rig}}(\cdot)$, $\mathbb{D}^{\dagger}_{\mathrm{rig}}(\cdot)$, $\widetilde{\mathbb{D}}^{\dagger}(\cdot)$, $\mathbb{D}^{\dagger}(\cdot)$.

4.6: $\widetilde{\mathbb{N}}^{\nabla+}_{\mathrm{rig}}(\cdot)$, $\mathcal{V}_i$, $\mathrm{Swan}(\cdot)$.

Acknowledgement. The author would like to thank Atsushi Shiho and Takeshi Tsuji for encouragement. He thanks Liang Xiao for the proof of Lemma 3.1.7, Adriano Marmora for helpful discussions, and the referee for helpful advice. The author is supported by the Research Fellowships of the Japan Society for the Promotion of Science for Young Scientists.

References

[Abbes and Saito 2002] A. Abbes and T. Saito, "Ramification of local fields with imperfect residue fields", *Amer. J. Math.* **124**:5 (2002), 879–920. MR 2003m:11196 Zbl 1084.11064

[Abbes and Saito 2003] A. Abbes and T. Saito, "Ramification of local fields with imperfect residue fields II", *Doc. Math.* Extra Vol. (2003), 5–72. MR 2005g:11231 Zbl 1127.11349

[Andreatta 2006] F. Andreatta, "Generalized ring of norms and generalized (ϕ, Γ)-modules", *Ann. Sci. École Norm. Sup.* (4) **39**:4 (2006), 599–647. MR 2007k:12006 Zbl 1123.13007

[Andreatta and Brinon 2008] F. Andreatta and O. Brinon, "Surconvergence des représentations p-adiques: le cas relatif", pp. 39–116 in *Représentations p-adiques de groupes p-adiques I: Représentations galoisiennes et (ϕ, Γ)-modules*, Astérisque **319**, Société Mathématique de France, Paris, 2008. MR 2010c:11139 Zbl 1168.11018

[Andreatta and Brinon 2010] F. Andreatta and O. Brinon, "B_{dR}-représentations dans le cas relatif", *Ann. Sci. Éc. Norm. Supér.* (4) **43**:2 (2010), 279–339. MR 2011e:11097 Zbl 1195.11074

[Berger 2002] L. Berger, "Représentations p-adiques et équations différentielles", *Invent. Math.* **148**:2 (2002), 219–284. MR 2004a:14022 Zbl 1113.14016

[Berger 2008a] L. Berger, "Construction de (ϕ, Γ)-modules: représentations p-adiques et B-paires", *Algebra Number Theory* **2**:1 (2008), 91–120. MR 2009j:14025 Zbl 1219.11078

[Berger 2008b] L. Berger, "Équations différentielles p-adiques et (ϕ, N)-modules filtrés", pp. 13–38 in *Représentations p-adiques de groupes p-adiques I: Représentations galoisiennes et (ϕ, Γ)-modules*, Astérisque **319**, Société Mathématique de France, Paris, 2008. MR 2010d:11056 Zbl 1168.11019

[Bosch et al. 1984] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis: a systematic approach to rigid analytic geometry*, Grundlehren der Mathematischen Wissenschaften **261**, Springer, Berlin, 1984. MR 86b:32031 Zbl 0539.14017

[Bourbaki 1998] N. Bourbaki, *Commutative algebra: Chapters 1–7*, Springer, Berlin, 1998. MR 2001g:13001 Zbl 0902.13001

[Bourbaki 2006] N. Bourbaki, *Éléments de mathématique: Algèbre commutative, Chapitres 8 et 9*, Springer, Berlin, 2006. MR 2007h:13001 Zbl 0579.13001

[Cherbonnier and Colmez 1998] F. Cherbonnier and P. Colmez, "Représentations p-adiques surconvergentes", *Invent. Math.* **133**:3 (1998), 581–611. MR 2000d:11146 Zbl 0928.11051

[Colmez 2008a] P. Colmez, "Conducteur d'Artin d'une représentation de de Rham", pp. 187–212 in *Représentations p-adiques de groupes p-adiques I: Représentations galoisiennes et (ϕ, Γ)-modules*, Astérisque **319**, Société Mathématique de France, Paris, 2008. MR 2010j:11168 Zbl 1168.11052

[Colmez 2008b] P. Colmez, "Espaces vectoriels de dimension finie et représentations de de Rham", pp. 117–186 in *Représentations p-adiques de groupes p-adiques I: Représentations galoisiennes et (ϕ, Γ)-modules*, Astérisque **319**, Société Mathématique de France, Paris, 2008. MR 2010d:11137 Zbl 1168.11021

[Cox et al. 1997] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, 2nd ed., Springer, New York, 1997. MR 97h:13024

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001

[Fontaine 1990] J.-M. Fontaine, "Représentations p-adiques des corps locaux, I", pp. 249–309 in *The Grothendieck Festschrift, Vol. II*, edited by P. Cartier et al., Progr. Math. **87**, Birkhäuser, Boston, 1990. MR 92i:11125 Zbl 0743.11066

[Fontaine 1994] J.-M. Fontaine, "Représentations p-adiques semi-stables", pp. 113–184 in *Périodes p-adiques* (Bures-sur-Yvette, 1988), Astérisque **223**, Société Mathématique de France, Paris, 1994. MR 95g:14024 Zbl 0865.14009

[Hattori 2014] S. Hattori, "Ramification theory and perfectoid spaces", *Compos. Math.* **150**:5 (2014), 798–834. MR 3209796

[Helmer 1943] O. Helmer, "The elementary divisor theorem for certain rings without chain condition", *Bull. Amer. Math. Soc.* **49** (1943), 225–236. MR 4,185d Zbl 0060.07606

[Hyodo 1986] O. Hyodo, "On the Hodge–Tate decomposition in the imperfect residue field case", *J. Reine Angew. Math.* **365** (1986), 97–113. MR 87m:14052 Zbl 0571.14004

[Kato 2004] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", pp. ix, 117–290 in *Cohomologies p-adiques et applications arithmétiques, III*, Astérisque **295**, Société Mathématique de France, Paris, 2004. MR 2006b:11051

[Kedlaya 2004] K. S. Kedlaya, "A p-adic local monodromy theorem", *Ann. of Math.* (2) **160**:1 (2004), 93–184. MR 2005k:14038 Zbl 1088.14005

[Kedlaya 2005] K. S. Kedlaya, "Slope filtrations revisited", *Doc. Math.* **10** (2005), 447–525. MR 2007c:14016 Zbl 1081.14028

[Kedlaya 2007] K. S. Kedlaya, "Swan conductors for p-adic differential modules, I: a local construction", *Algebra Number Theory* **1**:3 (2007), 269–300. MR 2009b:11205

[Kedlaya 2010] K. S. Kedlaya, *p-adic differential equations*, Cambridge Studies in Advanced Mathematics **125**, Cambridge University Press, Cambridge, 2010. MR 2011m:12016 Zbl 1213.12009

[Kedlaya 2013] K. S. Kedlaya, "Some slope theory for multivariate Robba rings", preprint, 2013. arXiv 1311.7468

[Lazard 1962] M. Lazard, "Les zéros des fonctions analytiques d'une variable sur un corps valué complet", *Inst. Hautes Études Sci. Publ. Math.* 14 (1962), 47–75. MR 27 #2497 Zbl 0119.03701

[Marmora 2004] A. Marmora, "Irrégularité et conducteur de Swan p-adiques", *Doc. Math.* **9** (2004), 413–433. MR 2005i:11169 Zbl 1071.11065

[Matsuda 1995] S. Matsuda, "Local indices of p-adic differential operators corresponding to Artin–Schreier–Witt coverings", *Duke Math. J.* **77**:3 (1995), 607–625. MR 97a:14019 Zbl 0849.12013

[Matsumura 1980] H. Matsumura, *Commutative algebra*, 2nd ed., Mathematics Lecture Note Series **56**, Benjamin/Cummings Publishing Co., Reading, MA, 1980. MR 82i:13003 Zbl 0441.13001

[Ohkubo 2010] S. Ohkubo, "Galois theory of B_{dR}^{+} in the imperfect residue field case", *J. Number Theory* **130**:7 (2010), 1609–1641. MR 2011i:11169 Zbl 1208.11129

[Ohkubo 2013] S. Ohkubo, "The p-adic monodromy theorem in the imperfect residue field case", *Algebra Number Theory* **7**:8 (2013), 1977–2037. MR 3134041 Zbl 1312.11046

[Raynaud 1970] M. Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Mathematics **169**, Springer, Berlin, 1970. MR 43 #3252 Zbl 0203.05102

[Schneider 2002] P. Schneider, *Nonarchimedean functional analysis*, Springer, Berlin, 2002. MR 2003a:46106 Zbl 0998.46044

[Scholl 2006] A. J. Scholl, "Higher fields of norms and (ϕ, Γ)-modules", *Doc. Math.* Extra Vol. (2006), 685–709. MR 2007k:11199 Zbl 1186.11070

[Scholze 2012] P. Scholze, "Perfectoid spaces", *Publ. Math. Inst. Hautes Études Sci.* **116** (2012), 245–313. MR 3090258 Zbl 1263.14022

[Tsuzuki 1998] N. Tsuzuki, "The local index and the Swan conductor", *Compositio Math.* **111**:3 (1998), 245–288. MR 99g:14021 Zbl 0926.12004

[Xiao 2010] L. Xiao, "On ramification filtrations and p-adic differential modules, I: the equal characteristic case", *Algebra Number Theory* **4**:8 (2010), 969–1027. MR 2832631

[Xiao 2012] L. Xiao, "On ramification filtrations and p-adic differential equations, II: mixed characteristic case", *Compos. Math.* **148**:2 (2012), 415–463. MR 2904193

Communicated by Brian Conrad
Received 2015-02-27 Revised 2015-05-28 Accepted 2015-06-25

shuno@math.nagoya-u.ac.jp *Graduate School of Mathematics, Nagoya University, Furocho, Chikusaku, Nagoya 4648602, Japan*

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 9 No. 8 2015

1937-0652(2015)9:8;1-1