Algebra & Number Theory

Volume 4

2010

No. 8

mathematical sciences publishers

Algebra & Number Theory

www.jant.org

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

The subscription price for 2010 is US $140/year for the electronic version, and $200/year (+$30 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

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

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

PUBLISHED BY

mathematical sciences publishers

http://www.mathscipub.org

A NON-PROFIT CORPORATION

Typeset in LaTeX

ALGEBRA AND NUMBER THEORY 4:8(2010)

On ramification filtrations and p-adic differential modules I: the equal characteristic case

Liang Xiao

Let k be a complete discretely valued field of equal characteristic $p > 0$ with possibly imperfect residue field, and let G_k be its Galois group. We prove that the conductors computed by the arithmetic ramification filtrations on G_k defined by Abbes and Saito (*Amer. J. Math* **124**:5, 879–920) coincide with the differential Artin conductors and Swan conductors of Galois representations of G_k defined by Kedlaya (*Algebra Number Theory* **1**:3, 269–300). As a consequence, we obtain a Hasse–Arf theorem for arithmetic ramification filtrations in this case. As applications, we obtain a Hasse–Arf theorem for finite flat group schemes; we also give a comparison theorem between the differential Artin conductors and Borger's conductors (*Math. Ann.* **329**:1, 1–30).

Introduction

Let k be a complete discretely valued field and let G_k be the Galois group of a fixed separable closure k^{sep} over k. When the residue field κ_k of k is perfect, classical ramification theory gives Artin conductors and Swan conductors, which measure the ramification of representations of G_k of finite local monodromy (i.e., the image of the inertia group being finite). A fundamental result, the Hasse–Arf theorem, states that Artin and Swan conductors are nonnegative integers. However, when the residue field κ_k is not perfect, classical ramification theory is no longer applicable.

MSC2000: primary 11S15; secondary 14G22, 12H25.

Keywords: ramification, p-adic differential equation, Swan conductors, Artin conductors, Hasse–Arf theorem.

For one thing, the transition functions ϕ and ψ in [Serre 1979, §IV.3] fail the basic properties; for another, the extension of the rings of integers may not be generated by a single element (compare [Serre 1979, §III.6, Proposition 12]).

Kato [1989] defined Swan conductors for one-dimensional representations when the residue field is not perfect. Later, Abbes and Saito [2002; 2003] defined an arithmetic (nonlogarithmic) filtration and a logarithmic variant on G_k by counting geometric connected components of certain rigid spaces $as^a_{l/k}$ and $as^a_{l/k,\log}$ over k, which we refer to as Abbes–Saito spaces. The filtrations give the arithmetic Artin conductors and Swan conductors naturally.

Abbes and Saito [2009] showed that their definition of Swan conductors coincides with Kato's when k is of equal characteristic $p > 0$. Moreover, they proved that the subquotients of both filtrations are abelian groups [Abbes and Saito 2003]. (See also Saito's proof [2009] that the subquotients of the logarithmic filtration on wild inertia are elementary abelian p-groups.) However, they were not able to establish an integrality result analogous to the classical Hasse–Arf theorem.

Through a completely different path, when k is of equal characteristic $p > 0$ and has perfect residue field, Christol, Cook, Matsuda, Mebkhout, and Tsuzuki (see [Matsuda 2002]) gave a completely new interpretation of the classical Swan conductors using the theory of p-adic differential modules. Given a p-adic Galois representation of finite local monodromy, they associated a p-adic differential module over the Robba ring and proved that the Swan conductor of the representation can be retrieved from the irregularity of the differential module, or equivalently, the spectral norms of the differential operator.

Partly inspired by [Matsuda 2004], Kedlaya generalized this framework to the case when the residue field κ_k is not perfect. In [Kedlaya 2007], he adopted the same construction and counted in the effects of other differential operators corresponding to elements in a p-basis of κ_k. He defined the differential Swan conductor to be, vaguely speaking, the maximum of the numbers computed by each of the differential operators, under certain normalization; he was aware of a definition for differential Artin conductors using a slightly different normalization. Most importantly, he was able to prove a Hasse–Arf theorem for differential Swan conductors [Kedlaya 2007, Theorem 3.5.8]; his argument can easily be adapted to prove a Hasse–Arf theorem for differential Artin conductors. For a precise statement, see Theorem 2.4.1.

Kedlaya [2007] asked, as Matsuda suggested, whether the differential conductors are the same as the arithmetic ones, in which case the Hasse–Arf theorem for the arithmetic filtrations in the equal characteristic case would follow from that for the differential conductors. Chiarellotto and Pulita [2009] gave an affirmative answer to this question when the representations are one-dimensional, using the setting of Kato's conductors [Kato 1989].

There is a third story of defining conductors. Borger [2004] introduced the notation of generic perfection of a complete discretely valued field and defined the Artin conductors to be the ones obtained by base change to the generic residual perfection of k, which is a complete discretely valued field with perfect residue field satisfying certain universal properties. The Hasse–Arf theorem of these conductors will follow immediately from that of the classical ones. Kedlaya [2007, p. 297] asked if this also coincides with the two definitions above.

This paper answers these questions in the affirmative for all representations of finite local monodromy. Our precise result is the following.

Theorem. *Let k be a complete discretely valued field of equal characteristic $p > 0$ and let G_k be its absolute Galois group.*

(1) (Hasse–Arf Theorem) *Let $\rho : G_k \to \mathrm{GL}(V_\rho)$ be a p-adic representation of finite local monodromy. Then the arithmetic Artin conductor* $\mathrm{Art}_{\mathrm{ar}}(\rho)$, *the differential Artin conductor* $\mathrm{Art}_{\mathrm{dif}}(\rho)$, *and the Borger's conductor* $\mathrm{Art}_B(\rho)$ *are the same. Similarly, the arithmetic Swan conductor* $\mathrm{Swan}_{\mathrm{ar}}(\rho)$ *is the same as the differential Swan conductor* $\mathrm{Swan}_{\mathrm{dif}}(\rho)$. *As a consequence, they are all nonnegative integers.*

(2) *The subquotients* $\mathrm{Fil}^a G_k/\mathrm{Fil}^{a+} G_k$ *of the arithmetic ramification filtrations are trivial if $a \notin \mathbb{Q}$ and are elementary p-abelian groups if $a \in \mathbb{Q}_{>1}$; the subquotients* $\mathrm{Fil}^a_{\log} G_k/\mathrm{Fil}^{a+}_{\log} G_k$ *of the arithmetic logarithmic ramification filtrations are trivial if $a \notin \mathbb{Q}$ and are elementary p-abelian groups if $a \in \mathbb{Q}_{>0}$.*

This theorem consists of Theorems 4.4.1 and 5.4.3 and Corollary 4.4.3.

We now explain the main idea of the proof, which shows that arithmetic conductors and differential conductors coincide in a natural way. (We will use the comparison of Artin conductors as an example; that of Swan conductors is proved similarly.)

Let k be a complete discretely valued field of equal characteristic p, with residue field κ_k. Let l be a finite Galois extension of k with residue field κ_l. One immediately reduces the comparison to proving that the arithmetic highest ramification break of l/k is the same as the differential one. There are three main ingredients.

(a) A useful way of visualizing spectral norms is to consider the convergence loci or radii at a generic point; see for example [Kedlaya 2005, §5]. However, the convergence loci cannot be defined on the rigid annulus because one cannot separate $m+1$ differential operators on a one-dimensional space. Matsuda [2004] made a pioneering attempt to obtain an $(m+1)$-dimensional space on which we may discuss convergence loci. Our approach, which is independently developed and looks very similar to Matsuda's work, uses a thickening technique. (Alas, we do not know how to relate the two methods.) If the field k can be realized as the field of rational functions on a smooth variety over certain perfect field, the thickening space is just a subspace of the generic fiber of the tube corresponding to the diagonal embedding in a formal lifting (see Section 3.1). This thickening space, after a certain base change, “looks the same” as the Abbes–Saito space $as^a_{l/k}$, whose geometric connected components give the ramification information. However, we have the following technical issue.

(b) The thickening space is a rigid space over K, the fraction field of a Cohen ring of κ_k, which in particular is a field of characteristic zero. In contrast, the Abbes–Saito space $as^a_{l/k}$ is a rigid space over k, which is of characteristic p. In order to relate the two spaces, we need a lifting technique (see Section 1) to lift the Abbes–Saito space to characteristic zero and compare the geometric connected components before and after the lifting process. A similar idea is also alluded to as a conjecture in [Matsuda 2004]. (Again, we do not know whether our result answers Matsuda’s conjecture.)

(c) The lifted Abbes–Saito space is isomorphic to the thickening space after a certain base change (Theorem 4.3.6), but not in the naïve way. Very vaguely speaking, if the extension l/k is generated by a series of equations, then the Abbes–Saito space consists of the points which are close to the solutions to those equations; in contrast, the (base change of the) thickening space consists of points which are solutions to some equations whose coefficients are close to the original equations. These two types of points coincide when l/k is totally and wildly ramified.

Combining these three ingredients, we can prove the comparison between the arithmetic conductors and the differential ones. The following diagram may be helpful to illustrate the process:

$$\begin{tikzcd}
Y = A^1_L[\eta_0^{1/e}, 1) \arrow[d] & & TS^a \times_{\tilde{\pi}, Z} Y \arrow[ll] \arrow[d] \arrow[r, squiggly, dash, "(c)"] & AS^a_{l/k} & as^a_{l/k} \arrow[l, squiggly, "(b)"'] \\
Z = A^1_K[\eta_0, 1) & & TS^a = \text{“}\bigcup_{\eta \in [\eta_0, 1)} A^1_K[\eta, 1) \times A^{m+1}_K[0, \eta^a)\text{.”} \arrow[ll, "\tilde{\pi}", "(a)"'] & &
\end{tikzcd}$$

Here K and L are the fraction fields of Cohen rings of κ_k and κ_l, respectively; $A^1_K[\eta_0, 1)$ is the half-open annulus over K (centered at the origin) with inner radius η_0 and outer radius 1, for some $\eta_0 \in (0, 1)$; $A^{m+1}_K[0, \eta^a)$ is the open polydisc (centered at the origin) of dimension $m + 1$ and radius η^a for some $a \in \mathbb{Q}_{>1}$ (for the quotation marks on $\bigcup_{\eta \in [\eta_0, 1)} A^1_K[\eta, 1) \times A^{m+1}_K[0, \eta^a)$, see Caution 3.2.4); TS^a denotes the space obtained by the thickening process (a); $as^a_{l/k}$ is the rigid analytic space over k defined by Abbes and Saito with respect to a set of distinguished generators; and $AS^a_{l/k}$ is the lifting space given by lifting process (b); the argument in (c) links the two spaces as shown in the diagram.

Part (a) is carried out throughout Section 3 (see Theorem 3.4.12). Part (b) is developed in Section 1 (see Corollary 1.2.12 and Example 1.3.4). Part (c) occupies Section 4 (see Theorem 4.3.6). We finally wrap up the proof in Theorem 4.4.1.

We also obtain a comparison theorem between Borger's Artin conductors and the differential Artin conductors, or equivalently the arithmetic Artin conductors. The key is to show that the differential Artin conductors are invariant under the operation of adding generic p^∞-th roots (see Definition 5.2.2). This fact follows easily from the study of differential operators.

Plan of the paper. In Section 1, we make a construction to lift a rigid space over k to a rigid space over an annulus over K. We prove that the connected components of the original rigid space are in one-to-one correspondence with the connected components of the lifting space, when the annulus is "thin" enough. This part is written in a relatively independent and self-contained manner, since we feel that it is interesting on its own.

In Section 2, we discuss how to associate a differential module $\mathscr{E}_\rho$ on the Robba ring over K with a representation ρ of G_k of finite local monodromy. Then we review the definition of differential Swan conductors following [Kedlaya 2007]. We also introduce differential Artin conductors and discuss their properties.

Section 3 introduces a thickening construction. In Section 3.1, as an intuitive example, we construct the thickening space when k can be realized geometrically. In Section 3.2, we define thickening spaces for general k and discuss spectral properties of the differential module obtained by pulling back $\mathscr{E}_\rho$ to the thickening spaces. In Sections 3.3 and 3.4, we link the (highest) differential breaks and spectral norms with the connected components of a certain base change of the thickening spaces.

In Section 4, we first quickly review the definition of arithmetic ramification filtrations, following [Abbes and Saito 2002]. Then, in Section 4.2, we define the standard Abbes–Saito spaces $as^a_{l/k}$ and their lifts $AS^a_{l/k}$. Next, we prove in Section 4.3 that the lifted Abbes–Saito spaces and (the base change of) the thickening spaces are isomorphic (Theorem 4.3.6). From this, in Section 4.4, we deduce our main result, Theorem 4.4.1: differential conductors coincide with arithmetic conductors.

Section 5 gives two applications. In Section 5.1 we deduce a Hasse–Arf theorem for finite flat group schemes; in Sections 5.2–5.4 we compare the arithmetic and differential Artin conductors with Borger's Artin conductors [Borger 2004].

1. Lifting rigid spaces

In this section, which is largely self-contained, we introduce a construction to lift a rigid space over a field of characteristic $p > 0$ to a rigid space over an annulus over a field of characteristic zero. The notation will not be carried over to later sections unless explicitly noted.[1]

Remark 1.0.1. For most of this paper, we implicitly use rigid analytic spaces in the sense of Berkovich spaces [1990] by allowing discs or annuli with irrational radii. This is mostly for notational convenience. Only in two places (see Remarks 1.2.13 and 4.2.5) will we have to shift back to the classical rigid analytic setting to talk about connected components by assuming some rationality on the radii of discs or annuli.

1.1. ***A Gröbner basis argument.*** In this subsection, we introduce a division algorithm using a Gröbner basis, which enables us to find a representative in the quotient ring achieving the quotient norm.

Notation 1.1.1. Let K be a complete discretely valued field of mixed characteristic $(0, p)$, with ring of integers $\mathcal{O}_K$ and residue field κ. Fix a uniformizer π_K and normalize the valuation $v_K(\cdot)$ on K so that $v_K(\pi_K) = 1$. We also normalize the norm on K so that $|p| = p^{-1}$.

Notation 1.1.2. For a nonarchimedean ring R, we use $R\langle u_1, \dots, u_n\rangle$ to denote the Tate algebra, consisting of formal power series $\sum_{i_1,\dots,i_n\in\mathbb{Z}_{\geq 0}} f_{i_1,\dots,i_n} u_1^{i_1}\cdots u_n^{i_n}$ with $f_{i_1,\dots,i_n} \in R$ and $|f_{i_1,\dots,i_n}| \to 0$ as $i_1 + \dots + i_n \to +\infty$. For $\eta_1, \dots, \eta_n \in (0, 1]$, the ring admits a $(\eta_1, \dots, \eta_n)$-*Gauss norm* given by

$$\Big|\sum_{i_1,\dots,i_n\in\mathbb{Z}_{\geq 0}} f_{i_1,\dots,i_n} u_1^{i_1}\cdots u_n^{i_n}\Big|_{\eta_1,\dots,\eta_n} = \max_{i_1,\dots,i_n} \{|f_{i_1,\dots,i_n}|\eta_1^{i_1}\dots\eta_n^{i_n}\}.$$

Notation 1.1.3. Fix a positive integer n, and put

$$R^{\mathrm{int}} = \mathcal{O}_K\langle u_1, \dots, u_n\rangle((S)), \qquad R = R^{\mathrm{int}} \otimes_{\mathcal{O}_K} K,$$
$$R_\kappa = R^{\mathrm{int}} \otimes_{\mathcal{O}_K} \kappa \cong \kappa[u_1, \dots, u_n]((S)) = \kappa((S))\langle u_1, \dots, u_n\rangle.$$

For $\eta \in (0, 1]$, let $|\cdot|_\eta$ (for short) denote the $(1, \dots, 1, \eta)$-Gauss norm on R.

Notation 1.1.4. The *lexicographic* order on $\mathbb{Z}^n$ is: for $(i_1, \dots, i_n)$ and $(i'_1, \dots, i'_n)$ both in $\mathbb{Z}^n$, we have $(i_1, \dots, i_n) \succ (i'_1, \dots, i'_n)$ if there exists some $j \in \{1, \dots, n\}$ such that $i_1 = i'_1, \dots, i_{j-1} = i'_{j-1}$ and $i_j > i'_j$.

Definition 1.1.5. We equip R_κ with the lexicographic term ordering induced by the correspondence $u_1^{i_1}\cdots u_n^{i_n} S^j \mapsto (-j, i_1, \dots, i_n)$, i.e., we write $\bar\alpha u_1^{i_1}\cdots u_n^{i_n} S^j \succeq \bar\beta u_1^{i'_1}\cdots u_n^{i'_n} S^{j'}$ if $(-j, i_1, \dots, i_n) \succeq (-j', i'_1, \dots, i'_n)$ under the lexicographic order, where $\bar\alpha, \bar\beta \in \kappa^\times$.

Using this ordering, we define the *leading term* $\mathrm{lead}(\bar f)$ of a nonzero element $\bar f \in R_\kappa$ to be its largest term under the ordering. In particular, for $\bar f, \bar g \in R_\kappa\backslash\{0\}$, $\mathrm{lead}(\bar f\bar g) = \mathrm{lead}(\bar f)\,\mathrm{lead}(\bar g)$.

[1]Most of the proofs in this section should be credited to Kedlaya, to whom I am thankful for allowing their inclusion.

For an ideal I_κ of R_κ, a *Gröbner basis* of I_κ is a finite subset $\{\bar{r}_1, \dots, \bar{r}_m\} \subset I_\kappa$ such that no leading term of an $\bar{r}_i$ has exponents in S and such that the ideal consisting of the leading terms of all elements of I_κ is generated by $\mathrm{lead}(\bar{r}_1), \dots, \mathrm{lead}(\bar{r}_m)$. Such a basis exists because R_κ is Noetherian. By [Eisenbud 1995, Lemma 15.5], $\bar{r}_1, \dots, \bar{r}_m$ also generate I_κ.

Proposition 1.1.6. *For any $\bar{f} \in R_\kappa$, there exists $\bar{g}_1, \dots, \bar{g}_m, \bar{f}' \in R_\kappa$ such that*

$$\bar{f} = \bar{g}_1\bar{r}_1 + \cdots + \bar{g}_m\bar{r}_m + \bar{f}', \tag{1.1.7}$$

where any term of $\bar{f}'$ is not divisible by any $\mathrm{lead}(\bar{r}_h)$, *and* $\mathrm{lead}(\bar{f}) \succeq \mathrm{lead}(\bar{g}_h\bar{r}_h)$ *for all h.*

Proof. Let j be the exponent of S in $\mathrm{lead}(\bar{f})$ and let $S^j \bar{f}_{(j)}$ be the sum of terms in $\bar{f}$ for which the exponents of S are j. Applying [Eisenbud 1995, Proposition-Definition 15.6] to $\bar{f}_{(j)}$, we can write

$$\bar{f}_{(j)} \equiv \bar{g}_{1,(j)}\bar{r}_1 + \cdots + \bar{g}_{m,(j)}\bar{r}_m + \bar{f}'_{(j)} \pmod{S \cdot \kappa[u_1, \dots, u_m][\![S]\!]},$$

where $\bar{g}_{h,(j)} \in \kappa[u_1, \dots, u_m]$ and $\mathrm{lead}(\bar{g}_{h,(j)}\bar{r}_h) \preceq \mathrm{lead}(\bar{f}_{(j)})$ for $h = 1, \dots, m$ and any term in $\bar{f}'_{(j)} \in \kappa[u_1, \dots, u_m]$ is not divisible by any $\mathrm{lead}(\bar{r}_h)$.

If we repeat the above argument for $\bar{f}_{(j)} - S^j(\bar{g}_{1,(j)}\bar{r}_1 + \cdots + \bar{g}_{m,(j)}\bar{r}_m + \bar{f}'_{(j)}) \in S^{j+1} \cdot \kappa[u_1, \dots, u_m][\![S]\!]$ in place of $\bar{f}$, we will obtain $\bar{f}'_{(j')}$ and $\bar{g}_{h,(j')}$ for $h = 1, \dots, m$ and for some $j' \geq j+1$. We can then iterate this process.

For $h = 1, \dots, m$, put $\bar{g}_h = S^j \bar{g}_{h,(j)} + S^{j+1}\bar{g}_{h,(j+1)} + \cdots$ and $\bar{f}' = S^j \bar{f}'_{(j)} + S^{j+1} \bar{f}'_{(j+1)} + \cdots$; the power series converge to the elements in R_κ we seek. □

Definition 1.1.8. For $f \in R$, write

$$f = \sum_{i_1,\dots,i_n,j} f_{i_1,\dots,i_n,j} u_1^{i_1} \cdots u_n^{i_n} S^j. \tag{1.1.9}$$

Of the monomials for which $|f_{i_1,\dots,i_n,j}| = |f|_1$, there must be one which is lexicographically largest; we call the corresponding term $f_{i_1,\dots,i_n,j} u_1^{i_1} \cdots u_n^{i_n} S^j$ the 1-*leading term* of f, denoted by $\mathrm{Lead}(f)$.

Hypothesis 1.1.10. Let I^{int} be an ideal of R^{int} such that $R^{\mathrm{int}}/I^{\mathrm{int}}$ is *flat* over $\mathfrak{o}_K$.

Notation 1.1.11. Define $I = I^{\mathrm{int}} \otimes_{\mathcal{O}_K} K$ and $I_\kappa = I^{\mathrm{int}} \otimes_{\mathcal{O}_K} \kappa$; the latter is an ideal in R_κ by the flatness hypothesis above. Choose $r_1, \dots, r_m \in I^{\mathrm{int}}$ which project to elements of a Gröbner basis $\bar{r}_1, \dots, \bar{r}_m$ of I_κ.

For $f \in R$, let $\boldsymbol{j}_f$ denote the minimal exponents of S in the expression (1.1.9) of f. Set $\boldsymbol{j}_I = \min\{\boldsymbol{j}_{r_h}; h = 1, \dots, m\}$; it is a nonpositive integer.

Notation 1.1.12. In this subsection, fix $\eta_0 \in (|\pi_K|^{-1/\boldsymbol{j}_I}, 1)$. We have $|\pi_K|\,\eta_0^{\boldsymbol{j}_I} < 1$.

Notation 1.1.13. Let $\mathscr{R}_{\eta_0}$ be the Fréchet completion of R for $|\cdot|_\eta$ for $\eta \in [\eta_0, 1)$. Let $R^{\mathrm{int}}_{\eta_0}$ denote $\{f \in \mathscr{R}_{\eta_0} \mid |f|_1 \leq 1\}$ and put $R_{\eta_0} = R^{\mathrm{int}}_{\eta_0} \otimes_{\mathscr{O}_K} K$ and $I_{\eta_0} = I \otimes_R R_{\eta_0}$.

Notation 1.1.14. For an element $f \in \mathscr{R}_{\eta_0}$ written as in (1.1.9) and $l \in \mathbb{Z}$, let $\pi_K^l f_{(l)}$ be the sum of all terms $f_{i_1,\dots,i_n,j} u_1^{i_1} \cdots u_n^{i_n} S^j$ for which $v_K(f_{i_1,\dots,i_n,j}) = l$. Thus, $f_{(l)} \in R^{\mathrm{int}}_{\eta_0}$; we use $\bar{f}_{(l)}$ denote its reduction in R_κ.

Lemma 1.1.15. *For $h = 1, \dots, m$ and $\eta \in [\eta_0, 1]$,*

$$|r_h|_\eta = 1, \qquad |r_{h,(l)}|_\eta \leq \eta^{\boldsymbol{j}_I} \quad \text{for } l \in \mathbb{Z}_{\geq 0}.$$

Proof. The equality follows from the choice of η_0 in Notation 1.1.12. The rest follows from the definition of $\boldsymbol{j}_I$ in Notation 1.1.11. □

Construction 1.1.16. For $f \in R_{\eta_0}$ with $|f|_1 = |\pi_K|^{l_0}$, the *division algorithm* is the following procedure. Put $f_{l_0} = f$. Given f_l for $l \geq l_0$, we apply Proposition 1.1.6 to write

$$\bar{f}_{l,(l)} = \bar{g}_{l,1}\bar{r}_1 + \cdots + \bar{g}_{l,m}\bar{r}_m + \bar{f}'_{l,(l)},$$

where $\bar{g}_{l,h} \in R_\kappa$ and $\mathrm{lead}(\bar{g}_{l,h}\bar{r}_h) \preceq \mathrm{lead}(\bar{f}_{l,(l)})$ for $h = 1, \dots, m$ and any term of $\bar{f}'_{l,(l)} \in R_\kappa$ is not divisible by any $\mathrm{lead}(\bar{r}_h)$. For each h, pick lifts $g_{l,h}$ of $\bar{g}_{l,h}$ in R^{int} so that $g_{l,h} = g_{l,h,(0)}$, that is, we only lift nonzero terms. Put

$$f_{l+1} = f_l - \pi_K^l (g_{l,1} r_1 + \cdots + g_{l,m} r_m).$$

Remark 1.1.17. The division algorithm depends on many choices, but we prove in Proposition 1.1.21 that the outcome $\lim_{l \to +\infty} f_l$ is uniquely determined by f.

Lemma 1.1.18. *At each step of the division algorithm, for $\eta \in [\eta_0, 1]$, $h = 1, \dots, m$, we have*

$$|g_{l,h}|_\eta \leq |f_{l,(l)}|_\eta, \quad |f_{l+1,(l')} - f_{l,(l')}|_\eta \begin{cases} \leq \eta^{\boldsymbol{j}_I} |f_{l,(l)}|_\eta & \text{if } l' > l, \\ \leq |f_{l,(l)}|_\eta & \text{if } l' = l, \\ = 0 & \text{if } l' < l. \end{cases} \tag{1.1.19}$$

Proof. The inequality on the left holds because $\mathrm{lead}(\bar{g}_{l,h}\bar{r}_h) \preceq \mathrm{lead}(\bar{f}_{l,(l)})$. The rest follows using Lemma 1.1.15. □

Corollary 1.1.20. *For $h = 1, \dots, m$, the series $g_h = \pi_K^{l_0} g_{l_0,h} + \pi_K^{l_0+1} g_{l_0+1,h} + \cdots$ converges under $|\cdot|_\eta$ for $\eta \in [\eta_0, 1)$. Consequently, $g_h \in R_{\eta_0}$ for $h = 1, \dots, m$.*

Proof. By Lemma 1.1.18,

$$\begin{aligned}
|\pi_K^l g_{l,h}|_\eta \leq |\pi_K^l f_{l,(l)}|_\eta &\leq |\pi_K|^l \max\{\eta^{\boldsymbol{j}_I} |f_{l-1,(l-1)}|_\eta, |f_{l-1,(l)}|_\eta\} \\
&\leq |\pi_K|^l \max\{\eta^{2\boldsymbol{j}_I} |f_{l-2,(l-2)}|_\eta, \eta^{\boldsymbol{j}_I} |f_{l-2,(l-1)}|_\eta, \eta^{\boldsymbol{j}_I} |f_{l-2,(l-2)}|_\eta, |f_{l-2,(l)}|_\eta\} \\
&\leq \cdots \\
&\leq |\pi_K|^l \max_{l' < l} \{\eta^{(l-l')\boldsymbol{j}_I} |f_{(l')}|_\eta\} \leq \max_{l' < l} \{(|\pi_K| \eta_0^{\boldsymbol{j}_I})^{l-l'} |\pi_K^{l'} f_{(l')}|_\eta\}.
\end{aligned}$$

This goes to zero as $l \to +\infty$. □

Proposition 1.1.21. *Keep the notation as above. The quantity $f - g_1 r_1 - \cdots - g_m r_m$ is the unique element of $f + I_{\eta_0}$ for which none of its terms is divisible by any* $\mathrm{Lead}(r_h)$.

Proof. It follows from the definition of $g_1, \ldots, g_m$ that no term of $f - \sum_{i=1}^m g_i r_i$ is divisible by any $\mathrm{Lead}(r_h)$.

Assume that $f \in R_{\eta_0}$ does not contain any term divisible by any of $\mathrm{Lead}(r_h)$, then we need to show that for any nonzero $g \in I_{\eta_0}$, there is a term in $f + g$ divisible by some of $\mathrm{Lead}(r_h)$. Assume the contrary. Let $n = \log_{|\pi_K|} |g|_1$. Then $\bar{g}_{(n)} \in I_\kappa$ does not contain any term which divides any of $\mathrm{lead}(\bar{r}_h)$. This forces $\bar{g}_{(n)} = 0$ because the leading term of any nonzero element in I_κ is divisible by some $\mathrm{lead}(\bar{r}_h)$. This is a contradiction. The lemma follows. $\square$

Lemma 1.1.22. *For $\eta \in [\eta_0, 1]$, $\left| f - \sum_{i=1}^m g_i r_i \right|_\eta$ equals the minimum η-norm of any element of $f + I_{\eta_0}$. Moreover, this continues to hold if we pass from R_{η_0} to its completion $R_{\eta_0}^{\wedge,\eta}$ under $|\cdot|_\eta$.*

Proof. For $\eta \in [\eta_0, 1]$, by Lemma 1.1.18, $|f_{l+1}|_\eta \le |f_l|_\eta$, so $\left| f - \sum_{i=1}^m g_i r_i \right|_\eta \le |f|_\eta$. By Proposition 1.1.21, starting with any element in $f + I_{\eta_0}$, the division algorithm will eventually lead to a unique element $f - \sum_{i=1}^m g_i r_i$; hence the first statement follows.

The second statement follows from the fact that any element in $f + I_{\eta_0} R_{\eta_0}^{\wedge,\eta}$ is a limit of elements in $f + I_{\eta_0}$. $\square$

Proposition 1.1.23. *Let f be a rigid analytic function on the space*

$$X_{\eta_0} = \left\{ (u_1, \ldots, u_n, S) \in \mathbb{A}_K^{n+1} \,\middle|\, \eta_0 \le |S| < 1;\ |u_1|, \ldots, |u_n| \le 1;\ r_1, \ldots, r_m = 0 \right\}.$$

Then the following are equivalent:

(a) *f is induced by an element of $R_{\eta_0}^{\mathrm{int}}$.*

(b) *There exists a function $r : [\eta_0, 1) \to \mathbb{R}$ with $\lim_{\eta \to 1^-} r(\eta) \le 1$, such that for each $\eta \in [\eta_0, 1)$, f lifts to an element of the $|\cdot|_\eta$-completion of R_{η_0} having η-norm less than or equal to $r(\eta)$.*

Proof. It is clear that (a) implies (b), so assume (b). We can write f as a Fréchet limit of the projections of some sequence of elements $f_1, f_2, \ldots$ of R, under the quotient norms associated with $|\cdot|_\eta$ for $\eta \in [\eta_0, 1)$. Use the division algorithm to write $f_l = g_{l,1} r_1 + \cdots + g_{l,m} r_m + h_l$ with $g_{l,1}, \ldots, g_{l,m}, h_l \in R_{\eta_0}$. Moreover, as $f_l - f_{l+1}$ tends to zero under the Fréchet topology, so does $h_l - h_{l+1}$ since it can be obtained from the division algorithm of $f_l - f_{l+1}$ and Lemma 1.1.18 ensures that $|f_l - f_{l+1}|_\eta \ge |h_l - h_{l+1}|_\eta$. Hence, the h_l form a Fréchet convergent sequence; denote the limit by h, which is a lift of f. Note that for a fixed η, $|h_l|_\eta$ equals the η-quotient norm of f_l, which in turn equals the η-quotient norm of f when l is large enough. Thus, $|h|_\eta \le r(\eta)$ for all $\eta \in [\eta_0, 1)$. Hence it lies in $R_{\eta_0}^{\mathrm{int}}$. $\square$

Notation 1.1.24. Define

$$A^{\mathrm{int}} = R^{\mathrm{int}}/I^{\mathrm{int}}, \quad A = R/I, \quad A_{\eta_0} = R_{\eta_0}/I_{\eta_0}, \quad A_\kappa = A^{\mathrm{int}} \otimes_{\mathfrak{o}_K} \kappa \cong R_\kappa/I_\kappa.$$

We may view A_κ as an affinoid algebra over $\kappa((S))$, whose corresponding rigid analytic space is denoted by X.

1.2. ***Quotient norms versus spectral norms.*** In this subsection, we compare spectral norms with the quotient norms discussed in previous section. As an application, we deduce that the connected components of $\boldsymbol{X}_{\eta_0}$ when $\eta_0 \to 1^-$ as a rigid space over K are the same as the connected components of X as a rigid space over $\kappa((S))$.

Hypothesis 1.2.1. In this subsection, we assume that A_κ is reduced.

Notation 1.2.2. Let $|\cdot|_{\kappa,\mathrm{quot}}$ denote the quotient norm on A_κ induced by the Gauss norm on R_κ. Let $|\cdot|_{\kappa,\mathrm{sp}} = \lim_{n\to+\infty} |\cdot^n|_{\kappa,\mathrm{quot}}^{1/n}$ be the spectral norm; it is a norm because A_κ is reduced. By [Bosch et al. 1984, Theorem 6.2.4/1], there exists $c > 0$ such that $|\cdot|_{\kappa,\mathrm{sp}} \le |\cdot|_{\kappa,\mathrm{quot}} \le |S|_\kappa^{-c}|\cdot|_{\kappa,\mathrm{sp}}$, where $|S|_\kappa$ is the norm of S in $\kappa((S))$.

Notation 1.2.3. In this subsection, we fix η_0 in the interval $(|\pi_K|^{1/(-\boldsymbol{j}_I+pc)}, 1)$. In particular, $|\pi_K|\eta_0^{\boldsymbol{j}_I} < \eta_0^{pc}$ and $\eta_0 > p^{-1/pc}$.

Notation 1.2.4. For $\eta \in [\eta_0, 1]$, let $|\cdot|_{\eta,\mathrm{quot}}$ denote the quotient norm on A_{η_0} or A induced by the η-Gauss norm on R_{η_0} or R. Similarly, we have the η-spectral seminorm $|\cdot|_{\eta,\mathrm{sp}} = \lim_{n\to+\infty} |\cdot^n|_{\eta,\mathrm{quot}}^{1/n}$; we will see in Lemma 1.2.6 that it is a norm.

Proposition 1.2.5. *The quotient norm $|\cdot|_{1,\mathrm{quot}}$ on A is the same as the spectral (semi)norm $|\cdot|_{1,\mathrm{sp}}$. As a consequence, the map $A^{\mathrm{int}} \to A_\kappa$ induces an isomorphism $A^\circ/A^{\circ\circ} \cong A_\kappa$, where $A^\circ = \{f \in A \mid |f|_{1,\mathrm{sp}} \le 1\}$ and $A^{\circ\circ} = \{f \in A \mid |f|_{1,\mathrm{sp}} < 1\}$.*

Proof. Since $A^{\mathrm{int}}/\mathfrak{m}_K A^{\mathrm{int}} = A_\kappa$ is reduced, by [Bosch et al. 1984, 6.2.1/4(iii)], the quotient norm on A is equal to the spectral seminorm, $A^\circ = A^{\mathrm{int}}$, and $A^{\circ\circ} = \mathfrak{m}_K A^{\mathrm{int}}$. This proves the claim. $\square$

Lemma 1.2.6. *For $\eta \in [\eta_0, 1)$, we have $|\cdot|_{\eta,\mathrm{sp}} \le |\cdot|_{\eta,\mathrm{quot}} \le \eta^{-pc/(p-1)}|\cdot|_{\eta,\mathrm{sp}}$ on A_{η_0}. The same is true when extending both norms to the completion of A_{η_0} with respect to $|\cdot|_{\eta,\mathrm{quot}}$ (which is the same as the completion with respect to the spectral norm). In particular, this shows that $|\cdot|_{\eta,\mathrm{sp}}$ is a norm on A_{η_0}.*

Proof. It suffices to show that for any $f \in A_{\eta_0}$, $|f^p|_{\eta,\mathrm{quot}} \ge \eta^{pc}|f|_{\eta,\mathrm{quot}}^p$; then it would follow that $|f^{p^n}|_{\eta,\mathrm{quot}} \ge \eta^{(p^n-1)pc/(p-1)}|f|_{\eta,\mathrm{quot}}^{p^n}$ for all $n \in \mathbb{N}$ by iteration, and hence the statement follows by taking the limit.

Pick a representative $\tilde{f}$ of f in R_{η_0} containing no terms divisible by any $\mathrm{Lead}(r_h)$ (hence by Proposition 1.1.21, $|\tilde{f}|_\eta = |f|_{\eta,\mathrm{quot}}$). Fixing $\eta \in [\eta_0, 1)$, we will show that

$$|\tilde{f}^p|_{\eta,\mathrm{quot}} = \Big|\sum_l (\pi_K^l \tilde{f}_{(l)})^p\Big|_{\eta,\mathrm{quot}} \ge \eta^{pc}|\tilde{f}|_\eta^p = \eta^{pc}|f|_{\eta,\mathrm{quot}}^p. \tag{1.2.7}$$

First, we remark that, given the middle inequality, the former equality follows; this is because $\tilde f^p - \sum_l (\pi_K^l \tilde f_{(l)})^p$ consists of products of $\pi_K^l \tilde f_{(l)}$ with an extra factor p from the multinomial coefficients. Then

$$\Big|\tilde f^p - \sum_l (\pi_K^l \tilde f_{(l)})^p\Big|_{\eta,\mathrm{quot}} \leq \Big|\tilde f^p - \sum_l (\pi_K^l \tilde f_{(l)})^p\Big|_{\eta} \leq p^{-1}|\tilde f|_\eta^p < \eta^{pc}|\tilde f|_\eta^p,$$

for $\eta \in [\eta_0, 1)$. So it suffices to prove the middle inequality in (1.2.7). For any l, we have

$$|(\bar{\tilde f}_{(l)})^p|_{\kappa,\mathrm{quot}} \geq |(\bar{\tilde f}_{(l)})^p|_{\kappa,\mathrm{sp}} = |\bar{\tilde f}_{(l)}|^p_{\kappa,\mathrm{sp}} \geq |S|_\kappa^{pc} \cdot |\bar{\tilde f}_{(l)}|^p_{\kappa,\mathrm{quot}}.$$

Let $(\tilde f_{(l)})^p = g_{l,1} r_1 + \cdots + g_{l,m} r_m + h_l$ be the result of the first step of applying the division algorithm to $(\tilde f_{(l)})^p$. Then $\log_\eta |h_{l,(0)}|_\eta = \log_{|S|_\kappa} |(\bar{\tilde f}_{(l)})^p|_{\kappa,\mathrm{quot}}$ and hence $|h_{l,(0)}|_\eta \geq \eta^{pc}|\tilde f_{(l)}|_\eta^p$. Moreover, by Lemma 1.1.18, $|h_l - h_{l,(0)}|_\eta \leq \eta^{j_l}|\pi_K||\tilde f_{(l)}|_\eta^p < \eta^{pc}|\pi_K|^{-pl}|\tilde f|_\eta^p$; this implies that $|h_{l,(0)}|_{\eta,\mathrm{quot}} = |h_{l,(0)}|_\eta$.

Now, we can write

$$\sum_l (\pi_K^l \tilde f_{(l)})^p = \sum_l \pi_K^{pl} h_{l,(0)} + \sum_l \pi_K^{pl}(h_l - h_{l,(0)}) \tag{1.2.8}$$

in the quotient ring. The first term on the right-hand side of (1.2.8) has (quotient) norm at least $\eta^{pc}|\tilde f|_\eta^p$ because none of the summands is divisible by any $\mathrm{Lead}(r_h)$. In contrast, the latter term on the right-hand side of (1.2.8) has norm strictly less than $\eta^{pc}|\tilde f|_\eta^p$. Thus, the inequality in (1.2.7) holds. □

Remark 1.2.9. It is attractive to think that $|\cdot|_{\eta,\mathrm{sp}} \leq |\cdot|_{\eta,\mathrm{quot}} \leq \eta^{-c}|\cdot|_{\eta,\mathrm{sp}}$ when $\eta \to 1^-$. However, the best we know is that for any $c' > c$, we have an ϵ depending on c', for which $|\cdot|_{\eta,\mathrm{sp}} \leq |\cdot|_{\eta,\mathrm{quot}} \leq \eta^{-c'}|\cdot|_{\eta,\mathrm{sp}}$ for all $\eta \in [\epsilon, 1)$.

Corollary 1.2.10. *For a rigid analytic function f on $\boldsymbol{X}_{\eta_0}$, the following are equivalent.*

(a) *f is an element in $A^{\mathrm{int}}_{\eta_0}$.*

(b) *There exists a function $r : [\eta_0, 1) \to \mathbb{R}$ with $\lim_{\eta\to 1} r(\eta) \leq 1$, such that for each $\eta \in [\eta_0, 1)$, $|f|_{\eta,\mathrm{sp}} \leq r(\eta)$.*

Proof. It follows from combining Lemma 1.2.6 with Proposition 1.1.23. □

Theorem 1.2.11. *There are one-to-one correspondences among the following sets*: (a) *the idempotent elements of A_κ*; (b) *the idempotent elements of $A^{\mathrm{int}}_{\eta_0}$*; (c) *the idempotent elements of A_{η_0}*; *and* (d) *the idempotent elements on $\boldsymbol{X}_{\eta_0}$*.

Proof. By Corollary 1.2.10, the sets (b), (c), and (d) are the same because idempotent elements have spectral norms 1. It suffices to match up (a) and (b). We have a map from the set of idempotent elements of $A_{\eta_0}^{\mathrm{int}}$ to the set of idempotent elements of A_κ by reducing modulo π_K. We first show the injectivity. Let $f, g \in R_{\eta_0}^{\mathrm{int}}$ be idempotents whose reductions modulo π_K are the same, i.e., $\bar{f} = \bar{g} \in A_\kappa$. This implies that $\bar{f}^{p-1} + \bar{f}^{p-2}\bar{g} + \cdots + \bar{g}^{p-1} = 0$ in A_κ. Since $f - g = f^p - g^p = (f-g)(f^{p-1} + f^{p-2}g + \cdots + g^{p-1})$, we have

$$\begin{aligned}|f-g|_{1,\mathrm{quot}} &= |(f-g)(f^{p-1}+f^{p-2}g+\cdots+g^{p-1})|_{1,\mathrm{quot}}\\ &\leq |f-g|_{1,\mathrm{quot}}\,|f^{p-1}+f^{p-2}g+\cdots+g^{p-1}|_{1,\mathrm{quot}} \leq |f-g|_{1,\mathrm{quot}}\,|\pi_K|.\end{aligned}$$

This forces $|f-g|_{1,\mathrm{quot}} = 0$ and hence $f = g$.

To prove surjectivity, we start with an idempotent $\bar{f} \in A_\kappa$, viewed as an element in R_κ with none of its terms divisible by any of $\mathrm{Lead}(\bar{r}_h)$; pick a lift $\tilde{f}_0 \in R^{\mathrm{int}}$ of $\bar{f}$ which only contains terms present in $\bar{f}$, and let $f_0 \in A^{\mathrm{int}}$ denote its image in A^{int}. If we set $\tilde{h}_0$ to the result of applying the division algorithm to $\tilde{f}_0^2 - \tilde{f}_0$ and $h_0 = f_0^2 - f_0$, then $|h_0|_{1,\mathrm{quot}} = |\tilde{h}_0|_{1,\mathrm{quot}} \leq |\pi_K|$ and $|h_0|_{\eta,\mathrm{quot}} = |\tilde{h}_0|_{\eta,\mathrm{quot}} \leq p^{-1}\eta^{-2c} < 1$ for all $\eta \in [\eta_0, 1)$, where the latter inequality holds because all terms in $\tilde{f}_0$ come from terms in $\bar{f}$ having norms at most $|\bar{f}|_{\kappa,\mathrm{quot}} \leq |S|_\kappa^{-c}|\bar{f}|_{\kappa,\mathrm{sp}} = |S|_\kappa^{-c}$. As in the proof of Hensel's lemma, we iteratively modify f_0 as follows. For $\alpha \geq 0$, we set $f_{\alpha+1} = f_\alpha + h_\alpha - 2h_\alpha f_\alpha$ and

$$h_{\alpha+1} := f_{\alpha+1}^2 - f_{\alpha+1} = (f_\alpha + h_\alpha - 2h_\alpha f_\alpha)^2 - (f_\alpha + h_\alpha - 2h_\alpha f_\alpha) = h_\alpha^2(4h_\alpha - 3).$$

Hence, $|h_{\alpha+1}|_{\eta,\mathrm{quot}} \leq |h_\alpha|_{\eta,\mathrm{quot}}^2$ for all $\eta \in [\eta_0, 1]$. Thus $|h_\alpha|_{\eta,\mathrm{quot}} \to 0$ as $\alpha \to +\infty$; hence f_α converges to an element $f \in A_{\eta_0}^{\mathrm{int}}$ which is idempotent. It is clear from the construction that the reduction of f modulo π_K is the same as $\bar{f}$. This proves the surjectivity. □

Corollary 1.2.12. *When $\eta_0 \in p^{\mathbb{Q}}$, there is a one-to-one correspondence between the connected components of X and those of $\boldsymbol{X}_{\eta_0}$.*

Remark 1.2.13. This is the first place where we need the rationality of $\log_p \eta_0$ to ensure that we are in the classical rigid analytic space setting to talk about connected components [Bosch et al. 1984, 9.1.4/8].

1.3. ***Lifting construction.*** In order to apply the results from the previous two subsections later in the paper, we, reversing the picture, start with a rigid analytic space X and try to construct $\boldsymbol{X}_{\eta_0}$ from it.

Let κ and K be as before.

Definition 1.3.1. Let X be a *reduced* affinoid rigid space over $\kappa((S))$ with ring of analytic functions $A_\kappa = R_\kappa / I_\kappa$ where $R_\kappa = \kappa((S))\langle u_1, \ldots, u_n\rangle$ and I_κ is some ideal. The *lifting construction* refers to the following.

(1) Find an ideal I^{int} in $R^{\mathrm{int}} = K\langle u_1, \dots, u_n\rangle((S))$ so that $R^{\mathrm{int}}/I^{\mathrm{int}}$ is *flat* over $\mathcal{O}_K$ and $I^{\mathrm{int}} \otimes_{\mathcal{O}_K} \kappa = I_\kappa$.

(2) Choose a Gröbner basis of I_κ, lift its elements to $r_1, \dots, r_m \in I^{\mathrm{int}}$ as in Notation 1.1.11, and define η_0 as in Notation 1.2.3.

(3) We call the rigid analytic space

$$\boldsymbol{X}_{\eta_0} = \left\{(u_1, \dots, u_n, S) \in \mathbb{A}_K^{n+1} \;\middle|\; \eta_0 \le |S| < 1;\, |u_1|, \dots, |u_n| \le 1;\, r_1, \dots, r_m = 0\right\}$$

the *lifting space* of X; it depends only on the choice of I^{int} and η_0.

Remark 1.3.2. We do not know if such a lifting space exists in general. The only obstruction is finding an ideal I^{int} lifting I_κ such that $R^{\mathrm{int}}/I^{\mathrm{int}}$ is flat over $\mathcal{O}_K$.

Question 1.3.3. It would be interesting to know if this lifting construction can be globalized for arbitrary rigid spaces over $\kappa((S))$. In particular, given a morphism between two rigid spaces over $\kappa((S))$, can we lift the morphism (noncanonically) to a morphism between (some strict neighborhood of) their lifting spaces? Can we "glue" the lifting spaces up to homotopy? This situation is very similar to Berthelot's construction [1996] of rigid cohomology.

For an affinoid subdomain of a polydisc, we explicate this lifting process.

Example 1.3.4. Let $p_1, \dots, p_m \in \kappa[\![S]\!][u_1, \dots, u_n]$ be polynomials and take $a_1, \dots, a_m \in \mathbb{N}$. Consider the following affinoid subdomain of the unit polydisc:

$$X = \left\{(u_1, \dots, u_n) \in \mathbb{A}^n_{\kappa((S))} \;\middle|\; |u_1|, \dots, |u_n| \le 1;\, |p_1| \le |S|^{a_1}, \dots, |p_m| \le |S|^{a_m}\right\}.$$

The ring of analytic functions on X is

$$\kappa((S))\langle u_1, \dots, u_n, v_1, \dots, v_m\rangle \big/ (v_1 S^{a_1} - p_1, \dots, v_m S^{a_m} - p_m).$$

For each i, let P_i be a lift of p_i in $\mathcal{O}_K[\![S]\!][u_1, \dots, u_n]$ (here we allow P_i to have new terms other than the terms of p_i). We claim that the ring

$$\mathcal{O}_K\langle u_1, \dots, u_n, v_1, \dots, v_m\rangle((S)) \big/ (v_1 S^{a_1} - P_1, \dots, v_m S^{a_m} - P_m) \tag{1.3.5}$$

is flat over $\mathcal{O}_K$. This is because the ring

$$\mathcal{O}_K((S))[u_1, \dots, u_n, v_1, \dots, v_m] \big/ (v_1 S^{a_1} - P_1, \dots, v_m S^{a_m} - P_m),$$

being isomorphic to $\mathcal{O}_K((S))[u_1, \dots, u_n]$, is flat and hence torsion-free over $\mathcal{O}_K$, and (1.3.5) is its completion with respect to the topology induced by the various $(p, S)^r \mathcal{O}_K[\![S]\!][u_1, \dots, u_n, v_1, \dots, v_m]$, for $r \in \mathbb{N}$. Therefore, by Definition 1.3.1,

$$\boldsymbol{X}_{\eta_0} = \Big\{(u_1, \dots, u_n, S) \in \mathbb{A}_K^{n+1} \;\Big|\; \eta_0 \le |S| < 1,\; |u_1|, \dots, |u_n| \le 1,\\ |P_1| \le |S|^{a_1}, \dots, |P_m| \le |S|^{a_m}\Big\}$$

is a lifting space for X, for some $\eta_0 \in (0, 1)$.

2. Differential conductors

In this section, we recall the definition of differential Swan conductors following [Kedlaya 2007]. Along the way, we define the differential Artin conductors using a slightly different normalization.

2.1. ***Setup.*** Recall that we do not use any notation from the previous section.

Convention 2.1.1. Let J be an index set. We write e_J for a tuple $(e_j)_{j\in J}$. For an element x, we use x^{e_J} to denote $(x^{e_j})_{j\in J}$. For another tuple b_J, we set $b_J^{e_J} = \prod_{j\in J} b_j^{e_j}$ if only a finite number of e_j are nonzero. We also use $\sum_{e_J=0}^n$ to mean the sum over $e_j \in \{0, 1, \dots, n\}$ for each $j \in J$, only allowing finitely many summands to be nonzero.

Definition 2.1.2. For a finite field extension l/k of characteristic $p > 0$, a *p-basis* of l over k is a set $(c_j)_{j\in J} \subset l$ such that $c_J^{e_J}$, where $e_j \in \{0, 1, \dots, p-1\}$ for all $j \in J$ and $e_j = 0$ for all but a finite number of j, form a basis of the vector space l over kl^p. By a *p-basis* of l we mean a p-basis of l over l^p; it is an empty set if and only if l is perfect. (For more details, see [Eisenbud 1995, p. 565] or [Grothendieck 1964, Ch. 0, §21].)

Remark 2.1.3. For a p-basis $c_J \subset l$, the dc_J form a basis for the differentials Ω^1_l as an l-vector space.

Convention 2.1.4. Throughout this paper, all differentials are p-adically continuous. In other words, for a continuous homomorphism $A \to B$ of p-adic rings, $\Omega^1_{B/A}$ is the relative p-adically continuous differentials. Sometimes, we may use in the notation the corresponding geometric objects, such as the rigid space $\mathrm{Max}(B)$, instead of A or B. When $A = \mathbb{Z}_p$, we may suppress it from the notation, writing simply Ω^1_B.

For a homomorphism $A \to B$ between rings, a *∇-module* or a *differential module* over B *relative to* A is a finite projective B-module M equipped with an integrable connection $\nabla : M \to M \otimes \Omega^1_{B/A}$. Sometimes, we may use the corresponding geometric objects instead of A or B in the notation. When $A = \mathbb{Z}_p$, we may omit the reference to the base ring.

Notation 2.1.5. Let k be a complete discretely valued field of equal characteristic $p > 0$. Denote its ring of integers, maximal ideal, and residue field by $\mathbb{O}_k$, $\mathfrak{m}_k$, and κ_k, respectively. Fix a uniformizer s and a noncanonical isomorphism

$$\kappa_k((s)) \simeq k. \tag{2.1.6}$$

Let $v_k(\cdot)$ denote the valuation, normalized so that $v_k(s) = 1$. Let $(\bar{b}_j)_{j\in J}$ be a p-basis of κ_k, where J is an index set. Let b_j be the image of $\bar{b}_j$ in k under the isomorphism (2.1.6). Hence, $(db_j)_{j\in J}$ and ds form a basis of $\Omega^1_{\mathbb{O}_k/\mathbb{F}_p}$. We set $\kappa_0 = \bigcap_{n>0} k^{p^n} \cong \bigcap_{n>0} \kappa_k^{p^n}$; it is a perfect field.

Notation 2.1.7. Let $\mathbb{O}_K$ denote the Cohen ring of κ_k with respect to $(\bar{b}_j)_{j\in J}$ and let $(B_j)_{j\in J} \subset \mathbb{O}_K$ be the canonical lifts of the p-basis. (For more about Cohen rings, see [Kedlaya 2007, §3.1] or [Whitney 2002].) Let $K = \operatorname{Frac} \mathbb{O}_K$. We use $\mathbb{O}_{K_0}$ to denote the ring of Witt vectors $W(\kappa_0)$ of κ_0, as a subring of $\mathbb{O}_K$. Let $K_0 = \operatorname{Frac} \mathbb{O}_{K_0}$.

We insert here a proposition discussing the functoriality of Cohen rings. For a more detailed study of functoriality of Cohen rings, see [Whitney 2002].

Proposition 2.1.8. *Keep the notation as above and let R be a complete Noetherian local ring with the maximal ideal $\mathfrak{m}$ containing p. Assume that we have a homomorphism $\overline{\psi} : \kappa_k \hookrightarrow R/\mathfrak{m}$. Then, for any $B'_J \subseteq R$ lifting $\overline{\psi}(\bar{b}_J)$, there exists a unique continuous homomorphism $\psi : \mathbb{O}_K \to R$ lifting $\overline{\psi}$ and sending B_j to B'_j for all $j \in J$.*

Proof. For any $n \in \mathbb{N}$, a *level-n expression* of an element $g \in \mathbb{O}_K$ is a (noncanonical) way of writing g as

$$g = \sum_{i,i'\geq 0} \sum_{e_J=0}^{p^n-1} p^i A_{i,i',e_J}^{p^n} B_J^{e_J} \tag{2.1.9}$$

for some $A_{i,i',e_J} \in \mathbb{O}_K$ and for a fixed i, $A_{i,i',e_J} = 0$ when $i' \gg 0$ for all e_J. Then we set

$$\psi_n(g) = \sum_{i,i'\geq 0} \sum_{e_J=0}^{p^n-1} p^i \tilde{A}_{i,i',e_J}^{p^n} B_J'^{e_J}$$

where $\tilde{A}_{i,i',e_J}$ is some lift of $\overline{\psi}(a_{i,i',e_J})$ in R with a_{i,i',e_J} being the reduction of A_{i,i',e_J} in κ_k. Different choices of lifts $\tilde{A}_{i,i',e_J}$ may change the definition of $\psi_n(g)$ by an element in $\mathfrak{m}^n$; a different level-n expression as in (2.1.9) may also vary $\psi_n(g)$ by some element in $\mathfrak{m}^n$. If $n \geq 1$, we can rewrite a level-n expression of g as in (2.1.9) in the form

$$g = \sum_{i,i'\geq 0} \sum_{e'_J=0}^{p-1} \sum_{e_J=0}^{p^{n-1}-1} p^i (A_{i,i',e_J+p^{n-1}e'_J}^{p} B_J^{e'_J})^{p^{n-1}} B_J^{e_J},$$

lowering the level by 1. From this we conclude that $\psi_n(g) \equiv \psi_{n-1}(g) \bmod \mathfrak{m}^{n-1}$. Taking $n \to \infty$, we get our map $\psi(g) = \lim_{n\to\infty} \psi_n(g)$. It is not hard to check that ψ is actually a homomorphism; this is because for $g, h \in \mathbb{O}_K$, the formal sum and product of level-n expressions of g and h are level-n expressions of $g+h$ and gh, respectively.

To prove the uniqueness, take another continuous homomorphism $\psi' : \mathbb{O}_K \to R$ satisfying all the conditions. Then, for a level-n expression of g as in (2.1.9),

$$\psi'\Big(\sum_{i,i'\geq 0} \sum_{e_J=0}^{p^n-1} p^i A_{i,i',e_J}^{p^n} B_J^{e_J}\Big) = \sum_{i,i'\geq 0} \sum_{e_J=0}^{p^n-1} p^i \psi'(A_{i,i',e_J})^{p^n} B_J'^{e_J}$$

is exactly one possible definition for ψ_n. As we proved above, $\psi'(g) \equiv \psi_n(g) \equiv \psi(g) \bmod \mathfrak{m}^n$. Let $n \to \infty$ and we have $\psi = \psi'$. $\square$

Corollary 2.1.10. *Suppose $J = \{1, \dots, m\}$. There exists a unique continuous homomorphism $\psi : \mathbb{O}_K \to \mathbb{O}_K[\![\delta_1, \dots, \delta_m]\!]$ such that for all $j \in J$, $\psi(B_j) = B_j + \delta_j$ and for any $g \in \mathbb{O}_K$, $\psi(g) - g$ lies in the ideal generated by $\delta_1, \dots, \delta_m$. Moreover, ψ is an $\mathbb{O}_{K_0}$-homomorphism.*

Proof. The first statement follows from previous proposition. By the functoriality of Witt vectors, ψ has to be identity when restricted to $\mathbb{O}_{K_0}$ because κ_0 is perfect. Hence, ψ is an $\mathbb{O}_{K_0}$-homomorphism. $\square$

Corollary 2.1.11. *Assume that κ_k has a finite p-basis b_J. Fix $j \in J$ and let $b'_j \in \mathbb{O}_k$ be an element such that $b'_j \equiv b_j \pmod{\mathfrak{m}_k}$. Then there exists an automorphism $g^* : k \to k$ such that $g^*(s) = s$, $g^*(b_j) = b'_j$, and $g^*(b_{J\setminus j}) = b_{J \setminus j}$.*

Proof. Applying Proposition 2.1.8 to $R = \kappa_k[\![s]\!]$ and $\mathfrak{m} = (s)$ gives us a homomorphism $g^* : \mathbb{O}_K/(p) = \kappa_k \to k[\![s]\!]$ such that $g^*(b_j) = b'_j$, and $g^*(b_{J\setminus j}) = b_{J\setminus j}$. One can extend this to an automorphism $g^* : k \to k$ by setting $g^*(s) = s$. $\square$

2.2. ***Construction of differential modules.*** In this subsection we review Tsuzuki's construction [2002] of differential modules over the Robba ring associated with p-adic Galois representations. For a systematic treatment, one may consult, for example, [Kedlaya 2007, §3].

Notation 2.2.1. Keep the notation as in the previous subsection. Fix a separable closure k^{sep} of k and let $G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ be the absolute Galois group of k.

For a (not necessarily algebraic) separable extension l/k of complete discretely valued fields, the *naïve ramification degree e* is the index of the valuation group of k in that of l; note that this might not be the same as the usual ramification degree because the inseparable part of the residue field extension κ_l/κ_k is not counted in. We say l/k is *tamely ramified* if $p \nmid e$ and the residue field extension is algebraic and separable. Moreover, if $e = 1$, we say that l/k is *unramified*.

Notation 2.2.2. By a *representation* of G_k, we mean a continuous homomorphism $\rho : G_k \to \mathrm{GL}(V_\rho)$, where V_ρ is a vector space over a (topological) field F of characteristic zero. We say that ρ is a *p-adic representation* if F is a finite extension of $\mathbb{Q}_p$.

Let F be a finite extension of $\mathbb{Q}_p$. Let $\mathbb{O}$ and $\mathbb{F}_q$ denote its ring of integers and residue field, respectively, where q is a power of p. Write $\mathbb{Z}_q$ for the Witt vectors $W(\mathbb{F}_q)$ and $\mathbb{Q}_q$ for its fraction field. By an *$\mathbb{O}$-representation* of G_k, we mean a continuous homomorphism $\rho : G_k \to \mathrm{GL}(V_\rho)$ with V_ρ a finite free $\mathbb{O}$-module.

We always assume that $\mathbb{F}_q \subseteq \kappa_0$ (see Remark 2.4.2). Let $K' = KF$. Since $F/\mathbb{Q}_q$ is totally ramified, we have the ring of integers $\mathbb{O}_{K'} \cong \mathbb{O}_K \otimes_{\mathbb{Z}_q} \mathbb{O}$. Let $v_{K'}$ denote the valuation on K' normalized so that $v_{K'}(p) = 1$.

Notation 2.2.3. Let C_k be the Cohen ring of k relative to the p-basis $\{(b_j)_{j\in J}, s\}$. By the functoriality of Cohen rings (Proposition 2.1.8), C_k has a natural structure as an $\mathbb{O}_K$-algebra, via the isomorphism (2.1.6). In particular, the (canonical) lifts of $(b_j)_{j\in J}$ in C_k are $(B_j)_{j\in J}$. We denote the canonical lift of s in C_k by S.

Put $\Gamma = C_k \otimes_{\mathbb{Z}_q} \mathbb{O}$; it is a complete discrete valuation ring since $\mathbb{O}$ is totally ramified over $\mathbb{Z}_q$. It carries a Frobenius structure ϕ lifting the q-th power Frobenius on k which acts trivially on $\mathbb{O}$.

Definition 2.2.4. Let $\sigma : R \to R$ be an endomorphism. A (σ, ∇)-*module* over R is a ∇-module over R (relative to $\mathbb{Z}_p$) equipped with an isomorphism $\sigma^* M \to M$ of ∇-modules.

Definition 2.2.5. For every $\mathbb{O}$-representation $\rho : G_k \to \mathrm{GL}(V_\rho)$, define its associated (ϕ, ∇)-module over Γ by

$$D(\rho) = (V_\rho \otimes_{\mathbb{O}} \widehat{\Gamma^{\mathrm{unr}}})^{G_k},$$

where $\widehat{\Gamma^{\mathrm{unr}}}$ is the p-adic completion of the maximal unramified extension of Γ. All ∇-modules we encounter in this section are relative to $\mathbb{Z}_p$, so we omit the reference to the base ring $\mathbb{Z}_p$ in the notation.

Proposition 2.2.6. *For any Frobenius lift ϕ on Γ, the functor D from $\mathbb{O}$-representations of G_k to (ϕ, ∇)-modules over Γ is an equivalence of categories.*

Proof. For the convenience of the reader, we briefly describe the functor here; for more details, one may consult [Kedlaya 2007, Propositions 3.2.7 and 3.2.8]. It is well-known that D establishes an equivalence between the category of representations and the category of ϕ-modules over Γ (finite free Γ-modules with semilinear ϕ-actions), with $V(M) = (M \otimes_\Gamma \widehat{\Gamma^{\mathrm{unr}}})^{\phi=1}$ as the inverse. The nontrivial part is that every ϕ-module over Γ admits a unique structure of (ϕ, ∇)-module; this involves a standard approximation argument. □

Definition 2.2.7. Let $I_k = \mathrm{Gal}(k^{\mathrm{sep}}/k^{\mathrm{unr}})$ be the inertia subgroup of G_k, where k^{unr} is the maximal unramified extension of k in k^{sep}. We say that an ($\mathbb{O}$-)representation ρ has *finite local monodromy* if the image $\rho(I_k)$ is finite.

For an $\mathbb{O}$-representation ρ of finite monodromy, one can refine the (ϕ, ∇)-module associated with ρ as follows.

Construction 2.2.8. Since C_k has an $\mathbb{O}_K$-algebra structure, any element $x \in \Gamma$ can be uniquely written in the form of $\sum_{i\in\mathbb{Z}} x_i S^i$ for $x_i \in \mathbb{O}_K \otimes_{\mathbb{Z}_q} \mathbb{O} = \mathbb{O}_{K'}$ such that the indices i for which $v_{K'}(x_i) \leq n$ are bounded below.

For $r > 0$, put $\Gamma^r = \{x \in \Gamma \mid \lim_{n\to-\infty} v_{K'}(x_n) + rn = \infty\}$ and $\Gamma^\dagger = \bigcup_{r>0} \Gamma^r$; the latter is commonly known as the *integral Robba ring* over K'. It is not hard to show that the Frobenius ϕ preserves $\Gamma^\dagger$ and that $\Omega^1_{\Gamma^\dagger/\mathbb{O}} = \bigoplus_{j\in J} \Gamma^\dagger dB_j \oplus \Gamma^\dagger dS$. Also, $\Gamma^\dagger$ is a Henselian discrete valuation ring as cited in Lemma 2.2.10.

Since $\mathbb{O}_{K'} \hookrightarrow \Gamma^\dagger$, we can identify $\mathbb{O}_{K'}^{\mathrm{unr}} \hookrightarrow (\Gamma^\dagger)^{\mathrm{unr}}$, where the superscript unr means taking the maximal unramified extensions of discrete valuation rings. Put

$$\tilde{\Gamma}^\dagger = \widehat{\mathbb{O}_K^{\mathrm{unr}}} \otimes_{\mathbb{O}_K^{\mathrm{unr}}} (\Gamma^\dagger)^{\mathrm{unr}} \subset \widehat{\Gamma^{\mathrm{unr}}},$$

where we take the p-adic completion. For a p-adic representation ρ with finite local monodromy, define

$$D^\dagger(\rho) = D(\rho) \cap (V_\rho \otimes_{\mathbb{O}} \tilde{\Gamma}^\dagger) = (V_\rho \otimes_{\mathbb{O}} \tilde{\Gamma}^\dagger)^{G_k}. \tag{2.2.9}$$

Lemma 2.2.10 [Kedlaya 2005, Proposition 3.20]. *The integral Robba ring $\Gamma^\dagger$ is a henselian discrete valuation ring.*

Theorem 2.2.11 [Kedlaya 2007, Theorem 3.3.6]. *Let ϕ be a Frobenius lift on Γ acting on $\Gamma^\dagger$. Then $D^\dagger$ induces an equivalence between the category of $\mathbb{O}$-representations with finite local monodromy and the category of (ϕ, ∇)-modules over $\Gamma^\dagger$.*

Notation 2.2.12. For $I \subset [0, +\infty)$ an interval, let $A_K^1(I)$ denote the annulus (centered at the origin) with radii in I. We do not impose any rationality condition on the endpoints of I, so this space should be viewed as an analytic space in the sense of [Berkovich 1990]. If $I = [\alpha, \beta]$, we write $A_K^1[\alpha, \beta]$ for $A_K^1([\alpha, \beta])$.

For $0 \leq \alpha \leq \beta < \infty$, let $K\langle \alpha/t, t/\beta\rangle$ denote the ring of analytic functions on $A_K^1[\alpha, \beta]$. (If $\alpha = 0$, we write $K\langle t/\beta\rangle$ instead.) For $\eta \in [\alpha, \beta]\backslash\{0\}$, the ring $K\langle \alpha/t, t/\beta\rangle$ admits an η-Gauss norm: for $f = \sum_{i\in\mathbb{Z}} a_i x^i \in K\langle \alpha/t, t/\beta\rangle$,

$$|f|_\eta = \max_{i\in\mathbb{Z}}\{|a_i|\eta^i\}.$$

Notation 2.2.13. For $\eta_0 \in (0, 1)$, we use $Z_k^{\geq\eta_0}$ as a shorthand for $A_K^1[\eta_0, 1)$. Denote the ring of analytic functions on it by $\mathcal{R}_K^{\eta_0}$. We define the *Robba ring over K* to be $\mathcal{R}_K = \bigcup_{\eta\in[\eta_0,1)} \mathcal{R}_K^\eta$. Also let $\mathcal{R}_{K'}^{\eta_0} = \mathcal{R}_K^{\eta_0} \otimes_{\mathbb{Q}_q} F$ and $\mathcal{R}_{K'} = \mathcal{R}_K \otimes_{\mathbb{Q}_q} F$. We will only be interested in the behavior when η_0 is close to 1.

Remark 2.2.14. We use k in the subscript of $Z_k^{\geq\eta_0}$ because the space is functorial in k but not in K, as we made a noncanonical choice in (2.1.6).

Now, we restrict the (ϕ, ∇)-module $D^\dagger(\rho)$ to the Robba ring over K as follows.

Construction 2.2.15. Consider the natural injection $\Gamma^\dagger \hookrightarrow \mathcal{R}_{K'}$. Note that the Frobenius ϕ extends by continuity to $\mathcal{R}_{K'}$. Thus, from an $\mathbb{O}$-representation ρ with finite local monodromy, we obtain a differential module $\mathscr{E}_\rho = D^\dagger(\rho) \otimes_{\Gamma^\dagger} \mathcal{R}_{K'}$ over $\mathcal{R}_{K'}$.

Moreover, if we start with a p-adic representation $\rho : G_k \to \mathrm{GL}(V_\rho)$ of finite local monodromy, we can choose an $\mathbb{O}$-lattice V_ρ^{int} of V_ρ stable under the action of G_k. Then we associate a differential module $\mathscr{E}_\rho$ with the $\mathbb{O}$-representation given by V_ρ^{int}. It is clear that $\mathscr{E}_\rho$ does not depend on the choice of the lattice V_ρ^{int}. We call $\mathscr{E}_\rho$ the *differential module associated to ρ*.

Proposition 2.2.16 [Kedlaya 2007, Proposition 3.5.1]. *The (ϕ,∇)-module $\mathscr{E}_\rho$ over $\mathscr{R}_{K'}$ does not depend on the choice of the p-basis (up to a canonical isomorphism).*

Proposition 2.2.17. *The differential module $\mathscr{E}_\rho$ descends to a differential module over $\mathscr{R}_{K'}^{\eta_0}$ for some $\eta_0 \in (0,1)$.*

Proof. Defining a differential module requires only a finite amount of data. So, we can realize it on a certain annulus. See [Kedlaya 2007, Remark 3.4.1]. □

Remark 2.2.18. We will often make η_0 closer to 1^- in proving the main theorems. We will see later that all we care about is the asymptotic behavior of $\mathscr{E}_\rho$ as $\eta_0 \to 1^-$.

Remark 2.2.19. The current construction of associating a differential module with a representation (Constructions 2.2.8 and 2.2.15) is *not* functorial with respect to the base field F of the representation. If F' is a finite extension of F, for a p-adic representation ρ over F of finite local monodromy, one can naturally obtain $\rho\otimes_F F'$ as a p-adic representation over F'. Assume that κ_k contains the residue field $\mathbb{F}_{q'}$ of F'. Then the differential modules associated with ρ and $\rho\otimes_F F'$ are the same if F'/F is unramified and $\mathscr{E}_\rho \otimes_F F' = \mathscr{E}_{\rho\otimes_F F'}$ if F'/F is totally ramified.

There are two reasons for keeping this nonfunctoriality flaw. For one, the differential conductors we define later will be the same if we change ρ to $\rho\otimes_F F'$. For the other, if we define $\mathscr{E}_\rho$ using the tensor over $\mathbb{Z}_p$ instead of $\mathbb{Z}_q$ in Notation 2.2.3, in which case we do have the functoriality, we will get the direct sum of $[\mathbb{F}_q:\mathbb{F}_p]$ copies of $\mathscr{E}_\rho$ as differential modules. When proving the integrality of Swan conductors, we have to come back to study $\mathscr{E}_\rho$ because $K\otimes_{\mathbb{Z}_p}\mathbb{O} \simeq K'^{\oplus[\mathbb{F}_q:\mathbb{F}_p]}$ is not a field if $q>p$.

2.3. *Differential conductors.* Given a p-adic representation ρ of finite local monodromy, Kedlaya [2007, §3.5] showed that one can define a differential Swan conductor for ρ, using the p-adic differential module associated with ρ. In this subsection, we review this definition and give an analogous definition for the differential Artin conductor.

Remark 2.3.1. Starting from this subsection, the Frobenius ϕ plays almost no role in our theory; most of the arguments work for solvable differential modules [Kedlaya 2007, Definition 2.5.1], and since all the decompositions for differential modules we encounter are canonical, they automatically respect the Frobenius structure. The only place we need Frobenius is to link back with representations; see Proposition 2.3.22.

Hypothesis 2.3.2. In this subsection, we make an auxiliary hypothesis that k admits a *finite* p-basis $\{b_1,\dots,b_m,s\}$.

Notation 2.3.3. Let $J=\{1,\dots,m\}$ for notational convenience. We save the letters j and m for indexing the p-basis, except in Section 4.1 (see Notation 4.1.2). We also use J^+ to denote $J\cup\{0\}$, where 0 refers to the uniformizer s in the p-basis.

Definition 2.3.4. Let E be a differential field of order 1 and characteristic zero, i.e., a field of characteristic zero equipped with a derivation ∂. Assume that E is complete for a nonarchimedean norm $|\cdot|$. Let M be a finite differential module over E, i.e., a finite dimensional E-vector space equipped with an action of ∂ satisfying the Leibniz rule. The *spectral norm of* ∂ *on* M is defined to be

$$|\partial|_{M,\mathrm{sp}} = \lim_{n\to\infty} |\partial^n|_M^{1/n}$$

for any norm $|\cdot|_M$ on M; it does not depend on the choice of $|\cdot|_M$. One can prove that $|\partial|_{M,\mathrm{sp}} \geq |\partial|_{E,\mathrm{sp}}$ [Kedlaya 2010, Lemma 6.2.4].

Remark 2.3.5. For a complete extension E' of E, to which the derivation ∂ extends, $M \otimes_E E'$ can be viewed as a differential module over E' with spectral norm $|\partial|_{M\otimes_E E',\mathrm{sp}} = \max\{|\partial|_{M,\mathrm{sp}}, |\partial|_{E',\mathrm{sp}}\}$.

Notation 2.3.6. Let $\partial_0 = \partial/\partial S$, $\partial_1 = \partial/\partial B_1, \dots, \partial_m = \partial/\partial B_m$ denote the elements of a dual basis of $\Omega^1_{\mathcal{O}_K[\![S]\!]/\mathcal{O}_{K_0}}$ with respect to $dS, dB_1, \dots, dB_m$; they also give a dual basis of $\Omega^1_{\mathcal{R}^{\eta_0}_{K'}/K_0}$ for all $\eta_0 \in (0, 1)$. For a (ϕ, ∇)-module $\mathscr{E}$ over $\mathcal{R}^{\eta_0}_{K'}$, these differential operators act on $\mathscr{E}$, commuting with each other and commuting with the Frobenius action.

Notation 2.3.7. For $\eta \in [\alpha, \beta] \subset (0, +\infty)$, we denote by F'_η the completion of $\mathrm{Frac}(K'\langle \alpha/t, t/\beta\rangle)$ with respect to the η-Gauss norm; this does not depend on the choices of α and β.

Example 2.3.8. For $\eta \in \mathbb{R}_{>0}$, the operator norms of ∂_{J^+} and spectral norms on F'_η are as follows.

$$|\partial_j|_{F'_\eta} = \begin{cases} \eta^{-1} & \text{for } j = 0, \\ 1 & \text{for } j \in J; \end{cases} \qquad |\partial_j|_{F'_\eta,\mathrm{sp}} = \begin{cases} p^{-1/(p-1)}\eta^{-1} & \text{for } j = 0, \\ p^{-1/(p-1)} & \text{for } j \in J. \end{cases}$$

Definition 2.3.9. Let $\mathscr{E}$ be a ∇-module over $\mathcal{R}^{\eta_0}_{K'}$. For $\eta \in [\eta_0, 1)$, we set $\mathscr{E}_\eta = \mathscr{E} \otimes_{\mathcal{R}^{\eta_0}_{K'}} F'_\eta$, which inherits differential operators ∂_{J^+}. Define the (*nonlogarithmic*) *generic radius* (*of convergence*) $\boldsymbol{T}(\mathscr{E}, \eta)$ of $\mathscr{E}_\eta$ to be

$$\min\left\{\frac{p^{-1/(p-1)}}{|\partial_j|_{\mathscr{E}_\eta,\mathrm{sp}}};\ j \in J^+\right\}. \tag{2.3.10}$$

If $\mathscr{E}_{\eta,i}$ $(i = 1, \dots, n)$ are the Jordan–Hölder factors of $\mathscr{E}_\eta$ as a ∇-module over F'_η, we define the (*nonlogarithmic*) *radius multiset* $\boldsymbol{S}(\mathscr{E}, \eta)$ to be the set consisting of the generic radius of $\mathscr{E}_{\eta,i}$ with multiplicity $\dim_{F'_\eta} \mathscr{E}_{\eta,i}$ for each i.

We define the *logarithmic generic radius (of convergence)* $\boldsymbol{T}_{\log}(\mathscr{E}, \eta)$ to be

$$\min\left\{\frac{p^{-1/(p-1)}\eta^{-1}}{|\partial_0|_{\mathscr{E}_\eta,\mathrm{sp}}},\ \frac{p^{-1/(p-1)}}{|\partial_j|_{\mathscr{E}_\eta,\mathrm{sp}}};\ j \in J\right\}. \tag{2.3.11}$$

Similarly, we define the *logarithmic radius multiset* $\boldsymbol{S}_{\log}(\mathscr{E}, \eta)$ of $\mathscr{E}$.

Remark 2.3.12. We have $\boldsymbol{T}(\mathscr{E}, \eta) \leq \eta$; more generally, every element in $\boldsymbol{S}(\mathscr{E}, \eta)$ is less than or equal to η.

Remark 2.3.13. The logarithmic generic radius and logarithmic radius multiset are the same as the notions of the generic radius of convergence and radius multiset in [Kedlaya 2007].

Definition 2.3.14. For $j \in J^+$, we call ∂_j *dominant* for $\mathscr{E}_\eta$ if the minimum of $\boldsymbol{T}(\mathscr{E}, \eta)$ in (2.3.10) is achieved by the term involving the spectral norm of ∂_j. The term *log-dominant* is defined likewise, with reference to $\boldsymbol{T}_{\log}(\mathscr{E}, \eta)$ in (2.3.11).

Lemma 2.3.15. *For a (ϕ, ∇)-module $\mathscr{E}$ over $\mathscr{R}_{K'}^{\eta_0}$ and $j \in J^+$, there exists $\eta_0' \in (0, 1)$ such that one of the following two statements is true*:

- *For all $\eta \in [\eta_0', 1)$, ∂_j is (log-)dominant for $\mathscr{E}_\eta$.*
- *For all $\eta \in [\eta_0', 1)$, ∂_j is not (log-)dominant for $\mathscr{E}_\eta$.*

Proof. The logarithmic case is proved in [Kedlaya 2007, Lemma 2.7.5]. The proof for nonlogarithmic case is very similar. □

Definition 2.3.16. Keep the notation as in previous lemma. For $j \in J^+$, ∂_j is called *eventually (log-)dominant* for $\mathscr{E}$ if it is (log-)dominant for $\mathscr{E}_\eta$ for $\eta \to 1^-$.

Lemma 2.3.17. *Keep the notation as in Lemma 2.3.15. Assume that ∂_0 is* not *eventually dominant and ∂_j is. Consider the rotation $g^* : B_j \mapsto B_j + S$, $B_{J\setminus j} \mapsto B_{J\setminus j}$, and $S \mapsto S$ given by Proposition 2.1.8. Then $\partial_0 = \partial/\partial S$ is eventually dominant in $g^*\mathscr{E}$.*

Proof. Use the fact that the action of ∂_0 on $g^*\mathscr{E}$ is the pull-back of the action of $\partial_0 + \partial_j$ on $\mathscr{E}$. For details, see the proof of [Kedlaya 2007, Lemma 2.7.9]. □

Remark 2.3.18. The rotation g in the lemma corresponds to changing the isomorphism (2.1.6) so that $\bar{b}_j$ is sent to $b_j + s$ instead; such an isomorphism can be obtained by Corollary 2.1.11. In particular, if $\mathscr{E}_\rho$ comes from a p-adic representation ρ of finite local monodromy by Constructions 2.2.8 and 2.2.15, $g^*\mathscr{E}_\rho$ is the differential module associated with the same ρ using the aforementioned alternative isomorphism in place of (2.1.6).

Proposition 2.3.19. *The functions*

$$f(r) = \log \boldsymbol{T}(\mathscr{E}, e^{-r}) \quad \text{and} \quad f_{\log}(r) = \log \boldsymbol{T}_{\log}(\mathscr{E}, e^{-r})$$

on $(0, -\log \eta_0]$ are piecewise linear, concave functions with slopes in $\dfrac{1}{(\operatorname{rank} \mathscr{E})!}\mathbb{Z}$. They are linear in a neighborhood of 0.

Proof. The logarithmic case is proved in [Kedlaya 2007, §2.5]. For the nonlogarithmic case, the only difference is a factor η^{-1} in the spectral norm of ∂_0, which gives an extra linear term r. □

Definition 2.3.20. As a consequence of the previous proposition, there exists $b_{\mathrm{dif}}(\mathscr{E}) \in \mathbb{Q}_{\geq 0}$ and $\eta_0 \in (0,1)$ such that $\boldsymbol{T}(\mathscr{E}, \eta) = \eta^{b_{\mathrm{dif}}(\mathscr{E})}$ for all $\eta \in [\eta_0, 1)$. This $b_{\mathrm{dif}}(\mathscr{E})$ is called the (*nonlogarithmic*) *differential ramification break* of $\mathscr{E}$. We say that $\mathscr{E}$ has *uniform slope* b if the radius multiset $\boldsymbol{S}(\mathscr{E}, \eta)$ consists only of η^b when $\eta \to 1$. The notions of *logarithmic differential ramification break* $b_{\mathrm{dif,log}}(\mathscr{E})$ and *uniform log-slope* b are defined likewise, with reference to $\mathbf{T}_{\log}(\mathscr{E}, \eta)$ and $\mathbf{S}_{\log}(\mathscr{E}, \eta)$.

The ramification breaks give rise to the break decomposition.

Theorem 2.3.21. *Let $\mathscr{E}$ be a (ϕ, ∇)-module over $\mathscr{R}_{K'}^{\eta_0}$, for some $\eta_0 \in (0,1)$. Then after making η_0 sufficiently close to 1^-, there exists a* unique *decomposition of (ϕ, ∇)-modules $\mathscr{E} = \bigoplus_{b \in \mathbb{Q}_{\geq 1}} \mathscr{E}_b$ (resp. $\mathscr{E} = \bigoplus_{b \in \mathbb{Q}_{\geq 0}} \mathscr{E}_{b,\log}$) over $\mathscr{R}_{K'}^{\eta_0}$, where each of $\mathscr{E}_b$ (resp. $\mathscr{E}_{b,\log}$) has uniform slope (resp. log-slope) b.*

Proof. Since the differential operators act trivially on $\mathbb{O}$ and commute with ϕ, It suffices to obtain the decomposition of $\mathscr{E}$ as a ∇-module over $A_{K'}^1[\eta_0, 1)$; the uniqueness of the decomposition of $\mathscr{E}$ follows from the uniqueness of that over F_η' for $\eta \in [\eta_0, 1)$. The logarithmic part of this theorem is proved in [Kedlaya 2007, Theorem 2.7.2]. We will give the proof of the nonlogarithmic decomposition by applying several lemmas from the same paper.

We need to show that if $\mathscr{E}$ does not have uniform slope at least 1, then $\mathscr{E}$ is decomposable when η_0 is taken sufficiently close to 1. (See Remark 2.3.12 for the reason for having 1 instead of 0.) If ∂_0 is eventually dominant, the decomposition theorem of Christol and Mebkhout [Kedlaya 2007, Lemma 2.7.3] gives the decomposition. If ∂_0 is not eventually dominant, Lemma 2.3.15 implies that ∂_j is eventually dominant for some $j \in J$. By Lemma 2.3.17, ∂_0 is eventually dominant for $g^*\mathscr{E}$. Applying the decomposition theorem [Kedlaya 2007, Lemma 2.7.3] to $g^*\mathscr{E}$ and pulling back the decomposition along g^{-1}, we obtain a nontrivial decomposition of $\mathscr{E}$ on $\mathscr{R}_{K'}^{\eta_0}$ for some $\eta_0 \in (0,1)$. □

Proposition 2.3.22. *In Theorem 2.3.21, if the (ϕ, ∇)-module $\mathscr{E}_\rho$ is associated with a p-adic representation ρ of finite local monodromy, then the decomposition of (ϕ, ∇)-modules induces a direct sum decomposition of the representation ρ so that each direct summand of $\mathscr{E}_\rho$ is the differential module associated with a direct summand of ρ.*

Proof. By slope filtration [Kedlaya 2007, Theorem 3.4.6], the Frobenius action on each direct summand of $\mathscr{E}$ is of unit-root; the decomposition of the representation follows by [Kedlaya 2007, Proposition 3.4.4]. □

Definition 2.3.23. Let $\rho : G_k \to \mathrm{GL}(V_\rho)$ be a p-adic representation with finite local monodromy. Let $\mathscr{E}$ be the differential module corresponding to $V_\rho / V_\rho^{I_k}$ by Constructions 2.2.8 and 2.2.15, where $V_\rho^{I_k}$ is the unramified piece of V_ρ consisting of the elements in V_ρ which are fixed by I_k. By Theorem 2.3.21 above, there exists a multiset $\{a_1, \ldots, a_d\}$ such that for all η sufficiently close to 1, $\boldsymbol{S}(\mathscr{E}, \eta) = \{\eta^{a_1}, \ldots, \eta^{a_d}\}$. Define the *differential Artin conductor* of $\mathscr{E}$ (or ρ) by

$$\mathrm{Art}_{\mathrm{dif}}(\mathscr{E}) = \mathrm{Art}_{\mathrm{dif}}(\rho) = a_1 + \cdots + a_d.$$

The *differential Swan conductor* of $\mathscr{E}$ (or ρ), denoted by $\mathrm{Swan}_{\mathrm{dif}}(\mathscr{E})$ or $\mathrm{Swan}_{\mathrm{dif}}(\rho)$, is defined similarly, by adding the subscript log everywhere.

Remark 2.3.24. In this definition, we split off the unramified part, because it has both conductors 0. We need to do so because the convergence radius multiset cannot distinguish between the unramified and the tame parts, which give different contributions to the Artin conductor. This does not matter for Swan conductors, and we may define the Swan conductor without first taking out the unramified piece.

Remark 2.3.25. By [Kedlaya 2007, Proposition 2.6.6], the definition of differential Swan conductors does not depend on the choice of a uniformizer s and a p-basis $\{b_1, \ldots, b_m, s\}$. We are also free to remove Hypothesis 2.3.2 and define the differential Swan conductors for arbitrary complete discretely valued fields of equal characteristic p [Kedlaya 2007, Corollary 3.5.7]. A similar statement holds for differential Artin conductors; the proof is the same as for Swan conductors.

2.4. ***Basic properties.*** We do not impose any hypothesis on k.

Theorem 2.4.1. *Differential conductors satisfy the following properties*:

(0) *When the residue field κ_k is perfect*, *the differential Artin and Swan conductors are the same as the classical ones defined in* [Serre 1979].

(1) *For any representation ρ of finite local monodromy*, $\mathrm{Swan}_{\mathrm{dif}}(\rho) \in \mathbb{Z}_{\geq 0}$ *and* $\mathrm{Art}_{\mathrm{dif}}(\rho) \in \mathbb{Z}_{\geq 0}$.

(2) *Let k'/k be a tamely ramified extension of ramification degree e'. Let ρ be a representation of G_k of finite local monodromy and let ρ' denote the restriction of ρ to $G_{k'}$. Then* $\mathrm{Swan}_{\mathrm{dif}}(\rho') = e' \cdot \mathrm{Swan}_{\mathrm{dif}}(\rho)$. *If $e' = 1$*, *i.e.*, *k'/k is unramified*, *then* $\mathrm{Art}_{\mathrm{dif}}(\rho') = \mathrm{Art}_{\mathrm{dif}}(\rho)$.

(3) *Let ρ be a faithful p-adic representation of the Galois group of a Galois extension l/k. If l/k is tamely ramified and not unramified*, *then* $b_{\mathrm{dif}}(\rho) = 1$ *and* $b_{\mathrm{dif},\log}(\rho) = 0$. *If l/k is unramified*, $b_{\mathrm{dif}}(\rho) = b_{\mathrm{dif},\log}(\rho) = 0$.

(4) *Put $G_k^0 = G_k$ and $G_k^a = I_k$ for $a \in (0, 1]$. For $a > 1$*, *let R_a be the set of finite image representations ρ with differential ramification breaks less than a. Define $G_k^a = \bigcap_{\rho \in R_a} (I_k \cap \ker \rho)$ and write G_k^{a+} for the closure of $\bigcup_{b>a} G_k^b$. This defines a differential filtration on G_k such that for all finite image representations ρ*, *$\rho(G_k^a)$ is trivial if and only if $\rho \in R_a$.*

Similarly, put $G^0_{k,\log} = G_k$. *For* $a > 0$, *let* $R_{a,\log}$ *be the set of finite image representations* ρ *with logarithmic differential ramification breaks less than* a. *Define* $G^a_{k,\log} = \bigcap_{\rho\in R_{a,\log}}(I_k \cap \ker\rho)$ *and write* $G^{a+}_{k,\log}$ *for the closure of* $\bigcup_{b>a} G^b_{k,\log}$. *This defines a differential logarithmic filtration on* G_k *such that for all finite image representations* ρ, $\rho(G^a_{k,\log})$ *is trivial if and only if* $\rho \in R_{a,\log}$.

For $a > 0$, *the group* G^a_k/G^{a+}_k *is abelian and killed by* p (*and trivial if* $a \notin \mathbb{Q}$).

For $a > 1$, *the group* $G^a_{k,\log}/G^{a+}_{k,\log}$ *is abelian and killed by* p (*and trivial if* $a \notin \mathbb{Q}$).

Proof. For (0), see [Kedlaya 2005, Theorem 5.23]. For the rest of the statements, the proof for Swan conductors can be found in [Kedlaya 2007, §3.5]; we will only prove the corresponding properties for differential Artin conductors. As in the proof for differential Swan conductors, we may first reduce to the case where Hypothesis 2.3.2 holds.

(1) We can follow the proof of [Kedlaya 2007, Theorem 2.8.2], because of the decomposition Theorem 2.3.21. An alternative proof is to apply Lemma 2.3.17, and reduce to the case where ∂_0 is dominant (see also Remark 2.3.18); then one can forget about $\partial_1, \dots, \partial_m$ and hence reduce to the perfect residue field case, which is statement (0) of the theorem.

(2) Since an unramified extension l/k only changes the field K but not the uniformizer s, we can use the same s as the uniformizer of l. The corresponding differential module $\mathscr{E}_{\rho'}$ of ρ' is just a simple extension of scalars. Since the calculation of spectral norms does not depend on the base field (see Remark 2.3.5), we compute the same result on spectral norms and hence have the same Artin conductor.

(3) is an immediate consequence of the Swan case. Attention: differential ramification breaks cannot distinguish unramified extensions from tamely ramified ones. (See also Remark 2.3.24.)

(4) The proof for the nonlogarithmic differential filtration is much simpler than the logarithmic case because of the different normalization in Definition 2.3.9. By virtue of the proof of [Kedlaya 2007, Theorem 3.5.13], it suffices to show that we can rotate so that ∂_0 becomes dominant; this is the content of Lemma 2.3.17. $\square$

Remark 2.4.2. The invariance of the differential conductors under unramified base changes enables us to assume that κ_0 is algebraically closed. This justifies the assumption we made in Notation 2.2.2.

3. The thickening technique

In this section, we introduce a thickening technique. Loosely speaking, it consists in constructing what can be thought of as a tubular neighborhood of the diagonal embedding of $A^1_K[\eta_0, 1)$ into $A^1_K[\eta_0, 1) \times_{K_0} A^1_K[\eta_0, 1)$, but note that the latter rigid space is not really well-defined.

We start with a geometric interpretation of this construction and then move on to the abstract definition of the thickening space.

We keep Hypothesis 2.3.2 throughout this section.

Notation 3.0.1. For $\alpha \in (0, +\infty)$, denote by $A^m_K[0, \alpha]$ and $A^m_K[0, \alpha)$ the closed and open polydiscs with radius α and center at the origin. Let $K\langle u_1/\alpha, \dots, u_m/\alpha\rangle$ denote the ring of analytic functions on the disc $A^m_K[0, \alpha]$.

Later, we will see many homomorphisms between rings of functions on K-rigid spaces, which are only K_0-linear. It is unfair to say that they induce morphisms of rigid spaces; however, we prefer to keep some geometric flavor of the whole construction. On the other hand, these rigid spaces are all quasi-Stein or affinoid; knowing the ring of analytic functions is equivalent to knowing the rigid spaces.

Notation 3.0.2. For a continuous homomorphism $f^* : A \to B$ between affinoid or Fréchet algebras (not necessarily respecting the ground field K), we write formally $f : \mathrm{Max}(B) \to \mathrm{Max}(A)$, as the *geometric incarnation* of the homomorphism. Pullbacks along maps and Cartesian diagrams are thought of as (completed) tensor products. (In fact, in all cases we encounter, we do not need to take the completion for the tensor products.) In short, whenever such a map is given, strictly speaking, we should view it as a continuous ring homomorphism.

3.1. *Geometric thickening.* In this subsection, we describe the thickening technique when the residue field κ_k can be realized as the field of rational functions on a smooth κ_0-variety. The purpose of this subsection is solely to provide some geometric intuition for the thickening construction in the next subsection; the content in this subsection will not be used in the rest of this paper.

Hypothesis 3.1.1. *Only* in this subsection, we assume that the field κ_k is a finite separable extension of $\kappa_0(\bar{b}_1, \dots, \bar{b}_m)$.

Construction 3.1.2. Let $\bar{X}$ be a smooth variety over κ_0 whose field of rational functions is κ_k; such an $\bar{X}$ exists because we may realize it as an affine scheme étale over $\operatorname{Spec} \kappa_0[\bar{b}_1, \dots, \bar{b}_m]$ which induces the extension $\kappa_k/\kappa_0(\bar{b}_1, \dots, \bar{b}_m)$. We may further shrink $\bar{X}$ so that it is the special fiber of an affine smooth formal scheme $\mathfrak{X}$ over $\mathcal{O}_{K_0}$ of topological finite type, i.e., $\mathfrak{X} \times_{\operatorname{Spf} \mathcal{O}_{K_0}} \operatorname{Spec} \kappa_0 = \bar{X}$. We may further shrink $\mathfrak{X}$ and $\bar{X}$ so that we have lifts $B_1, \dots, B_m$ of $\bar{b}_1, \dots, \bar{b}_m$ on $\mathfrak{X}$ and $dB_1, \dots, dB_m$ form a basis of the sheaf of relative differentials $\Omega^1_{\mathfrak{X}/\mathcal{O}_{K_0}}$. We use $\boldsymbol{X}$ to denote the "generic fiber" of $\mathfrak{X}$ as a rigid space over $\mathrm{Sp}(K_0)$, in the sense of Raynaud; it is affinoid.

Consider the commutative diagram

$$\begin{tikzcd}
\overline{X} \arrow[r] \arrow[d, hook] & \mathfrak{X} \arrow[d, hook] & \boldsymbol{X} \arrow[l] \arrow[d, hook] \\
P = \overline{X} \times_{\kappa_0} \mathbb{A}^1_{\kappa_0} \arrow[r] \arrow[d] & \mathcal{P} = \mathfrak{X} \times_{\operatorname{Spf} \mathcal{O}_{K_0}} \widehat{\mathbb{A}}^1_{\mathcal{O}_{K_0}} \arrow[d] & \boldsymbol{P} = \boldsymbol{X} \times_{K_0} A^1_{K_0}[0, 1] \arrow[l] \arrow[d] \\
\operatorname{Spec} \kappa_0 \arrow[r] & \operatorname{Spf} \mathcal{O}_{K_0} & \operatorname{Sp}(K_0). \arrow[l]
\end{tikzcd}$$

where the vertical arrows from the first row to the second are all embeddings of zero sections and the coordinates of $\mathbb{A}^1_{\kappa_0}$ and $\widehat{\mathbb{A}}^1_{\mathcal{O}_{k_0}}$ are denoted by s and S, respectively.

The tube of $\overline{X}$ in $\boldsymbol{P}$, denoted by $]\overline{X}[_{\mathcal{P}}$, is isomorphic to $\boldsymbol{X} \times A^1_{K_0}[0, 1)$. Let $\mathcal{O}_{\boldsymbol{X}}$ be the ring of rigid analytic functions on $\boldsymbol{X}$; then K is exactly the p-adic completion of $\operatorname{Frac} \mathcal{O}_{\boldsymbol{X}}$. If we base-change the tube $]\overline{X}[_{\mathcal{P}}$ from $\boldsymbol{X}$ over to K, we get $A^1_K[0, 1)$. We are interested in the annulus $A^1_K[\eta_0, 1)$ for some $\eta_0 \in (0, 1)$, which can be obtained by base-changing $\boldsymbol{X} \times A^1_{K_0}[\eta_0, 1)$ from $\boldsymbol{X}$ to K.

Now, we consider the thickening space of this annulus $A^1_K[\eta_0, 1)$.

Construction 3.1.3. Consider the commutative diagram

$$\begin{tikzcd}
\overline{X} \arrow[r, hook] \arrow[dr] & P \arrow[r, hook, "\Delta_P"] \arrow[d] & P \times_{\kappa_0} P \arrow[r, hook] \arrow[dl] & \mathcal{P} \times_{\mathcal{O}_{K_0}} \mathcal{P} \arrow[d] & \boldsymbol{P} \times_{K_0} \boldsymbol{P} \arrow[l] \arrow[d] \\
 & \operatorname{Spec} \kappa_0 \arrow[rr] & & \operatorname{Spf} \mathcal{O}_{K_0} & \operatorname{Sp}(K_0) \arrow[l]
\end{tikzcd}$$

where we use $\operatorname{pr}_i : \mathcal{P} \times_{\mathcal{O}_{K_0}} \mathcal{P} \to \mathcal{P}$ to denote the projection to the i-th factor for $i = 1, 2$. Then $\mathcal{P} \times_{\mathcal{O}_{K_0}} \mathcal{P}$ has a set of local parameters given by $B_1 = \operatorname{pr}_1^*(B_1), \dots, B_m = \operatorname{pr}_1^*(B_m)$, $S = \operatorname{pr}_1^*(S)$, $B'_1 = \operatorname{pr}_2^*(B_1), \dots, B'_m = \operatorname{pr}_2^*(B_m)$, and $S' = \operatorname{pr}_2^*(S)$. By Berthelot's fibration theorem [1996, théorème 1.3.2], we have an isomorphism

$$]\overline{X}[_{\mathcal{P} \times_{\mathcal{O}_{K_0}} \mathcal{P}} \simeq]\overline{X}[_{\mathcal{P}} \times_{K_0} A^{m+1}_{K_0}[0, 1),$$

where the factor $]\overline{X}[_{\mathcal{P}}$ respects the projection pr_1 and the coordinates for the open polydisc on the right-hand side are given by $\delta_0 = S - S'$, $\delta_1 = B_1 - B'_1, \dots, \delta_m = B_m - B'_m$. The geometric thickening space is the subspace of $]\overline{X}[_{\mathcal{P} \times_{\mathcal{O}_{K_0}} \mathcal{P}}$ where $|\delta_0| = |S - S'| < |S|$, or, more precisely,

$$\boldsymbol{X} \times_{K_0} \{(S, \delta_0) \in A^2_{K_0}[0, 1) \mid |\delta_0| < |S|\} \times_{K_0} A^m_{K_0}[0, 1).$$

Thus, the *thickening space*, denoted by $TS_k^{\geq \eta_0}$, of $A^1_K[\eta_0, 1)$ is the space obtained by base-changing

$$\boldsymbol{X} \times_{K_0} \{(S, \delta_0) \in A^2_{K_0}[0, 1) \mid |S| \geq \eta_0, |\delta_0| < |S|\} \times_{K_0} A^m_{K_0}[0, 1).$$

from $\boldsymbol{X}$ to K.

The projection $\mathrm{pr}_1 : \boldsymbol{P} \times_{K_0} \boldsymbol{P} \to \boldsymbol{P}$ gives a K-morphism of rigid spaces

$$\pi : TS_k^{\geq \eta_0} \to A_K^1[\eta_0, 1);$$

the projection $\mathrm{pr}_2 : \boldsymbol{P} \times_{K_0} \boldsymbol{P} \to \boldsymbol{P}$ gives a K_0-morphism of rigid spaces

$$\tilde{\pi} : TS_k^{\geq \eta_0} \to A_K^1[\eta_0, 1).$$

The morphism $\tilde{\pi}$ does not respect the K-rigid space structure; one should always think of $\tilde{\pi}$ as the ring homomorphism between the corresponding ring of analytic functions. In our earlier notation, this is just the geometric incarnation of the map on the ring of global sections.

3.2. ***General thickening construction.*** We now introduce thickening spaces and study basic properties of differential modules over them.

We keep Hypothesis 2.3.2 in this subsection. However, Hypothesis 3.1.1 is no longer in force from now on.

Definition 3.2.1. For $\eta \in (0, 1)$, we write $Z_k^\eta = A_K^1[\eta, \eta]$. For $a \in \mathbb{Q}_{>1}$ and $\eta_0 \in (0, 1)$, we define the *thickening space of* $A_K^1[\eta_0, 1)$ *and level* a to be the rigid space over K of the form

$$TS_k^{a, \geq \eta_0} = \left\{ (S, \delta_{J^+}) \in A_K^{m+2}[0, 1) \,\middle|\, |S| \geq \eta_0;\ |\delta_j| \leq |S|^a \text{ for } j \in J^+ \right\}. \tag{3.2.2}$$

For $\eta \in [\eta_0, 1)$, we put

$$TS_k^{a, \eta} = A_K^1[\eta, \eta] \times_K A_K^{m+1}[0, \eta^a].$$

Similarly, for $a \in \mathbb{Q}_{>0}$ and $\eta_0 \in (0, 1)$, we define the *log-thickening space of* $A_K^1[\eta_0, 1)$ *and level* a to be

$$TS_{k,\log}^{a, \geq \eta_0} = \left\{ (S, \delta_{J^+}) \in A_K^{m+2}[0, 1) \,\middle|\, |S| \geq \eta_0;\ |\delta_0| \leq |S|^{a+1};\ |\delta_j| \leq |S|^a \text{ for } j \in J \right\}. \tag{3.2.3}$$

For $\eta \in [\eta_0, 1)$, we set

$$TS_{k,\log}^{a, \eta} = A_K^1[\eta, \eta] \times_K A_K^1[0, \eta^{a+1}] \times_K A_K^m[0, \eta^a].$$

We denote by $\mathcal{O}_{TS_k^{a, \geq \eta_0}}$, $\mathcal{O}_{TS_k^{a, \eta}}$, $\mathcal{O}_{TS_{k,\log}^{a, \geq \eta_0}}$, and $\mathcal{O}_{TS_{k,\log}^{a, \eta}}$ the rings of analytic functions on these spaces.

Let $|\cdot|_{Z_k^\eta}$ denote the η-Gauss norm on Z_k^η. For $a \in \mathbb{Q}_{>1}$, let $|\cdot|_{TS_k^{a,\eta}}$ denote the Gauss norm on $TS_k^{a,\eta}$; for $a > 0$, let $|\cdot|_{TS_{k,\log}^{a,\eta}}$ denote the Gauss norm on $TS_{k,\log}^{a,\eta}$.

The union of all $TS_k^{a, \geq \eta_0}$ is the $TS_k^{\geq \eta_0}$ we discussed in Construction 3.1.3.

Caution 3.2.4. One may want to write $TS_k^{a, \geq \eta_0} = \bigcup_{\eta \in [\eta_0, 1)} A_K^1[\eta, 1) \times_K A_K^{m+1}[0, \eta^a]$ for simplicity, as in the introduction. However, this will not define the same rigid space as in (3.2.2), because the union does *not* give an admissible cover of $TS_k^{a, \geq \eta_0}$.

A similar expression for log-thickening space is not valid either. Nevertheless, it might be helpful to think the space and picture the geometry this way.

On the other hand, it is true that an element of $K[\![S, \delta_0, \dots, \delta_m]\!]$ lies in $\mathcal{O}_{TS_k^{a,\geq\eta_0}}$ (resp. $\mathcal{O}_{TS_{k,\log}^{a,\geq\eta_0}}$) if and only if it has bounded norms for all $|\cdot|_{TS_k^{a,\eta}}$ (resp. $|\cdot|_{TS_{k,\log}^{a,\eta}}$) for all $\eta \in [\eta_0, 1)$.

Remark 3.2.5. We need $a \in \mathbb{Q}$ in Definition 3.2.1 to make sure that (3.2.2) and (3.2.3) actually define a (Berkovich) rigid analytic space. For individual spaces $TS_k^{a,\eta}$ and $TS_{k,\log}^{a,\eta}$, one can allow $a \in \mathbb{R}$.

Notation 3.2.6. For $a \in \mathbb{Q}_{>1}$ and $\eta_0 \in (0, 1)$, denote by $\Delta : Z_k^{\geq\eta_0} \hookrightarrow TS_k^{a,\geq\eta_0}$ the natural embedding of $Z_k^{\geq\eta_0}$ into the locus where $\delta_j = 0$ for $j \in J^+$. Also, we have the naïve projection $\pi : TS_k^{a,\geq\eta_0} \to Z_k^{\geq\eta_0}$ to the first factor.

For $a \in \mathbb{Q}_{>0}$, we define likewise $\Delta : Z_k^{\geq\eta_0} \hookrightarrow TS_{k,\log}^{a,\geq\eta_0}$ and $\pi : TS_{k,\log}^{a,\geq\eta_0} \to Z_k^{\geq\eta_0}$.

All these morphisms remain compatible under changes in a and η_0, and under the replacement of $\geq \eta_0$ by η for some $\eta \in [\eta_0, 1)$.

To simplify notation, for a and η_0 as above, we identify $\mathcal{O}_{Z_k^{\geq\eta_0}}$ with a subring of $\mathcal{O}_{TS_k^{a,\geq\eta_0}}$ and of $\mathcal{O}_{TS_{k,\log}^{a,\geq\eta_0}}$ via π^*, and likewise for η instead of $\geq \eta_0$. Note that π^* is an isometry; hence the identification will not change any calculation on norms.

Corollary 2.1.10 has this immediate consequence:

Proposition 3.2.7. *There is a unique continuous $\mathcal{O}_{K_0}$-homomorphism*

$$\tilde{\pi}^* : \mathcal{O}_K[\![S]\!] \to \mathcal{O}_K[\![S, \delta_{J^+}]\!]$$

such that $\tilde{\pi}^*(S) = S + \delta_0$ and $\tilde{\pi}^*(B_j) = B_j + \delta_j$ for all $j \in J$. Moreover, for $g \in \mathcal{O}_K$, $\tilde{\pi}^*(g) - g \in (\delta_1, \dots, \delta_m)(g)\mathcal{O}_K[\![\delta_1, \dots, \delta_m]\!]$.

Theorem 3.2.8. *For $a \in \mathbb{Q}_{>1}$ (resp. $a \in \mathbb{Q}_{>0}$) and $\eta_0 \in (0, 1)$, the homomorphism $\tilde{\pi}^*$ induces a K_0-homomorphism $\tilde{\pi}^* : \mathcal{O}_{Z_k^{\geq\eta_0}} = \mathcal{R}_K^{\eta_0} \to \mathcal{O}_{TS_k^{a,\geq\eta_0}}$ (resp. $\tilde{\pi}^* : \mathcal{O}_{Z_k^{\geq\eta_0}} \to \mathcal{O}_{TS_{k,\log}^{a,\geq\eta_0}}$) such that $\Delta^* \circ \tilde{\pi}^* = \mathrm{id}$; the same if replacing $\geq \eta_0$ by η for some $\eta \in [\eta_0, 1)$.*

For any $g \in \mathcal{O}_{Z_k^\eta}$ and for $a > 1$ (resp. $a > 0$),

$$|\tilde{\pi}^*(g) - g|_{TS_k^{a,\eta}} \leq \eta^{a-1} \cdot |g|_{Z_k^\eta} \quad (\textit{resp. } |\tilde{\pi}^*(g) - g|_{TS_{k,\log}^{a,\eta}} \leq \eta^a \cdot |g|_{Z_k^\eta}). \tag{3.2.9}$$

In particular, $|\tilde{\pi}^*(g)|_{TS_k^{a,\eta}} = |\tilde{\pi}^*(g)|_{TS_{k,\log}^{a,\eta}} = |g|_{Z_k^\eta}$. Moreover, we have the following bound for $TS_k^{a,\eta}$: if $g \in \mathcal{O}_{Z_k^\eta} \cap \mathcal{O}_K[\![S]\!]$, then

$$|\tilde{\pi}^*(g) - g|_{TS_k^{a,\eta}} \leq \eta^a. \tag{3.2.10}$$

Proof. We need only to establish the bound on the norms. Take

$$g = \sum_{i \in \mathbb{Z}} a_i S^i \in K[\![S]\!]$$

such that $|g|_{Z_k^\eta} < +\infty$. We have

$$\begin{aligned}\tilde{\pi}^*(g) - g &= \sum_{i\in\mathbb{Z}} \big(\tilde{\pi}^*(a_i)(S+\delta_0)^i - a_i S^i\big) \\ &= \sum_{i\in\mathbb{Z}} \big((\tilde{\pi}^*(a_i) - a_i)(S+\delta_0)^i + a_i((S+\delta_0)^i - S^i)\big). \qquad (3.2.11)\end{aligned}$$

Since $\tilde{\pi}^*(a_i) - a_i \in (\delta_1, \dots, \delta_m)(a_i)\mathbb{O}_K[\![\delta_1, \dots, \delta_m]\!]$, we have

$$|\tilde{\pi}(a_i) - a_i|_{TS_k^{a,\eta}} \le |a_i|\eta^a, \quad |\tilde{\pi}(a_i) - a_i|_{TS_{k,\log}^{a,\eta}} \le |a_i|\eta^a. \qquad (3.2.12)$$

We can bound $(S+\delta_0)^i - S^i$ by

$$|(S+\delta_0)^i - S^i|_{TS_k^{a,\eta}} \le \eta^{a+i-1}, \quad |(S+\delta_0)^i - S^i|_{TS_{k,\log}^{a,\eta}} \le \eta^{a+i}. \qquad (3.2.13)$$

Plugging the estimates (3.2.12) and (3.2.13) into (3.2.11), we obtain (3.2.9). When $g \in \mathbb{O}_K[\![S]\!]$, (3.2.13) always gives $|(S+\delta_0)^i - S^i|_{TS_k^{a,\eta}} \le \eta^a$ for $i \ge 0$ (when $i = 0$, we have zero). Equation (3.2.10) follows.

Finally, the equalities $|\tilde{\pi}^*(g)|_{TS_k^{a,\eta}} = |\tilde{\pi}^*(g)|_{TS_{k,\log}^{a,\eta}} = |g|_{Z_k^\eta}$ ensure that we have well-defined continuous homomorphisms $\tilde{\pi}^* : \mathbb{O}_{Z_k^{\ge\eta_0}} \to \mathbb{O}_{TS_k^{a,\ge\eta_0}}$ or $\mathbb{O}_{TS_{k,\log}^{a,\ge\eta_0}}$. □

Notation 3.2.14. We use $\tilde{\pi} : TS_k^{a,\ge\eta_0} \to Z_k^{\ge\eta_0}$ and $\tilde{\pi} : TS_{k,\log}^{a,\ge\eta_0} \to Z_k^{\ge\eta_0}$ to denote the geometric incarnations of the homomorphisms $\tilde{\pi}^*$ constructed in Theorem 3.2.8; the same for η in place of $\ge \eta_0$ when $\eta \in [\eta_0, 1)$. To emphasize again, whenever we refer to $\tilde{\pi}$, strictly speaking, we are referring to the corresponding homomorphism $\tilde{\pi}^*$ on rings.

Remark 3.2.15. For $a > 0$, one can factor the map $\tilde{\pi}$ for a nonlog thickening space as $TS_k^{a+1,\ge\eta_0} \to TS_{k,\log}^{a,\ge\eta_0} \xrightarrow{\tilde{\pi}} Z_k^{\ge\eta_0}$, where the second map is the $\tilde{\pi}$ for the log-thickening space. Again, this should be thought of as factorization for ring homomorphisms.

Notation 3.2.16. For a ∇-module $(\mathscr{E}, \nabla_{\mathscr{E}})$ over $Z_k^{\ge\eta_0}$ relative to K_0, we call $\tilde{\pi}^*\mathscr{E}$ the *thickened differential module* of $\mathscr{E}$, denoted by $\mathscr{F}$. We view $\mathscr{F}$ as a differential module over $TS_k^{a,\ge\eta_0}$ or $TS_{k,\log}^{a,\ge\eta_0}$ relative to $Z_k^{\ge\eta_0}$, with respect to the differential operators $\partial/\partial\delta_0, \dots, \partial/\partial\delta_m$. In precise terms, the connection is given by

$$\begin{aligned}\mathscr{F} = \mathscr{E} \otimes_{\mathscr{R}_K^{\eta_0}, \tilde{\pi}^*} \mathbb{O}_{TS_k^{a,\ge\eta_0}} &\xrightarrow{\nabla_{\mathscr{E}}} \mathscr{E} \otimes \Omega^1_{Z_k^{\ge\eta_0}/K_0} \otimes_{\mathscr{R}_K^{\eta_0}, \tilde{\pi}^*} \mathbb{O}_{TS_k^{a,\ge\eta_0}} \\ &\longrightarrow \mathscr{E} \otimes_{\mathscr{R}_K^{\eta_0}, \tilde{\pi}^*} \Omega^1_{TS_k^{a,\ge\eta_0}/K_0} \\ &\longrightarrow \mathscr{E} \otimes_{\mathscr{R}_K^{\eta_0}, \tilde{\pi}^*} \Omega^1_{TS_k^{a,\ge\eta_0}/Z_k^{\ge\eta_0}}\end{aligned}$$

in the nonlog case. The log case is obtained similarly, with subscript log at the appropriate places. This construction is compatible for different a's and η_0's.

We next link the spectral norms on $\mathscr{E}$ and the spectral norms on its thickening $\mathscr{F}$.

Proposition 3.2.17. *Let $\eta \in [\eta_0, 1)$. The spectral norms of ∂_{J^+} on $\mathscr{E}_\eta$ over Z_k^η and the spectral norms of $\partial/\partial\delta_{J^+}$ on $\mathscr{F}_{a,\eta} = \mathscr{F} \otimes \mathrm{Frac}(\mathbb{O}_{TS_k^{a,\eta}})^\wedge$ and $\mathscr{F}_{a,\eta,\log} = \mathscr{F} \otimes \mathrm{Frac}(\mathbb{O}_{TS_{k,\log}^{a,\eta}})^\wedge$ are related as follows*:

$$|\partial/\partial\delta_j|_{\mathscr{F}_{a,\eta},\mathrm{sp}} = \max\{|\partial_j|_{\mathscr{E}_\eta,\mathrm{sp}}, p^{-1/(p-1)}\eta^{-a}\} \qquad \textit{for } j \in J^+,$$
$$|\partial/\partial\delta_0|_{\mathscr{F}_{a,\eta,\log},\mathrm{sp}} = \max\{|\partial_0|_{\mathscr{E}_\eta,\mathrm{sp}}, p^{-1/(p-1)}\eta^{-a-1}\},$$
$$|\partial/\partial\delta_j|_{\mathscr{F}_{a,\eta,\log},\mathrm{sp}} = \max\{|\partial_j|_{\mathscr{E}_\eta,\mathrm{sp}}, p^{-1/(p-1)}\eta^{-a}\} \qquad \textit{for } j \in J.$$

Proof. Note that $\tilde\pi^*(dB_j) = dB_j + d\delta_j$ for $j \in J$ and $\tilde\pi^*(dS) = dS + d\delta_0$. The actions of $\partial/\partial\delta_j$, $j \in J$ (resp. $j = 0$), on $\mathscr{F}_{a,\eta}$ and $\mathscr{F}_{a,\eta,\log}$ are the same as the action of $\partial/\partial B_j$ (resp. $\partial/\partial S$) on $\mathscr{E}_\eta$. More precisely, we have $\tilde\pi^*(\partial/\partial S(x)) = \partial/\partial\delta_0(\tilde\pi^*(x))$ and $\tilde\pi^*(\partial/\partial B_j(x)) = \partial/\partial\delta_j(\tilde\pi^*(x))$ for any $j \in J$ and $x \in \mathscr{R}_K^\eta$ *or* $\mathscr{E}_\eta$.

The statement follows, because that δ_J are transcendental over $\mathbb{O}_{Z_k^\eta}$ and the homomorphism $\tilde\pi^*$ is isometric (by Theorem 3.2.8). ☐

3.3. *Good generators of the extension.* We now show that when l/k is totally and wildly ramified, we can choose nice generators of $\mathbb{O}_l$ as an $\mathbb{O}_k$-algebra, so that the corresponding extension on the Robba rings takes a simple form. Then we give a more explicit construction of the differential module associated with a p-adic representation.

We keep Hypothesis 2.3.2 for this subsection.

Hypothesis 3.3.1. For the rest of this section, we assume that l/k is a finite totally and wildly ramified Galois extension.

Remark 3.3.2. This is a mild hypothesis, since both arithmetic and differential conductors behave well under unramified extensions and the tamely ramified case is well-known: see Theorem 2.4.1(3) and Proposition 4.1.7(6).

Notation 3.3.3. Let l be as above, and let $G_{l/k}$ denote the Galois group of l/k. Denote the ring of integers and the residue field of l by $\mathbb{O}_l$ and κ_l, respectively. Given a uniformizer t of l, we fix a noncanonical isomorphism $\kappa_l((t)) \simeq l$. For a p-basis $\bar c_J$ of κ_l, we use c_J to denote the image of $\bar c_J$ under this isomorphism; we may use the same index set J because κ_l/κ_k is a finite extension.

Let $\mathbb{O}_L$ be the Cohen ring of κ_l with respect to $\bar c_J$ and let C_J be the canonical lifts of $\bar c_J$. Set $L = \mathrm{Frac}\,\mathbb{O}_L$.

Caution 3.3.4. The residue field extension κ_l/κ_k is typically not separable and hence *cannot* be embedded into the extension $l = \kappa_l((t))$ over $k = \kappa_k((s))$.

The reader may skip the next construction and remark on first reading. Their gist is to provide "good" generators and relations of $\mathbb{O}_l$ as an $\mathbb{O}_k$-algebra.

Construction 3.3.5. We temporarily drop the finiteness Hypothesis 2.3.2 on the p-basis for this construction. Let $\boldsymbol{k}_0 = \kappa_k$ with p-basis $(\bar{b}_j)_{j\in J}$. By possibly rearranging the indexing in $\bar{b}_J$, we will inductively construct a "good" p-basis $(\bar{c}_j)_{j\in J}$ of κ_l and $\boldsymbol{k}_j = \kappa_k(\bar{c}_1, \dots, \bar{c}_j)$ with p-basis $\{\bar{c}_1, \dots, \bar{c}_j, \bar{b}_{J\backslash\{1,\dots,j\}}\}$ so that $\boldsymbol{k}_m = \kappa_l$ for m sufficiently large.

Assume that we have constructed $\boldsymbol{k}_{j-1}$. Let r_j be the unique integer such that $\kappa_l \subseteq \boldsymbol{k}_{j-1}^{p^{-r_j}}$ but $\kappa_l \nsubseteq \boldsymbol{k}_{j-1}^{p^{-r_j+1}}$. If $r_j = 0$, we must have $\boldsymbol{k}_{j-1} = \kappa_l$; in this case, we set $\bar{c}_\alpha = \bar{b}_\alpha$ and $r_\alpha = 0$ for all $\alpha \in J\backslash\{1, \dots, j-1\}$ and stop the induction. Otherwise we assume that $r_j > 0$. Take $\bar{c}_j$ to be any element in $\kappa_l\backslash \boldsymbol{k}_{j-1}^{p^{-r_j+1}}$ and let $\boldsymbol{k}_j = \boldsymbol{k}_{j-1}(\bar{c}_j)$. Then $\bar{c}_j^{p^{r_j}} \in \boldsymbol{k}_{j-1}$ and $[\boldsymbol{k}_j : \boldsymbol{k}_{j-1}] = p^{r_j}$. There must exist one element in $\bar{b}_{J\backslash\{1,\dots,j-1\}}$ such that the rest together with $\bar{c}_1, \dots, \bar{c}_j$ form a p-basis of $\boldsymbol{k}_j$. We assume that this element is $\bar{b}_j$ by reindexing $\bar{b}_{J\backslash\{1,\dots,j-1\}}$. This finishes the induction.

From the induction, one can see that the r_j form a decreasing sequence of nonnegative integers; but we do not need this fact.

Since κ_l/κ_k is finite, the construction ensures that $\bar{c}_j \in \kappa_k^\times$ for $j \in J\backslash J_0$ with $J_0 = \{1, \dots, m\}$ a finite subset. By the functoriality of p-bases (Corollary 2.1.11), we may change the isomorphism $\kappa_l((t)) \simeq l$ so that $\bar{c}_{J\backslash J_0}$ are sent to elements in $\mathbb{O}_k^\times$. Let c_J denote the images of $\bar{c}_J$ under the above isomorphism.

As a consequence, $c_1, \dots, c_m$ and t generate $\mathbb{O}_l$ over $\mathbb{O}_k$. More precisely,

$$\left\{c_J^{e_J} t^i \;\middle|\; i \in \{0, \dots, e-1\};\ e_j \in \{0, \dots, p^{r_j}-1\} \text{ for } j = 1, \dots, m\right\}$$

is a basis of $\mathbb{O}_l$ as a finite free $\mathbb{O}_k$-module. It is also a basis of l as a k-vector space.

Remark 3.3.6. It is attractive to hope that we can find a p-basis $(\bar{b}_j)_{j\in J}$ of κ_k such that $\kappa_l = \kappa_k(\bar{b}_j^{p^{-r_j}})$ for some $r_j \in \mathbb{Z}_{\geq 0}$. But this is false in general, as pointed out to us by Shun Ohkubo; a counterexample is provided by [Sweedler 1968, Example 1.1]. Sweedler called the case where such a basis can be found *modular*.

Let κ_0 be a perfect field of characteristic p and let X, Y, Z be indeterminates. Set $\kappa_k = \kappa_0(X^p, Y^p, Z^{p^2})$ and $\kappa_l = \kappa_k(Z, XY+Z)$. Then $[\kappa_l : \kappa_l \cap \kappa_k^{p^{-1}}] = p^2$ and $[\kappa_l \cap \kappa_k^{p^{-1}} : \kappa_k] = p$. Hence, κ_l/κ_k cannot be modular.

Now we go back to assuming Hypothesis 2.3.2.

Notation 3.3.7. For a nonarchimedean ring R, we use $R\langle u_0, \dots, u_m\rangle$ to denote the completion of $R[u_0, \dots, u_m]$ with respect to the natural topology induced from R. When $R = F$ is a complete nonarchimedean field, $F\langle u_0, \dots, u_m\rangle$ is the ring of analytic functions on the unit polydisc $A_F^{m+1}[0, 1]$.

Notation 3.3.8. Let $\mathbb{O}_k\langle u_0, \dots, u_m\rangle/\mathcal{J} \xrightarrow{\sim} \mathbb{O}_l$ be the homomorphism that sends u_0 to t and u_j to c_j, for each $j \in J$. We choose a set of generators $p_0, \dots, p_m$ of $\mathcal{J}$ as follows: each $c_j^{p^{r_j}}$ or t^e can be written in terms of the basis of $\mathbb{O}_l$ over $\mathbb{O}_k$ listed in

Construction 3.3.5. This gives us an element p_j in $\mathcal{I}$ (the index $j=0$ being used for t^e). Obviously, the p_i generate $\mathcal{I}$. Moreover,

$$p_0 \in u_0^e - \mathfrak{d}s + (u_0 s, s^2)\cdot \mathbb{O}_k[u_0,\dots,u_m],$$
$$p_j \in u_j^{p^{r_j}} - \mathfrak{b}_j + (u_0, s)\cdot \mathbb{O}_k[u_0,\dots,u_m] \quad \text{for } j=1,\dots,m,$$

where $\mathfrak{b}_j$ is a polynomial in $u_1,\dots,u_{j-1}$ with coefficients in $\mathbb{O}_k$ and with degree on $u_{j'}$ strictly smaller than $p^{r_{j'}}$ for $j'=1,\dots,j-1$, and $\mathfrak{d}\in\mathbb{O}_k[u_J]$ such that $\mathfrak{d}(c_1,\dots,c_m)\in\mathbb{O}_L^\times$. Let $\bar{\mathfrak{b}}_j$ be the reduction of $\mathfrak{b}_j$ in $\kappa_k[u_1,\dots,u_{j-1}]$.

Remark 3.3.9. The need for introducing $\mathfrak{d}$ was pointed out to us by Shun Ohkubo: in general, one may not be able to find uniformizers s and t of k and l, respectively, such that $t^e\equiv s \bmod t^{e+1}\mathbb{O}_l$. This is shown by the next example, provided by Ohkubo. (We do not know if there is a counterexample for which L/K is Galois.)

Example 3.3.10. Let k be a complete discretely valued field with nonperfect residue field κ_k. Let $b\in\mathbb{O}_k$ be such that $\bar b\in\kappa_k\backslash\kappa_k^p$. Choose $\alpha,\beta\in\overline{K}$ as follows: let α be a root of polynomial $X^p+sX+b\in k[X]$ and β a root of polynomial $Y^p+sY+s\alpha\in k(\alpha)[Y]$. Let $l=k(\alpha,\beta)$. Then l/k is a separable extension of degree p^2 with naïve ramification degree p. The rings of integers of $k(\alpha)$ and $k(\alpha,\beta)$ are $\mathbb{O}_k[\alpha]$ and $\mathbb{O}_k[\alpha,\beta]$, respectively. We claim that we cannot choose uniformizers t and s so that $t^p/s\equiv 1 \bmod \mathfrak{m}_l$.

It is clear that β is a uniformizer of l. For any uniformizer t of l,

$$\frac{t^p}{s}=\frac{\beta^p}{s}\Big(\frac{t}{\beta}\Big)^p\in(-\alpha-\beta)(\mathbb{O}_l^\times)^p \xrightarrow{(\mathrm{mod}\ \mathfrak{m}_l)} (-\alpha)\kappa_l^p\subset\kappa_l.$$

In particular, t^p/s is not congruent to 1 modulo $\mathfrak{m}_l$.

Remark 3.3.11. Generally, the kernel of $\mathbb{O}_k[u_0,\dots,u_m]\to\mathbb{O}_l$ is not generated by $p_0,\dots,p_m$. This will not matter since we take $a>0$ and $a>1$ in Definition 3.2.1.

Construction 3.3.12. For each $j\in J$, fix an element in $\mathbb{O}_L[\![T]\!]$ lifting $b_j\in\mathbb{O}_k\subset\kappa_l[\![t]\!]$; also fix an element in $T^e+T^{e+1}\mathbb{O}_L[\![T]\!]$ lifting $s\in\mathbb{O}_k\subset\kappa_l[\![t]\!]$. By Proposition 2.1.8, there exists a continuous homomorphism $f^*:C_k\hookrightarrow C_l$ sending B_J and S to the elements chosen above; it naturally restricts to $f^*:\mathbb{O}_K[\![S]\!]\hookrightarrow\mathbb{O}_L[\![T]\!]$.

The proof of the following lemma is not enlightening. The reader may skip it on a first reading. The upshot is that we can turn the good generators and relations of $\mathbb{O}_l$ as an $\mathbb{O}_k$-algebra into good generators and relations of $\mathcal{R}_L^{\eta_0^{1/e}}$ as an $\mathcal{R}_K^{\eta_0}$-algebra.

Lemma 3.3.13. *Keep the notation as above.*

(1) *The homomorphism f^* is finite, and $C_1,\dots,C_m$ and T generate $\mathbb{O}_L[\![T]\!]$ over $\mathbb{O}_K[\![S]\!]$. Hence, f^* induces a surjective map $\mathbb{O}_K[\![S]\!]\langle U_0,\dots,U_m\rangle\twoheadrightarrow\mathbb{O}_L[\![T]\!]$ sending U_0 to T and U_j to C_j for $j\in J$. Moreover, one can choose generators*

$P_0, \dots, P_m$ of the kernel so that, modulo p, they are exactly p_{J^+} in Notation 3.3.8. In particular,

$$P_0 \in U_0^e - \mathfrak{D}S + (p, U_0S, S^2) \cdot \mathcal{O}_K[\![S]\!]\langle U_0, \dots, U_m\rangle,$$
$$P_j \in U_j^{p^{r_j}} - \mathfrak{B}_j + (p, U_0, S) \cdot \mathcal{O}_K[\![S]\!]\langle U_0, \dots, U_m\rangle,$$

where $\mathfrak{B}_j$ is a polynomial in $U_1, \dots, U_{j-1}$ with coefficients in $\mathcal{O}_K$ and with degree on $U_{j'}$ strictly smaller than $p^{r_{j'}}$ for $j' = 1, \dots, j-1$, and $\mathfrak{D} \in \mathcal{O}_K[U_J]$ lifts $\mathfrak{d}$. Moreover, $\{U_{J^+}^{e_{J^+}} \mid 0 \le e_0 < e; 0 \le e_j < p^{r_j}, j \in J\}$ form a basis of $\mathcal{O}_K[\![S]\!]\langle U_0, \dots, U_m\rangle/(P_{J^+})$ over $\mathcal{O}_K[\![S]\!]$.

(2) *The map f^* extends to a map $f_\eta^* : K\langle \eta/S, S/\eta\rangle \to L\langle \eta^{1/e}/T, T/\eta^{1/e}\rangle$ for $\eta \in [0, 1)$. Thus f^* extends by continuity to a homomorphism $f^* : \mathcal{R}_K^{\eta_0} \to \mathcal{R}_L^{\eta_0^{1/e}}$, or in geometric notation, $f : A_K^1[\eta_0, 1) \to A_L^1[\eta_0^{1/e}, 1)$ for $\eta_0 \in (0, 1)$.*

(3) *Let $\Gamma_K^\dagger$ and $\Gamma_L^\dagger$ be the integral Robba rings over K and L, respectively, similarly constructed as in Construction 2.2.8 but without tensoring with F. Let $\mathcal{R}_L$ be the Robba ring over L as in Notation 2.2.13. Then $\Gamma_L^\dagger$ is a finite étale extension of $\Gamma_K^\dagger$ with Galois group $G_{l/k}$. Moreover, $\mathcal{R}_L \simeq \Gamma_L^\dagger \otimes_{\Gamma_K^\dagger} \mathcal{R}_K$.*

(4) *For some $\eta_0 \in (0, 1)$, $A_L^1[\eta_0^{1/e}, 1)$ is Galois étale over $\eta \in [\eta_0, 1)$ via f^* with Galois group $G_{l/k}$. Hence, $\mathcal{R}_L^{\eta_0^{1/e}}$ becomes a regular $G_{l/k}$-representation over $\mathcal{R}_K^{\eta_0}$ via f^*.*

Proof. (1) is equivalent to its mod p version, which is exactly Construction 3.3.5.

(2) It suffices to prove that f^* is continuous with respect to the norms $|\cdot|_{Z_k^\eta}$ on C_k and $|\cdot|_{Z_l^{\eta^{1/e}}}$ on C_l, for all $\eta \in [\eta_0, 1)$. Since $f^*(\mathcal{O}_K) \in \mathcal{O}_L[\![T]\!]$ and $f^*(S) \in T^e + T^{e+1}\mathcal{O}_L[\![T]\!]$, we have $|g|_{Z_k^\eta} = |f^*(g)|_{Z_l^{\eta^{1/e}}}$ for any $g \in C_k$. Hence the map f^* extends continuously to $f_\eta^* : K\langle \eta/S, S/\eta\rangle \to L\langle \eta^{1/e}/T, T/\eta^{1/e}\rangle$.

(3) The first statement follows from Lemma 2.2.10. The second statement is true because $\Gamma_L^\dagger \otimes_{\Gamma^\dagger} \mathcal{R}_K$ is complete and dense in $\mathcal{R}_L$.

(4) follows from (2) and (3) since $\mathcal{R}_K$ and $\mathcal{R}_L$ are limits of $\mathcal{R}_K^{\eta_0}$ and $\mathcal{R}_L^{\eta_0^{1/e}}$, respectively. □

Remark 3.3.14. The homomorphism f^* does not respect the naïve K-algebra structure on $\mathcal{R}_L^{\eta_0^{1/e}}$; this is precisely because of Caution 3.3.4. But it respects the K-algebra structure on $\mathcal{R}_L^{\eta_0^{1/e}}$ induced by $\mathcal{O}_K \hookrightarrow \mathcal{O}_K[\![S]\!] \xrightarrow{f^*} \mathcal{O}_L[\![T]\!]$. So, it might be better not to view $Z_l^{\ge \eta_0^{1/e}} \to Z_k^{\ge \eta_0}$ as a morphism between rigid spaces, but rather as the geometric incarnation of f^*.

Construction 3.3.15. Keep the notation as in Construction 2.2.15. Let $\rho : G_{l/k} \to \mathrm{GL}(V_\rho)$ be a p-adic representation, where V_ρ is a finite dimensional vector space over F. We have

$$\begin{aligned}\mathscr{E}_\rho &= D^\dagger(\rho) \otimes_{\Gamma_K^\dagger} \mathscr{R}_K = (V_\rho \otimes_{\mathbb{O}} \tilde{\Gamma}^\dagger)^{G_k} \otimes_{\Gamma_K^\dagger} \mathscr{R}_K \\ &= (V_\rho \otimes_{\mathbb{Z}_q} \Gamma_L^\dagger)^{G_{l/k}} \otimes_{\Gamma_K^\dagger} \mathscr{R}_K = (V_\rho \otimes_{\mathbb{Z}_q} \mathscr{R}_L)^{G_{l/k}}.\end{aligned}$$

Hence, for some $\eta_0 \in (0, 1)$, the differential module $\mathscr{E}_\rho$ descends to

$$\mathscr{E}_\rho = \big(V_\rho \otimes_{\mathbb{Z}_q} f_* \mathcal{O}_{Z_l^{\geq \eta_0^{1/e}}}\big)^{G_{l/k}};$$

this is a differential module over $\mathscr{R}_K^{\eta_0} \otimes_{\mathbb{Q}_q} F = \mathscr{R}_{K'}^{\eta_0}$ relative to K_0. This construction respects tensor products, i.e., given another p-adic representation ρ' of $G_{l/k}$ over F, we have

$$\mathscr{E}_{\rho \otimes \rho'} = \mathscr{E}_\rho \otimes_{\mathscr{R}_{K'}^{\eta_0}} \mathscr{E}_{\rho'}.$$

Hypothesis 3.3.16. From now on, we always assume that $\eta_0 \in (0, 1)$ is close enough to 1^- that all statements in Lemma 3.3.13 hold and $\mathscr{E}_\rho$ descends to $\mathscr{R}_{K'}^{\eta_0}$.

3.4. ***Spectral norms and connected components of thickening spaces.*** We now relate the spectral norms of differential operators on $\mathscr{E}$ to the connected components of certain rigid spaces. We keep Hypotheses 2.3.2, 3.3.1, and 3.3.16 in this subsection.

Definition 3.4.1. Let $a \in \mathbb{Q}_{>1}$. We define

$$\begin{aligned}\mathcal{O}_{TS_{l/k}^{a,\geq\eta_0}} &= \mathscr{R}_L^{\eta_0^{1/e}} \otimes_{f^*, \mathscr{R}_K^{\eta_0}, \pi^*} \mathcal{O}_{TS_k^{a,\geq\eta_0}}, \\ \mathcal{O}_{TS_{k\backslash l}^{a,\geq\eta_0}} &= \mathcal{O}_{TS_k^{a,\geq\eta_0}} \otimes_{\tilde{\pi}^*, \mathscr{R}_K^{\eta_0}, f^*} \mathscr{R}_L^{\eta_0^{1/e}}, \\ \mathcal{O}_{TS_{l/k\backslash l}^{a,\geq\eta_0}} &= \mathscr{R}_L^{\eta_0^{1/e}} \otimes_{f^*, \mathscr{R}_K^{\eta_0}, \pi^*} \mathcal{O}_{TS_k^{a,\geq\eta_0}} \otimes_{\tilde{\pi}^*, \mathscr{R}_K^{\eta_0}, f^*} \mathscr{R}_L^{\eta_0^{1/e}}.\end{aligned}$$

Here we do not have to complete the tensor products because f^* is finite. (We intentionally put the tensor products on different sides so that it is easy to distinguish the two base changes by f^* through π^* and $\tilde{\pi}^*$ respectively.) Let $TS_{l/k}^{a,\geq\eta_0}$, $TS_{k\backslash l}^{a,\geq\eta_0}$, and $TS_{l/k\backslash l}^{a,\geq\eta_0}$, respectively, denote the geometric incarnations of these rings. We have formally the following Cartesian diagram:

$$\begin{tikzcd}
Z_l^{\geq \eta_0^{1/e}} \arrow[d, "f"] & TS_{l/k}^{a,\geq\eta_0} \arrow[l, "1\times\pi"'] \arrow[d, "f\times 1"] & TS_{l/k\backslash l}^{a,\geq\eta_0} \arrow[l, "\tilde{f}"'] \arrow[d] \\
Z_k^{\geq\eta_0} & TS_k^{a,\geq\eta_0} \arrow[l, "\pi"'] \arrow[d, "\tilde{\pi}"] & TS_{k\backslash l}^{a,\geq\eta_0} \arrow[l, "1\times f"'] \arrow[d] \\
& Z_k^{\geq\eta_0} & Z_l^{\geq\eta_0^{1/e}}. \arrow[l, "f"']
\end{tikzcd} \tag{3.4.2}$$

We make similar constructions for the logarithmic version of all spaces if $a \in \mathbb{Q}_{>0}$.

Remark 3.4.3. The morphisms π and $1\times f$ are genuine morphisms between rigid spaces over $Z_k^{\geq\eta_0}$, and $\tilde f$ and $1\times\pi$ are genuine morphisms between rigid spaces over $Z_l^{\geq\eta_0^{1/e}}$. This is because the rigid space structures on thickening spaces are given by the projections π and $1\times\pi$, respectively. In contrast, all the vertical arrows in (3.4.2) should all be thought of as just geometric incarnations of the corresponding ring homomorphisms.

Remark 3.4.4. The naïve base change $f\times 1$ helps to realize geometric connected components as connected components (see Theorem 3.4.12). The base change $\tilde f$ (and also $1\times f$) encodes the ramification information, which is what we are interested in.

Remark 3.4.5. One may want to relate $TS_{l/k\backslash l}^{a,\geq\eta_0}$ to the thickening space of $Z_l^{\geq\eta_0^{1/e}}$. However, it is not clear how to compare the levels or radii of the two spaces. We will not need this result.

Corollary 3.4.6. *The space $TS_{l/k\backslash l}^{a,\geq\eta_0}$ admits an action of $G_{l/k}$ by morphisms between K-rigid spaces, obtained by pulling back the action on $Z_l^{\geq\eta_0^{1/e}}$ over $Z_k^{\geq\eta_0}$ via $\tilde\pi\circ(f\times 1)$. Under this action, $\tilde f_*\mathcal{O}_{TS_{l/k\backslash l}^{a,\geq\eta_0}}$ is a regular representation of $G_{l/k}$ over $\mathcal{O}_{TS_{l/k}^{a,\geq\eta_0}}$. For a p-adic representation ρ of $G_{l/k}$ over F, define*

$$\tilde{\mathcal{F}}_\rho=(V_\rho\otimes_{\mathbb{Q}_q}\tilde f_*\mathcal{O}_{TS_{l/k\backslash l}^{a,\geq\eta_0}})^{G_{l/k}};$$

this is a differential module over $TS_{l/k}^{a,\geq\eta_0}\times_{\mathbb{Q}_q}F$ relative to $Z_l^{\geq\eta_0^{1/e}}\times_{\mathbb{Q}_q}F$. Moreover, $\tilde{\mathcal{F}}_\rho\simeq(f\times 1)^*\tilde\pi^*\mathcal{E}_\rho$.

The same statement also holds for log-space.

Proof. The differential module structure on $\tilde f_*\mathcal{O}_{TS_{l/k\backslash l}^{a,\geq\eta_0}}$ is given by the composition of natural homomorphisms

$$\begin{aligned}\tilde f_*\mathcal{O}_{TS_{l/k\backslash l}^{a,\geq\eta_0}}\longrightarrow \tilde f_*\big(\Omega^1_{TS_{l/k\backslash l}^{a,\geq\eta_0}/Z_l^{\geq\eta_0^{1/e}}}\big)&\simeq \tilde f_*\Big(\tilde f^*\big(\Omega^1_{TS_{l/k}^{a,\geq\eta_0}/Z_l^{\geq\eta_0^{1/e}}}\big)\Big)\\&\simeq \tilde f_*\mathcal{O}_{TS_{l/k\backslash l}^{a,\geq\eta_0}}\otimes\Omega^1_{TS_{l/k}^{a,\geq\eta_0}/Z_l^{\geq\eta_0^{1/e}}}.\end{aligned}$$

(In fact this construction works for any finite étale morphisms.) The statement of the corollary is an easy consequence of flat base change for the two Cartesian squares on the right in (3.4.2). □

Notation 3.4.7. We may view $1\times\pi: TS_{l/k}^{a,\eta_0}\to Z_l^{\eta_0^{1/e}}$ as bundles, whose fibers are polydiscs (of different radii) with parameters $\delta_0,\dots,\delta_m$; again this morphism is a genuine morphism between rigid spaces. By the *zero section* $\mathbf{Z}$, we mean the natural closed subspace of this bundle defined by $\delta_0=0,\dots,\delta_m=0$.

Notation 3.4.8. Let M be a differential module over a differential ring R with derivatives $\partial_1,\dots,\partial_n$. For $x\in M$ and $r_1,\dots,r_n\in R$, we define the *Taylor series*

$$\mathbb{T}(x; \partial_1, \dots, \partial_n; r_1, \dots, r_n) = \sum_{\alpha_1, \dots, \alpha_n \in \mathbb{Z}_{\geq 0}} \frac{r_1^{\alpha_1} \dots r_n^{\alpha_n} \partial_1^{\alpha_1} \dots \partial_n^{\alpha_n}}{n!}(x),$$

if it converges. If $x \in R$, we have $\mathbb{T}(ax; \partial_1, \dots, \partial_n; r_1, \dots, r_n) = \mathbb{T}(a; \partial_1, \dots, \partial_n; r_1, \dots, r_n) \cdot \mathbb{T}(x; \partial_1, \dots, \partial_n; r_1, \dots, r_n)$ if all terms converge.

Notation 3.4.9. Let M be a differential module over a differential ring R with derivatives $\partial_1, \dots, \partial_n$. Let $H^0_\nabla(R, M) = \{x \in M \mid \partial_i(x) = 0, i = 1, \dots, n\}$ be the set of horizontal sections of M over R. In particular, if $r_1, \dots, r_n \in R$ are elements such that $\partial_i(r_j) = 1$ if $i = j$ and 0 otherwise, then an elementary calculation shows that the Taylor series $\mathbb{T}(x; \partial_i, \dots, \partial_n; r_1, \dots, r_n)$ is an element in $H^0_\nabla(R, M)$ for any $x \in M$ such that the Taylor series converges.

We usually use the geometric counterparts in places of R and M in the notation. For example, we write $H^0_\nabla(\mathrm{Max}(R), M)$ if R is an affinoid algebra.

The following lemma will be frequently used in proving the theorem below. It works in greater generality, but we content ourselves with this special case.

Lemma 3.4.10 (Dwork's transfer theorem). *Let $a > 1$. Let $\tilde{\mathscr{F}}$ be a differential module over $TS^{a,\geq\eta_0}_{l/k}$ relative to $Z_l^{\geq\eta_0^{1/e}}$. Assume $|\partial/\partial\delta_i|_{\tilde{\mathscr{F}}_{a,\eta}} \leq p^{-1/(p-1)}\eta^{-a}$ for all $j \in J$ and $\eta \in [\eta_0, 1)$. Then, for any rational number $c > a$, the natural homomorphism of finite $\mathscr{R}_L^{\eta_0^{1/e}}$-modules*

$$\Theta : H^0_\nabla(TS^{c,\geq\eta_0}_{l/k}, \tilde{\mathscr{F}}) \xrightarrow{\sim} \Gamma(\mathbf{Z}, \tilde{\mathscr{F}}|_{\mathbf{Z}}) \tag{3.4.11}$$

is an isomorphism. In particular, $\tilde{\mathscr{F}}$ is a trivial ∇-module relative to $Z_l^{\geq\eta_0^{1/e}}$. The same statement is also true if we base-change everything to F over $\mathbb{Q}_q$. When $\tilde{\mathscr{F}} = f_*\mathcal{O}_{TS^{a,\geq\eta_0}_{l/k\backslash l}}$, Θ induces a ring *homomorphism for any rational number $c > a$:*

$$\Gamma\big(\mathbf{Z}, f_*\mathcal{O}_{TS^{c,\geq\eta_0}_{l/k\backslash l}}\big|_{\mathbf{Z}}\big) \xleftarrow[\sim]{\Theta} H^0_\nabla\big(TS^{c,\geq\eta_0}_{l/k}, f_*\mathcal{O}_{TS^{c,\geq\eta_0}_{l/k\backslash l}}\big) \hookrightarrow \Gamma\big(TS^{c,\geq\eta_0}_{l/k\backslash l}, \mathcal{O}_{TS^{c,\geq\eta_0}_{l/k\backslash l}}\big).$$

The same statements hold for the log version with $a > 0$, inserting the subscript log *appropriately.*

Proof. We prove the lemma for the nonlog case over $\mathbb{Q}_q$. The proof for the log case differs only by inserting subscript log appropriately, using the δ_0 coordinate, and increasing the exponents on η by 1. The proof for the tensor F version is also the same, except we need to tensor F everywhere.

We may define an inverse of the map Θ using Taylor series:

$$\Theta^{-1}(x) = \mathbb{T}(\tilde{x}; \partial/\partial\delta_0, \dots, \partial/\partial\delta_m; \delta_0, \dots, \delta_m)$$

for $x \in \Gamma(\mathbf{Z}, \tilde{\mathscr{F}}|_{\mathbf{Z}})$, where $\tilde{x}$ is a lift of x in $\Gamma(TS^{c,\geq\eta_0}_{l/k}, \tilde{\mathscr{F}})$. The Taylor series converges over $TS^{c,\geq\eta_0}_{l/k}$ by the condition $|\partial/\partial\delta_i|_{\tilde{\mathscr{F}}_{a,\eta}} \leq p^{-1/(p-1)}\eta^{-a} < p^{-1/(p-1)}\eta^{-c}$ for all $j \in J$ and $\eta \in [\eta_0, 1)$. Moreover, the Taylor series converges to a horizontal section in $H^0_\nabla(TS^{c,\geq\eta_0}_{l/k}, \tilde{\mathscr{F}})$.

When $\tilde{\mathscr{F}} = f_*\mathbb{O}_{TS^{a,\geq\eta_0}_{l/k\backslash l}}$, Θ is a homomorphism, which can also be seen from the fact that the Taylor series gives a ring homomorphism (see Notation 3.4.8). $\square$

The following theorem is one of the key steps of the proof of the Hasse–Arf theorem. This is the main ingredient (a) described in the introduction. It allows us to compare the differential ramification breaks with the geometric connected components of the thickening spaces; we will later identify the thickening spaces with the lifts of the Abbes–Saito spaces (Theorem 4.3.6).

Theorem 3.4.12. *Let $\rho : G_{l/k} \to \mathrm{GL}(V_\rho)$ be a* faithful *p-adic representation over F with l/k satisfying Hypotheses 2.3.2 and 3.3.1. Then, for $b > 1$, the following conditions are equivalent*:

(a) *ρ has differential ramification break $\leq b$.*

(b) *For any rational number $c > b$, when $\eta_0 \to 1^-$, $\tilde{\mathscr{F}} = \tilde{\mathscr{F}}_\rho$ is a trivial ∇-module over $TS^{c,\geq\eta_0}_{l/k} \times_{\mathbb{Q}_q} F$ relative to $Z_l^{\geq\eta_0^{1/e}} \times_{\mathbb{Q}_q} F$.*

(c) *For any rational number $c > b$, when $\eta_0 \to 1^-$, $TS^{c,\geq\eta_0}_{l/k\backslash l}$ has exactly $[l : k]$ connected components.*

(d) *For any rational number $c > b$, when $\eta_0 \to 1^-$, $Z_{l'}^{\geq\eta_0^{1/e'}} \times_{Z_l^{\geq\eta_0^{1/e}},\pi} TS^{c,\geq\eta_0}_{l/k\backslash l}$ has exactly $[l : k]$ connected components for some finite extension l'/l, where e' is the naïve ramification degree of l'/k.*

For $b > 0$, the corresponding conditions for logarithmic spaces are equivalent.

Proof. We prove the statement for nonlogarithmic spaces; in the logarithmic case we just need to add the subscript log and change the scales on ∂_0 and $\partial/\partial\delta_0$ from η^b to η^{b+1} and η^c to η^{c+1}.

Further, Proposition 3.2.17 is unchanged if we replace $\mathscr{F}$ by $\tilde{\mathscr{F}}$, since the spectral norms are invariant under scalar extensions.

We first that (a) implies (b). Assume ρ has differential ramification break at most b. By Definition 2.3.20, for η_0 sufficiently close to 1^-, the generic radius of $\mathscr{E}_\rho$ satisfies $\boldsymbol{T}(\mathscr{E}_\rho, \eta) \geq \eta^b$ for $\eta \in [\eta_0, 1)$, or equivalently $|\partial_j|_{\mathscr{E}_{\rho,\eta},\mathrm{sp}} \leq p^{-1/(p-1)}\eta^{-b}$ for any $j \in J^+$ and $\eta \in [\eta_0, 1)$. Then Proposition 3.2.17 and Remark 2.3.5 imply that for all $\eta \in [\eta_0, 1)$, $|\partial/\partial\delta_j|_{\tilde{\mathscr{F}}_{b,\eta},\mathrm{sp}} \leq p^{-1/(p-1)}\eta^{-b}$, and hence $\tilde{\mathscr{F}}_\rho$ is a trivial differential module over $TS^{c,\geq\eta_0}_{l/k} \times_{\mathbb{Q}_q} F$ relative to $Z_l^{\geq\eta_0^{1/e}} \times_{\mathbb{Q}_q} F$ for any rational number $c > b$ by Dwork's transfer theorem (Lemma 3.4.10). This proves (b).

Now assume (b), i.e., $\tilde{\mathscr{F}}_\rho$ is trivial over $TS^{c,\geq\eta_0}_{l/k} \times_{\mathbb{Q}_q} F$ relative to $Z_l^{\geq\eta_0^{1/e}} \times_{\mathbb{Q}_q} F$ for any rational number $c > b$ and some $\eta_0 \in (0, 1)$. It follows that

$$|\partial/\partial\delta_j|_{\tilde{\mathscr{F}}_{c,\eta},\mathrm{sp}} = |\partial/\partial\delta_j|_{\mathrm{Frac}(\mathbb{O}_{TS^{c,\eta}_{l/k}})^\wedge,\mathrm{sp}} = p^{-1/(p-1)}\eta^{-c}.$$

By Proposition 3.2.17, $|\partial_j|_{\mathrm{sp},\mathscr{E}_\eta} \leq p^{-1/(p-1)}\eta^{-c}$, for any $j \in J^+$, $\eta \in [\eta_0, 1)$, and $c \in \mathbb{Q}_{>b}$. By Definition 2.3.20, this implies that the differential ramification break is at most b, since the rationals are dense in the real numbers.

Obviously, (c) implies (b). To see the converse, note first claim that if $c > b$ is rational, $f_*\mathcal{O}_{TS^{c,\geq\eta_0}_{l/k\backslash l}}$ is a trivial differential module over $TS^{c,\geq\eta_0}_{l/k}$ relative to $Z_l^{\geq\eta_0^{1/e}}$. Indeed, for a rational number $c' \in (b, c)$, we know that $\tilde{\mathscr{F}}_\rho$ is a trivial differential module over $TS^{c',\geq\eta_0}_{l/k} \times_{\mathbb{Q}_q} F$ relative to $Z_l^{\geq\eta_0^{1/e}} \times_{\mathbb{Q}_q} F$, then for any $n \in \mathbb{N}$, $\tilde{\mathscr{F}}_\rho^{\otimes n}$ is also a trivial differential module (relative to $Z_l^{\geq\eta_0^{1/e}} \times_{\mathbb{Q}_q} F$), which corresponds to $V_\rho^{\otimes n}$ by functoriality (Construction 3.3.15). By Lemma 3.4.16 below from the theory of representations of finite groups (or standard Tannakian arguments), the differential module

$$\big(F[G_{l/k}] \otimes_{\mathbb{Q}_q} f_*\mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}}\big)^{G_{l/k}} \xrightarrow{\simeq} F \otimes_{\mathbb{Q}_q} f_*\mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}} \tag{3.4.13}$$

corresponding to the regular representation is a direct summand of a direct sum of some $\tilde{\mathscr{F}}_\rho^{\otimes n}$'s and hence is a trivial differential module (relative to $Z_l^{\geq\eta_0^{1/e}} \times_{\mathbb{Q}_q} F$). To make it perfectly rigorous, here the isomorphism (3.4.13) of differential modules is given by $\sum_{g\in G_{l/k}} \boldsymbol{f} g \otimes g\boldsymbol{v} \mapsto \boldsymbol{f}\cdot\boldsymbol{v}$, where $\boldsymbol{f} \in F$ and $\boldsymbol{v} \in f_*\mathcal{O}_{TS^{c,\geq\eta_0}_{l/k\backslash l}}$; this map does *not* respect the $F[G_{l/k}]$-module structures.

We have finished the proof of the claim in the case $F = \mathbb{Q}_p$. If $F \neq \mathbb{Q}_p$, we know that, for all $j \in J^+$, the spectral norms of $\partial/\partial\delta_j$ at radius η on the right-hand side of (3.4.13) are $p^{-1/(p-1)}\eta^{-c'}$, which equal the spectral norms of $\partial/\partial\delta_j$ on $f_*\mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}}$ at radius η. By Dwork's transfer theorem (Lemma 3.4.10), the claim is proved.

We now apply the second part of Lemma 3.4.10 and obtain, for any rational numbers $c' > c$, a *ring* homomorphism

$$\Gamma\big(\boldsymbol{Z}, f_*\mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}}\big|_{\boldsymbol{Z}}\big) \overset{\Theta}{\underset{\sim}{\longleftarrow}} H^0_\nabla\big(TS^{c',\geq\eta_0}_{l/k}, f_*\mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}}\big) \hookrightarrow \Gamma\big(TS^{c',\geq\eta_0}_{l/k\backslash l}, \mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}}\big). \tag{3.4.14}$$

The key is that the left-hand side of (3.4.14) is isomorphic to the ring functions on $Z_l^{\geq\eta_0^{1/e}} \times_{Z_k^{\geq\eta_0}} Z_l^{\geq\eta_0^{1/e}}$ because the restrictions of $\tilde{\pi}$ and π to $\boldsymbol{Z}$ are both the same as f. Moreover, since $Z_l^{\geq\eta_0^{1/e}}$ is finite étale Galois over $Z_k^{\geq\eta_0}$ (Lemma 3.3.13), $Z_l^{\geq\eta_0^{1/e}} \times_{Z_k^{\geq\eta_0}} Z_l^{\geq\eta_0^{1/e}} = \coprod_{g\in G_{l/k}} Z_l^{\geq\eta_0^{1/e}}$. In particular, we have fundamental idempotent elements in $\Gamma(\boldsymbol{Z}, f_*\mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}}|_{\boldsymbol{Z}})$ corresponding to each connected component. Via the composition of the homomorphisms in (3.4.14), we can "lift" the idempotent elements on $Z_l^{\geq\eta_0^{1/e}} \times_{Z_k^{\geq\eta_0}} Z_l^{\geq\eta_0^{1/e}}$ to idempotent elements in $\mathcal{O}_{TS^{c',\geq\eta_0}_{l/k\backslash l}}$. This shows that $TS^{c',\geq\eta_0}_{l/k\backslash l}$ has at least $[l:k]$ connected components. But this space is finite and flat of degree $[l:k]$ over an irreducible rigid space $TS^{c',\geq\eta_0}_{l/k}$; it can have at most $[l:k]$ connected components. Therefore, (c) holds.

The equivalence between (b) and (d) can be proved similarly, using a version of Lemma 3.4.10 over $Z_{l'}^{\eta_0^{1/e'}}$. The upshot here is that we need a base change to at least $Z_l^{\geq\eta_0^{1/e}}$ in (c) so that we can split the fiber over $\boldsymbol{Z}$; this is why we did not state the theorem for $TS^{c,\geq\eta_0}_{k\backslash l}$ and $\tilde{\mathscr{F}}$ themselves. □

Remark 3.4.15. The faithfulness condition on ρ in the theorem is harmless: we will very easily reduce to this case later in the proof of Theorem 4.4.1.

Lemma 3.4.16. *Let G be a finite group and F be a field of characteristic* 0. *Let $\rho : G \to \mathrm{GL}(V_\rho)$ be a faithful representation over F. Then the regular representation $F[G]$ is a direct summand of a direct sum of some self-tensor products of V_ρ.*

This is an easy exercise of finite group representations but we do not know a good reference. The author thanks Xuhua He for providing the following proof.

Proof. Let χ be the character of V_ρ and let d be the dimension of V_ρ. Since the representation is injective, $\chi(1) = d$ and $\chi(g) \neq d$ for all $g \in G$ nontrivial. (This is because all the eigenvalues of $\rho(g)$ are roots of unity and cannot all be 1.)

Therefore, for each $g \neq 1$ there exists a polynomial P_g in χ with integer coefficients such that $P_g(\chi(g)) = 0$ but $P_g(d) \neq 0$. Let $P = \prod_{1 \neq g \in G} P_g$; then $P(d) \neq 0$ but $P(\chi(g)) = 0$ for all $g \neq 1$. Multiplying by a constant, we may assume that $\#G$ divides $P(d)$ and $P(d) > 0$. If $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$, then $(V^{\otimes n})^{\oplus a_n} \oplus \cdots \oplus V^{\oplus a_1} \oplus \mathbf{1}_F^{\oplus a_0} = F[G]^{P(d)/\#G}$ in the Grothendieck group of the representations of G, where $\mathbf{1}_F$ denotes the trivial representation. Consequently, if we take the direct sum of the terms on the left-hand side with positive a_i, the regular representation will be a natural direct summand of it. □

4. Arithmetic ramification filtrations

4.1. ***Review of Abbes and Saito's definition.*** We briefly review the definition of arithmetic ramification filtrations on the Galois group of a complete discretely valued field k. For more details, consult [Abbes and Saito 2002; 2003]. The filtrations can be defined for a k of mixed characteristic; however, for the purpose of this paper, we focus on the case where k is of equal characteristic $p > 0$.

In this subsection, we do *not* make any of the hypothesis we have been using in previous sections.

Notation 4.1.1. Keep the notation as in previous sections. Fix uniformizers s and t for k and l, respectively. Let $v_l(\cdot)$ be the valuation on l normalized so that $v_l(t) = 1$. Let $\theta = |s|$.

Notation 4.1.2. In this subsection, we temporarily free j and J from the restraint introduced in Notation 2.3.3. But in later applications, we will specialize to the case in which j and J actually index p-bases.

Definition 4.1.3. Take $Z = (z_j)_{j \in J} \subset \mathcal{O}_l$ to be a finite set of elements generating $\mathcal{O}_l$ as an $\mathcal{O}_k$-algebra, i.e., $\mathcal{O}_k[(u_j)_{j \in J}]/\mathcal{I} \xrightarrow{\sim} \mathcal{O}_l$ mapping u_j to z_j for $j \in J = \{1, \dots, m\}$ and for some appropriate ideal $\mathcal{I}$. Let $(f_i)_{i=1,\dots,n}$ be a finite set of generators of $\mathcal{I}$. For $a \in \mathbb{Q}_{>0}$, define the (*nonlogarithmic*) *Abbes–Saito space* to be

$$as^a_{l/k,Z} = \Big\{ (u_1, \dots, u_m) \in A^m_k[0, 1] \,\Big|\, |f_i(u_J)| \leq \theta^a,\ 1 \leq i \leq n \Big\}. \tag{4.1.4}$$

The *geometric* connected components (see [Bosch et al. 1984, 9.1.4/8] for the definition) of $as^a_{l/k,Z}$ are $\pi_0^{\mathrm{geom}}(as^a_{l/k,Z})$. The *arithmetic ramification break* $b_{\mathrm{ar}}(l/k)$ is defined as the minimal number b such that $\#\pi_0^{\mathrm{geom}}(as^a_{l/k,Z}) = [l:k]$ for any $a > b$.

Definition 4.1.5. Keep the notation as above. We single out a subset $P \subset Z$ and assume that P and hence Z contain the uniformizer t. For each $j \in J$, let $e_j = v_l(z_j)$. Take a lift $g_j \in \mathbb{O}_k[(u_j)_{j\in J}]$ of z_j^e/s^{e_j} for each $z_j \in P$, and take a lift $h_{i,j} \in \mathbb{O}_k[(u_j)_{j\in J}]$ of $z_j^{e_i}/z_i^{e_j}$ for each pair $(z_i, z_j) \in P \times P$. For $a \in \mathbb{Q}_{>0}$, define the *logarithmic Abbes–Saito space* to be

$$as^a_{l/k,\log,Z,P} = \left\{ (u_J) \in A^m_k[0,1] \;\middle|\; \begin{array}{ll} |f_i(u_J)| \le \theta^a, & 1 \le i \le n, \\ |u_j^e - s^{e_j} g_j| \le \theta^{a+e_j}, & \text{for all } z_j \in P, \\ |u_j^{e_i} - u_i^{e_j} h_{i,j}| \le \theta^{a+e_ie_j/e}, & \text{for all } (z_i, z_j) \in P \times P. \end{array} \right\}$$

Similarly, the *logarithmic arithmetic ramification break* $b_{ar,\log}(l/k)$ is defined to be the minimal number b such that for any $a > b$, $\#\pi_0^{\mathrm{geom}}(as^a_{l/k,\log,Z,P}) = [l:k]$.

Remark 4.1.6. To ease the readers who are not familiar with Abbes and Saito's definition, we give an intuitive way to understand the definition following [Abbes and Saito 2002].

First, if $a \to \infty$, the conditions on $f_1, \dots, f_n$ in (4.1.4) basically restrict the possible u_J to be very close to z_J or other solutions to the equations $f_1 = 0, \dots, f_n = 0$, which are exactly Galois conjugates of z_J. Thus, one may believe that $as^a_{l/k,Z}$ has exactly $[l:k]$ geometric connected components, each of which looks like a small polydisc centered at one of the solutions. In contrast, if $a \to 0^+$, the conditions on $f_1, \dots, f_n$ are almost vacuum and $as^a_{l/k,Z}$ is almost the whole unit polydisc. In particular, the space is likely to be geometrically connected. From the two extreme cases, we know that, when we increase a, the Abbes–Saito space shrinks from a whole unit polydisc to smaller polydiscs and, at some a, a bigger polydisc breaks apart into several smaller polydiscs. The arithmetic ramification break captures the last break point.

We reproduce several statements from [Abbes and Saito 2002; 2003].

Proposition 4.1.7. *Abbes–Saito spaces have the following properties.*

(1) *For $a > 0$, the spaces $as^a_{l/k,Z}$ and $as^a_{l/k,\log,Z,P}$ do not depend on the choice of generators $(f_i)_{i=1,\dots,n}$ of $\mathcal{I}$ and lifts g_j and $h_{i,j}$ for $i, j \in P$* [Abbes and Saito 2002, §3].

(1′) *If, in the definition of both spaces, we choose polynomials $(f_i)_{i=1,\dots,n}$ as a set of generators of* $\mathrm{Ker}(\mathbb{O}_k\langle(u_j)_{j\in J}\rangle \to \mathbb{O}_l)$ *instead of* $\mathrm{Ker}(\mathbb{O}_k[(u_j)_{j\in J}] \to \mathbb{O}_l)$, *the spaces will not change.*

(2) *If we substitute in another pair of generating sets Z and P satisfying the same properties, then we have a canonical bijection on the sets of the geometric connected components $\pi_0^{\mathrm{geom}}(as^a_{l/k,Z})$ and $\pi_0^{\mathrm{geom}}(as^a_{l/k,\log,Z,P})$ for different generating sets, where $a > 0$. In particular, both highest arithmetic ramification breaks are well-defined* [Abbes and Saito 2002, §3].

(3) *The highest arithmetic ramification break* (*resp. highest logarithmic arithmetic ramification break*) *gives rise to a filtration on the Galois group G_k consisting of normal subgroups* $\mathrm{Fil}^a G_k$ (*resp.* $\mathrm{Fil}^a_{\log} G_k$) *for $a > 0$ such that* $b_{\mathrm{ar}}(l/k) = \inf\{a \mid \mathrm{Fil}^a G_k \subseteq G_l\}$ (*resp.* $b_{ar,\log}(l/k) = \inf\{a \mid \mathrm{Fil}^a_{\log} G_k \subseteq G_l\}$) [Abbes and Saito 2002, Theorems 3.3 and 3.11]. *Moreover, for l/k a finite Galois extension, both arithmetic ramification breaks are rational numbers* [Abbes and Saito 2002, Theorems 3.8 and 3.16].

(4) *Let k'/k be an algebraic extension of complete discretely valued fields or the completion of such an extension. If k'/k is unramified, then* $\mathrm{Fil}^a G_{k'} = \mathrm{Fil}^a G_k$ *for $a > 0$* [Abbes and Saito 2002, Proposition 3.7]. *If k'/k is tamely ramified with ramification index e', then* $\mathrm{Fil}^{e'a}_{\log} G_{k'} = \mathrm{Fil}^a_{\log} G_k$ *for $a > 0$* [Abbes and Saito 2002, Proposition 3.15]. *More generally, for a* (*not necessarily algebraic*) *extension k'/k of complete discretely valued fields with the* same *valued group and linearly independent from l/k such that $\mathbb{O}_{lk'} = \mathbb{O}_{k'} \otimes_{\mathbb{O}_k} \mathbb{O}_l$, we have* $b_{\mathrm{ar}}(lk'/k') = b_{\mathrm{ar}}(l/k)$ *and* $b_{ar,\log}(lk'/k') = b_{ar,\log}(l/k)$ [Abbes and Mokrane 2004, lemme 2.1.5].

(5) *For $a > 0$, define* $\mathrm{Fil}^{a+} G_k = \overline{\bigcup_{b>a} \mathrm{Fil}^b G_k}$ *and* $\mathrm{Fil}^{a+}_{\log} G_k = \overline{\bigcup_{b>a} \mathrm{Fil}^b_{\log} G_k}$. *Then, the subquotients* $\mathrm{Fil}^a G_k / \mathrm{Fil}^{a+} G_k$ *are abelian p-groups if $a \in \mathbb{Q}_{>1}$ and are* 0 *if $a \notin \mathbb{Q}$* ([Abbes and Saito 2002, Theorem 3.8] *and* [Abbes and Saito 2003, Theorem 1]); *the subquotients* $\mathrm{Fil}^a_{\log} G_k / \mathrm{Fil}^{a+}_{\log} G_k$ *are elementary abelian p-groups if $a \in \mathbb{Q}_{>0}$ and are* 0 *if $a \notin \mathbb{Q}$* ([Abbes and Saito 2002, Theorem 3.16] *and* [Saito 2009, Theorem 1.3.3]).

(6) *The inertia subgroup is* $\mathrm{Fil}^a G_k$ *if $a \in (0, 1]$ and the wild inertia subgroup is* $\mathrm{Fil}^{1+} G_k = \mathrm{Fil}^{0+}_{\log} G_k$ [Abbes and Saito 2002, Theorems 3.7 and 3.15].

(7) *When the residue field κ_k is perfect, the arithmetic ramification filtrations agree with the classical upper numbered filtrations in the following way:* $\mathrm{Fil}^a G_k = \mathrm{Fil}^{a-1}_{\log} G_k = \mathrm{Gal}^{a-1}_k$ *for $a \geq 1$* [Abbes and Saito 2002, §6.1], *where* Gal^a_k *is the classical upper numbered filtration on G_k.*

Proof. For the convenience of readers, we point out some ingredients of the proof. For details, one can consult the original papers.

(1) is straightforward by matching up points.

(1′) is not in the literature. However, it can be proved identically to (1).

(2) One can show that if we add a new (dummy) generator in Z or P, the new Abbes–Saito space admits a fibration over the original Abbes–Saito space whose fibers are closed discs of radius θ^a.

(3) The first statement is just abstract nonsense. The second is true essentially because Abbes–Saito spaces are defined over k and the geometric connect components can be detected over the algebraic closure k^{alg}, which has valued group $|k^\times|^{\mathbb{Q}}$. However, realizing this principle requires formal models of rigid spaces. As we will reprove this result in Theorem 4.4.1, we refer to the original paper for the formal model proof.

(4) When $\mathbb{O}_{lk'} \simeq \mathbb{O}_l \otimes_{\mathbb{O}_k} \mathbb{O}_{k'}$, one can match up the nonlogarithmic Abbes–Saito space for lk'/k' and the extension of the scalar of that for lk'/k' in a natural way. Actually, the logarithmic ramification break is not considered in [Abbes and Mokrane 2004, lemme 2.1.5], but the proof carries over similarly. In the tamely ramified and logarithmic cases, one can also identify two logarithmic Abbes–Saito spaces [2002, Proposition 9.8]; this is slightly more complicated.

(5) The proof used the formal models of the Abbes–Saito spaces and their stable reductions, which is in an orthogonal direction from the present paper. One may consult [Abbes and Saito 2003; Saito 2009] for a complete treatment.

(6) is an easy fact.

(7) follows from an explicit calculation in the monogenic case. □

Remark 4.1.8. In fact, in the proof of the main theorem (Theorem 4.4.1), we do not need (5) or the second statement of (3) on the rationality of the breaks in the proposition above. Therefore, we can obtain these properties from the properties of differential conductors in Theorem 2.4.1 via the comparison in Theorem 4.4.1.

Definition 4.1.9. Let $\rho : G_k \to \mathrm{GL}(V_\rho)$ be a representation of finite local monodromy. Define the *arithmetic Artin and Swan conductors* as

$$\mathrm{Art}_{\mathrm{ar}}(\rho) \stackrel{\mathrm{def}}{=} \sum_{a \in \mathbb{Q}_{\geq 0}} a \cdot \dim\big(V_\rho^{\mathrm{Fil}^{a+} G_k} / V_\rho^{\mathrm{Fil}^{a} G_k}\big), \tag{4.1.10}$$

$$\mathrm{Swan}_{\mathrm{ar}}(\rho) \stackrel{\mathrm{def}}{=} \sum_{a \in \mathbb{Q}_{\geq 0}} a \cdot \dim\big(V_\rho^{\mathrm{Fil}^{a+}_{\log} G_k} / V_\rho^{\mathrm{Fil}^{a}_{\log} G_k}\big). \tag{4.1.11}$$

They are actually finite sums.

Conjecture 4.1.12 (Hasse–Arf Theorem). *Let k be a complete discretely valued field of equal characteristic p. For any representation ρ of G_k of finite local monodromy, the arithmetic conductors are nonnegative integers, namely,* $\mathrm{Art}_{\mathrm{ar}}(\rho) \in \mathbb{Z}_{\geq 0}$ *and* $\mathrm{Swan}_{\mathrm{ar}}(\rho) \in \mathbb{Z}_{\geq 0}$.

Proposition 4.1.13. *Conjecture 4.1.12 is true if the residue field κ_k is perfect.*

Proof. By Proposition 4.1.7(7), we are reduced to the classical Hasse–Arf theorem [Serre 1979, §VI.2, Theorem 1′ and §IV.2, Corollary 3]. Note that in this case, $\mathrm{Swan}_{\mathrm{ar}}(\rho) = \mathrm{Art}_{\mathrm{ar}}(\rho) - \dim V_\rho / V_\rho^{I_k}$. □

We will prove Conjecture 4.1.12 in Corollary 4.4.3.

4.2. *Standard Abbes–Saito spaces and their lifts.* In practice, we will only study Abbes–Saito spaces that are given by some particular generators. We explicitly write down spaces and their lifts in the sense of Section 1.

In this subsection, we retrieve Hypotheses 2.3.2 and 3.3.1, assuming that k has finite p-basis and the extension l/k is totally and wildly ramified. Also, we retrieve Notation 2.3.3 on indexing p-basis.

Construction 4.2.1. We take $Z = \{c_1, \dots, c_m, t\}$ to be the set of generators of $\mathbb{O}_l/\mathbb{O}_k$ given by Construction 3.3.5. (Maybe some of them are already in the field k, but we still keep those.) We take $P = \{t\}$. By Proposition 4.1.7(1′), we can take the relations to be $p_0, \dots, p_m$ from Notation 3.3.8. For $a \in \mathbb{Q}_{>0}$, we define the *standard Abbes–Saito spaces* as

$$as^a_{l/k} = \big\{(u_0, \dots, u_m) \in A_k^{m+1}[0, 1] \,\big|\, |p_0(u_{J^+})| \le \theta^a, \dots, |p_m(u_{J^+})| \le \theta^a\big\},$$
$$as^a_{l/k,\log} = \big\{(u_0, \dots, u_m) \in A_k^{m+1}[0, 1] \,\big|\, |p_0(u_{J^+})| \le \theta^{a+1}, |p_1(u_{J^+})| \le \theta^a, \dots, |p_m(u_{J^+})| \le \theta^a\big\}.$$

Let P_{J^+} be the lifts of p_{J^+} as in Lemma 3.3.13. For $a \in \mathbb{Q}_{>0}$ and $\eta_0 \in (0, 1)$, we define the *lifting Abbes–Saito spaces* to be

$$AS^{a,\ge\eta_0}_{l/k} = \left\{(U_{J^+}, S) \in A_K^{m+2}[0, 1] \,\middle|\, \begin{array}{l} \eta_0 \le |S| < 1, \\ |P_0(U_{J^+}, S)| \le |S|^a, \dots, |P_m(U_{J^+}, S)| \le |S|^a \end{array}\right\},$$
$$AS^{a,\ge\eta_0}_{l/k,\log} = \left\{(U_{J^+}, S) \in A_K^{m+2}[0, 1] \,\middle|\, \begin{array}{l} \eta_0 \le |S| < 1, \qquad |P_0(U_{J^+}, S)| \le |S|^{a+1}, \\ |P_1(U_{J^+}, S)| \le |S|^a, \dots, |P_m(U_{J^+}, S)| \le |S|^a \end{array}\right\};$$

they are viewed as rigid spaces over $Z_k^{\ge\eta_0}$.

Lemma 4.2.2. *Let k'/k be a finite Galois extension of naïve ramification degree e'. If we identify C_k as a subring of $C_{k'}$ as in Construction 3.3.12, we may view P_{J^+} as polynomials in U_{J^+} with coefficients in $\mathbb{O}_{K'}[\![S']\!]$, where K' is the fraction field of the Cohen ring of $\kappa_{k'}$ and S' is a lift of the uniformizer s' in k'. Then, for $\eta_0 \in (0, 1)$ and $a \in \mathbb{Q}_{>0}$, we have*

$$Z_{k'}^{\ge\eta_0^{1/e'}} \times_{Z_k^{\ge\eta_0}} AS^{a,\ge\eta_0}_{l/k} \cong \left\{(U_{J^+}, S') \in A_{K'}^{m+2}[0, 1] \,\middle|\, \begin{array}{c} \eta_0^{1/e'} \le |S'| < 1, \\ |P_0| \le |S'|^{e'a}, \dots, |P_m| \le |S'|^{e'a} \end{array}\right\},$$
$$Z_{k'}^{\ge\eta_0^{1/e'}} \times_{Z_k^{\ge\eta_0}} AS^{a,\ge\eta_0}_{l/k,\log} \cong \left\{(U_{J^+}, S') \in A_{K'}^{m+2}[0, 1] \,\middle|\, \begin{array}{c} \eta_0^{1/e'} \le |S'| < 1, \; |P_0| \le |S'|^{e'(a+1)}, \\ |P_1| \le |S'|^{e'a}, \dots, |P_m| \le |S'|^{e'a} \end{array}\right\};$$

Proof. The only thing not obvious is that we replace $|P_j| \leq |S|^{a(+1)}$ by $|P_j| \leq |S'|^{e'a(+e')}$; this is because $|S| = |S'|^{e'}$ as proved in Lemma 3.3.13(2). □

Remark 4.2.3. Note that $Z_k^{\geq \eta_0} \to Z_{k'}^{\eta_0^{1/e'}}$ is not a morphism between rigid spaces for the reason explained in Remark 3.3.14. So, strictly speaking, $Z_{\tilde{k}'}^{\geq \eta_0^{1/e'}} \times_{Z_k^{\geq \eta_0}} AS_{l/k}^{a, \geq \eta_0}$ and the log counterpart should be thought of as the geometric incarnations of the tensor products of the corresponding ring of analytic functions. The new spaces are, however, well-defined rigid analytic spaces over $Z_{\tilde{k}'}^{\geq \eta_0^{1/e'}}$.

Theorem 4.2.4. *For $a \in \mathbb{Q}_{>0}$, there is a one-to-one correspondence between the geometric connected components of $as^a_{l/k,(\log)}$ and the following limit of connected components*:

$$\varprojlim_{k'/k} \lim_{\eta_0 \to 1^-} \pi_0^{\mathrm{geom}}\big(Z_{k'}^{\geq \eta_0^{1/e'}} \times_{Z_k^{\geq \eta_0}} AS_{l/k(,\log)}^{a, \geq \eta_0}\big),$$

where e' is the naïve ramification degree of k'/k and the second limit only takes $\eta_0 \in p^{\mathbb{Q}} \cap (0, 1)$.

Proof. By Lemma 4.2.2 and Example 1.3.4, when $e'a \in \mathbb{Z}$, $Z_{\tilde{k}'}^{\geq \eta_0^{1/e'}} \times_{Z_k^{\geq \eta_0}} AS_{l/k(,\log)}^{a, \geq \eta_0}$ is a lifting space of $as^a_{l/k(,\log)}$. The theorem then follows from Corollary 1.2.12. □

Remark 4.2.5. Here, we need $\eta_0 \in p^{\mathbb{Q}} \cap (0, 1)$ since Corollary 1.2.12 requires it.

Remark 4.2.6. Introducing this ramified extension k'/k to make $e'a \in \mathbb{Z}$ may not be essential, but it eases the proof.

4.3. ***Comparison of rigid spaces.*** In this subsection, we will prove that the lifting Abbes–Saito spaces are isomorphic to some thickening spaces we constructed in Section 3.4. In this subsection, we continue to assume Hypotheses 2.3.2 and 3.3.1.

Before proving the comparison theorem, we need to analyze Construction 3.3.5 closely and give a new view of $\tilde{\pi}^*$ using differentials. However, the proofs of the following two lemmas are not so enlightening in this generality; the reader may skip them when reading the paper for the first time, but see Remark 4.3.5.

Lemma 4.3.1. *Modulo p, the homomorphism $\tilde{\pi}^*$ gives a continuous homomorphism $\bar{\tilde{\pi}}^* : \kappa_k \to \kappa_k[\![\delta_J]\!]$. For $\bar{g} \in \kappa_k$, we can write $d\bar{g} = \bar{g}_1 d\bar{b}_1 + \cdots + \bar{g}_m d\bar{b}_m$ in $\Omega^1_{\kappa_k/\mathbb{F}_p}$. Then $\bar{\tilde{\pi}}^*(\bar{g}) \equiv \bar{g} + \bar{g}_1\delta_1 + \cdots + \bar{g}_m\delta_m$ modulo $(\delta_J)^2 \cdot \kappa_K[\![\delta_J]\!]$.*

Proof. Use the p-basis to express $\bar{g}$ (uniquely) as $\bar{g} = \sum_{e_J=0}^{p-1} \bar{a}_{e_J}^p \bar{b}_J^{e_J}$ for some $\bar{a}_{e_J} \in \kappa_k$. Thus, $d\bar{g} = \sum_{e_J=0}^{p-1} \bar{a}_{e_J}^p d(\bar{b}_J^{e_J})$. On the other hand, we have

$$\bar{\tilde{\pi}}^*(\bar{g}) \equiv \sum_{e_J=0}^{p-1} \bar{a}_{e_J}^p (\bar{b}_J + \delta_J)^{e_J}$$

modulo $(\delta_J)^p \cdot \kappa_K[\![\delta_J]\!]$. The statement follows by comparing the two formulas. □

Remark 4.3.2. The analogous result for $\tilde{\pi}^*$ is true. Actually, $\tilde{\pi}^*$ is the Taylor expansion homomorphism [Kedlaya 2007, Definition 2.2.2].

Lemma 4.3.3. *Keep the notation as in Section 3.3. We have*

$$\det\left(\frac{\partial(\tilde{\pi}^*(P_i)-P_i)}{\partial\delta_j}\right)_{i,j\in J^+}\Bigg|_{\delta_{J^+}=0} \in \big(\mathbb{O}_K[\![S]\!]\langle U_{J^+}\rangle/(P_{J^+})\big)^\times = (\mathbb{O}_L[\![T]\!])^\times.$$

In particular, the corresponding matrix is invertible.

Proof. It is enough to prove that the matrix is of full rank modulo (p, T). First, modulo (p, T), the first row will be all zero except the first element which is $\mathfrak{d}(\bar{c}_1, \dots, \bar{c}_m) \in \kappa_l^\times$. Hence, we need only to look at

$$\left(\frac{\partial(\tilde{\pi}^*(P_i)-P_i)}{\partial\delta_j}\right)_{i,j\in J} \bmod (p, T, \delta_{J^+}) = \left(\frac{\partial(\bar{\tilde{\pi}}^*(\bar{\mathfrak{b}}_i)-\bar{\mathfrak{b}}_i)}{\partial\delta_j}\right)_{i,j\in J} \bmod (t, \delta_{J^+}). \quad (4.3.4)$$

Let $\bar{\alpha}_{ij} \in \kappa_l$ denote the entries in the matrix on the right-hand side of (4.3.4), where we identify $\mathbb{O}_k\langle u_{J^+}\rangle/(p_{J^+}, u_0) \xrightarrow{\sim} \kappa_l$. Under this identification, $\bar{\mathfrak{b}}_i$ will become $\bar{c}_i^{p^{r_i}}$ for all $i \in J$. It suffices to show that the i-th row is κ_l-linearly independent from the first $i-1$ rows for all i. Write

$$\bar{\mathfrak{b}}_i = \sum_{e_1=0}^{p^{r_0}-1} \cdots \sum_{e_{i-1}=0}^{p^{r_{i-1}}-1} \bar{\lambda}_{e_1,\dots,e_{i-1}} u_1^{e_1} \cdots u_{i-1}^{e_{i-1}},$$

where $\bar{\lambda}_{e_1,\dots,e_{i-1}} \in \kappa_k$ for which $d\bar{\lambda}_{e_1,\dots,e_{i-1}} = \bar{\mu}_{e_1,\dots,e_{i-1},1} d\bar{b}_1 + \cdots + \bar{\mu}_{e_1,\dots,e_{i-1},m} d\bar{b}_m$. Then, by Lemma 4.3.1, we can write

$$\begin{aligned}\bar{\alpha}_{i1} d\bar{b}_1 + \cdots + \bar{\alpha}_{im} d\bar{b}_m &\\ &= \sum_{e_1=0}^{p^{r_0}-1} \cdots \sum_{e_{i-1}=0}^{p^{r_{i-1}}-1} \bar{c}_1^{e_1} \dots \bar{c}_{i-1}^{e_{i-1}} (\bar{\mu}_{e_1,\dots,e_{i-1},1} d\bar{b}_1 + \cdots + \bar{\mu}_{e_1,\dots,e_{i-1},m} d\bar{b}_m) \\ &\equiv d(\bar{c}_i^{p^{r_i}}) \quad \text{modulo } (d\bar{c}_1, \dots, d\bar{c}_{i-1})\end{aligned}$$

in $\Omega^1_{\boldsymbol{k}_{i-1}/\mathbb{F}_p}$; it is in fact nontrivial because $d\bar{c}_1, \dots, d\bar{c}_m$ form a basis of $\Omega^1_{\kappa_L/\mathbb{F}_p}$ and hence there should not be any auxiliary relation among $d\bar{c}_1, \dots, d\bar{c}_i$ in $\Omega^1_{\boldsymbol{k}_i/\mathbb{F}_p}$. But we know that the sums $\bar{\alpha}_{i'1} d\bar{b}_1 + \cdots + \bar{\alpha}_{i'm} db_m$ for $i' < i$ all lie in the submodule of $\Omega^1_{\boldsymbol{k}_{i-1}/\mathbb{F}_p}$ generated by $d\bar{c}_1, \dots, d\bar{c}_{i-1}$. Hence the i-th row of the matrix in (4.3.4) is $\boldsymbol{k}_{i-1}$-linearly independent from the first $i-1$ rows. The lemma follows. $\square$

Remark 4.3.5. When κ_l/κ_k is modular in the sense of [Sweedler 1968], we can choose the p-basis of κ_k so that $\bar{c}_j^{p^{r_j}} = \bar{b}_j$; in that case, the above lemma is much easier to prove because the matrix, modulo (p, T), is lower triangular with 1 on the diagonal. However, this may not be the case in general; see also Remark 3.3.6.

Theorem 4.3.6. *There exists $\eta'_0 \in (0,1)$ such that for any $a \in \mathbb{Q}_{>1}$ and any $\eta_0 \in (\max\{p^{-1/a}, \eta'_0\}, 1)$, there exists an isomorphism of rigid spaces over $Z_k^{\geq \eta_0}$:*

$$TS_{k\backslash l}^{a,\geq\eta_0} \simeq AS_{l/k}^{a,\geq\eta_0}. \tag{4.3.7}$$

Similarly, There exists $\eta'_0 \in (0,1)$ such that for any $a \in \mathbb{Q}_{>0}$ and any $\eta_0 \in (\max\{p^{-1/a}, \eta'_0\}, 1)$, there exists an isomorphism of rigid spaces over $Z_k^{\geq \eta_0}$:

$$TS_{k\backslash l,\log}^{a,\geq\eta_0} \simeq AS_{l/k,\log}^{a,\geq\eta_0}. \tag{4.3.8}$$

Proof. We give the proof for the case of log-spaces and indicate the changes needed for the nonlog case. The only significant difference between the two is that when constructing the morphism χ_2, we have slightly different approximations. We will match up the ring of functions on the two rigid spaces in (4.3.8) in the log case and (4.3.7) in the nonlog case.

Fix an $\eta_0 \in (p^{-1/a}, 1)$ satisfying Hypothesis 3.3.16.

Recall that $\mathcal{O}_{TS_{k,\log}^{a,\geq\eta_0}} = \mathcal{R}_K^{\eta_0}\langle S^{-a-1}\delta_0, S^{-a}\delta_J\rangle$ (resp. $\mathcal{O}_{TS_k^{a,\geq\eta_0}} = \mathcal{R}_K^{\eta_0}\langle S^{-a}\delta_{J^+}\rangle$). For each $j \in J^+$, $\tilde{\pi}^*(P_j)$ is the polynomial P_j with coefficients replaced by their pull-backs to $\mathcal{O}_{TS_{k,\log}^{a,\geq\eta_0}}$ (resp. $\mathcal{O}_{TS_k^{a,\geq\eta_0}}$) via $\tilde{\pi}^*$. So the rings of functions on $TS_{k\backslash l,\log}^{a,\geq\eta_0}$ and $TS_{k\backslash l}^{a,\geq\eta_0}$ are, respectively,

$$\begin{aligned} \mathcal{R}_{1,\log} &= \mathcal{R}_K^{\eta_0}\langle S^{-a-1}\delta_0, S^{-a}\delta_J\rangle\langle U_{J^+}\rangle/\tilde{\pi}^*(P_{J^+}),\\ \mathcal{R}_1 &= \mathcal{R}_K^{\eta_0}\langle S^{-a}\delta_{J^+}\rangle\langle U_{J^+}\rangle/\tilde{\pi}^*(P_{J^+}). \end{aligned} \tag{4.3.9}$$

By Lemma 3.3.13(1),

$$\begin{aligned} &\tilde{\pi}^*(P_j) \in U_j^{p^{r_j}} - \tilde{\pi}^*(\mathfrak{B}_j) + (p, U_0, S, \delta_0)\cdot \mathcal{O}_K[\![\delta_{J^+}, S]\!][U_{J^+}],\\ &\tilde{\pi}^*(P_0) \in U_0^e - \tilde{\pi}^*(\mathfrak{D})S - \delta_0 + (p, U_0S, S^2, U_0\delta_0, S\delta_0, \delta_0^2)\cdot \mathcal{O}_K[\![\delta_{J^+}, S]\!][U_{J^+}]. \end{aligned}$$

Thus, we can view $\mathcal{R}_{1,\log}$ and $\mathcal{R}_1$ as finite free modules over $\mathcal{O}_{TS_{k,\log}^{a,\geq\eta_0}}$ and $\mathcal{O}_{TS_k^{a,\geq\eta_0}}$, respectively, with basis $\{U_{J^+}^{e_{J^+}} \mid 0 \leq e_0 < e;\ 0 \leq e_j < p^{r_j}, j \in J\}$. For each $\eta \in [\eta_0, 1)$, we norm $\mathcal{R}_{1,\log}$ and $\mathcal{R}_1$ as follows: for $g = \sum \lambda_{e_{J^+}} U_{J^+}^{e_{J^+}}$ with $\lambda_{e_{J^+}} \in \mathcal{O}_{TS_{k,\log}^{a,\geq\eta_0}}$ or $\lambda_{e_{J^+}} \in \mathcal{O}_{TS_k^{a,\geq\eta_0}}$, summed over $e_0 = 0, \dots, e-1$ and $e_j = 0, \dots, p^{r_j}-1$ for $j \in J$, we define

$$|g|_{\mathcal{R}_{1,\log},\eta} = \max_{e_{J^+}}\{|\lambda_{e_{J^+}}|_{TS_{k,\log}^{a,\eta}} \cdot \eta^{e_0/e}\} \quad \text{and} \quad |g|_{\mathcal{R}_1,\eta} = \max_{e_{J^+}}\{|\lambda_{e_{J^+}}|_{TS_k^{a,\eta}} \cdot \eta^{e_0/e}\}.$$

It is clear that $\mathcal{R}_{1,\log}$ and $\mathcal{R}_1$ are the Fréchet completions for the norms $|\cdot|_{\mathcal{R}_{1,\log},\eta}$ and $|\cdot|_{\mathcal{R}_1,\eta}$, for all $\eta \in [\eta_0, 1)$.

On the other hand, by the definition of $AS_{l/k,\log}^{a,\geq\eta_0}$ and $AS_{l/k}^{a,\geq\eta_0}$, their respective rings of functions are

$$\begin{aligned} \mathcal{R}_{2,\log} &= \mathcal{R}_K^{\eta_0}\langle S^{-a-1}V_0, S^{-a}V_J\rangle\langle U_{J^+}\rangle/(P_{J^+} - V_{J^+}),\\ \mathcal{R}_2 &= \mathcal{R}_K^{\eta_0}\langle S^{-a}V_{J^+}\rangle\langle U_{J^+}\rangle/(P_{J^+} - V_{J^+}), \end{aligned}$$

which are clearly finite free modules over $W_{\log} = \mathcal{R}_K^{\eta_0}\langle V_0/\eta^{a+1}, V_J/\eta^a\rangle$ and $W = \mathcal{R}_K^{\eta_0}\langle V_{J^+}/\eta^a\rangle$, respectively, with basis $\{U_{J^+}^{e_{J^+}} \mid 0 \le e_0 < e;\ 0 \le e_j < p^{r_j},\ j \in J\}$.

Similarly, for $\eta \in [\eta_0, 1)$, we norm $\mathcal{R}_{2,\log}$ and $\mathcal{R}_2$ as follows: for $g = \sum \lambda_{e_{J^+}} U_{J^+}^{e_{J^+}}$ with $\lambda_{e_{J^+}} \in W_{\log}$ or $\lambda_{e_{J^+}} \in W$, summed over $e_0 = 0, \ldots, e-1$ and $e_j = 0, \ldots, p^{r_j}-1$ for $j \in J$, we define

$$|g|_{\mathcal{R}_{2,\log},\eta} = \max_{e_{J^+}}\{|\lambda_{e_{J^+}}|_{W_{\log}} \cdot \eta^{e_0/e}\} \quad \text{and} \quad |g|_{\mathcal{R}_2,\eta} = \max_{e_{J^+}}\{|\lambda_{e_{J^+}}|_{W} \cdot \eta^{e_0/e}\}.$$

It is clear that $\mathcal{R}_{2,\log}$ and $\mathcal{R}_2$ are the Fréchet completions for the norms $|\cdot|_{\mathcal{R}_{2,\log},\eta}$ and $|\cdot|_{\mathcal{R}_2,\eta}$, for all $\eta \in [\eta_0, 1)$.

We will identify the U_{J^+} in different rings, but V_{J^+} will not be same as δ_{J^+}. Be cautioned that the two norms will not be the same under the identification; but they will give the same topology.

Now, we define a continuous K-homomorphism $\chi_1 : \mathcal{R}_{2,\log} \to \mathcal{R}_{1,\log}$ (resp. $\chi_1 : \mathcal{R}_2 \to \mathcal{R}_1$) so that $\chi_1(S) = S$, $\chi_1(U_j) = U_j$, $\chi_1(V_j) = P_j(U_{J^+})$ for all $j \in J^+$. We need only to check that for any $\eta \in [\eta_0, 1)$,

$$\begin{aligned} |\chi_1(V_j)|_{\mathcal{R}_{1,\log},\eta} &\le \begin{cases} \eta^{a+1} & \text{if } j = 0, \\ \eta^a & \text{if } j \in J, \end{cases} \\ |\chi_1(V_j)|_{\mathcal{R}_1,\eta} &\le \eta^a \ \text{ for all } j \in J^+. \end{aligned} \tag{4.3.10}$$

Here we need separate arguments for the logarithmic and nonlogarithmic cases. In the former case, inequality (3.2.9) says that

$$|P_j - \tilde{\pi}^*(P_j)|_{\mathcal{R}_{1,\log},\eta} \le \eta^a |P_j|_{\mathcal{R}_{2,\log},\eta}$$

for $j \in J^+$, which gives exactly the bound in (4.3.10) because $|P_0|_{\mathcal{R}_{2,\log},\eta} \le \eta$ and $|P_j|_{\mathcal{R}_{2,\log},\eta} \le 1$ for $j \in J$ by Lemma 3.3.13(1).

In the nonlogarithmic case, combining Lemma 3.3.13(1) and inequality (3.2.10), one has $|P_j - \tilde{\pi}^*(P_j)|_{\mathcal{R}_1,\eta} \le \eta^a$ for $j \in J^+$; inequality (4.3.10) follows.

Conversely, we will define a continuous K-homomorphism $\chi_2 : \mathcal{R}_{1,\log} \to \mathcal{R}_{2,\log}$ or $\chi_2 : \mathcal{R}_1 \to \mathcal{R}_2$ as the inverse to χ_1. Obviously, we need $\chi_2(S) = S$, $\chi_2(U_j) = U_j$ for all $j \in J^+$. The only thing not clear is $\chi_2(\delta_j)$ for all $j \in J^+$.

By Lemma 4.3.3, let

$$\begin{aligned} A := \big(\partial(\tilde{\pi}^*(P_i) - P_i)/\partial\delta_j\big)_{i,j \in J^+}\big|_{\delta_{J^+}=0} &\in \mathrm{GL}_{m+1}(\mathcal{O}_L[\![T]\!]) \\ &\cong \mathrm{GL}_{m+1}\big(\mathcal{O}_K[\![S]\!]\langle U_{J^+}\rangle/P_{J^+}\big). \end{aligned}$$

Let B be the $(m+1) \times (m+1)$ matrix whose entries are in the free $\mathcal{O}_K[\![S]\!]$-module generated by the basis in Lemma 3.3.13(1) and which has image A^{-1} in $M_{m+1}(\mathcal{O}_K[\![S]\!]\langle U_{J^+}\rangle/(P_{J^+}))$. Then, if I denotes the $(m+1) \times (m+1)$ identity matrix, we have

$$BA - I \in \mathrm{Mat}_{m+1}\big((\delta_{J^+}) \cdot \mathcal{O}_K[\![S]\!]\langle U_{J^+}\rangle\big), \tag{4.3.11}$$

Now, we write

$$\begin{pmatrix}\delta_0\\ \vdots\\ \delta_m\end{pmatrix} = (I-BA)\begin{pmatrix}\delta_0\\ \vdots\\ \delta_m\end{pmatrix} - B\left(\begin{pmatrix}\tilde{\pi}^*(P_0)-P_0\\ \vdots\\ \tilde{\pi}^*(P_m)-P_m\end{pmatrix} - A\begin{pmatrix}\delta_0\\ \vdots\\ \delta_m\end{pmatrix}\right) - B\begin{pmatrix}P_0\\ \vdots\\ P_m\end{pmatrix}, \tag{4.3.12}$$

the last term being just $-B\chi_1(V_{J^+})$. We need to bound the first two terms.

By (4.3.11), $I-BA$ has norm $\leq \eta^a$. Hence, in the nonlogarithmic case, the first term in (4.3.12) has norm $\leq \eta^{2a}$; in the logarithmic case the first term in (4.3.12) has norm $\leq \eta^{2a}$, except for the first row, which has norm $\leq \eta^{2a+1}$. By the definition of A and Theorem 3.2.8, the second term in (4.3.12) has norm $\leq \eta^{2a}$ in the nonlogarithmic case; it has norm $\leq \eta^{2a}$ in the logarithmic case, except for the first row, which has norm $\leq \eta^{2a+1}$.

Since we want χ_2 to be the inverse of χ_1, we define recursively

$$\chi_2\begin{pmatrix}\delta_0\\ \vdots\\ \delta_m\end{pmatrix} = -B\begin{pmatrix}V_0\\ \vdots\\ V_m\end{pmatrix} + \chi_2\begin{pmatrix}\Lambda_0\\ \vdots\\ \Lambda_m\end{pmatrix}, \tag{4.3.13}$$

where Λ_{J^+} denotes the sum of the first two terms in (4.3.12). Since Λ_{J^+} has strictly smaller norm than δ_{J^+} and is in the ideal (δ_{J^+}), one can plug the image of $\chi_2(\delta_{J^+})$ back into $\chi_2(\Lambda_{J^+})$ and iterate this substitution. This iteration will converge to the value of $\chi(\delta_{J^+})$ as an element in $\mathcal{R}_{2,\log}$ or $\mathcal{R}_2$. Moreover, from the construction, one can see that

$$|\chi_2(\delta_j)|_{\mathcal{R}_{1,\eta}} \leq \eta^a \qquad \text{for all } \eta \in [\eta_0, 1) \text{ and } j \in J^+,$$

$$\left.\begin{aligned} |\chi_2(\delta_0)|_{\mathcal{R}_{1,\log},\eta} &\leq \eta^{a+1}\\ |\chi_2(\delta_j)|_{\mathcal{R}_{1,\log},\eta} &\leq \eta^a \end{aligned}\right\} \qquad \text{for all } \eta \in [\eta_0, 1) \text{ and } j \in J.$$

Hence, if we define

$$\chi_2 : \mathcal{R}_K^{\eta_0}\langle S^{-a-1}\delta_0, S^{-a}\delta_J\rangle\langle U_{J^+}\rangle \to \mathcal{R}_{2,\log} \quad \text{and} \quad \chi_2 : \mathcal{R}_K^{\eta_0}\langle S^{-a}\delta_{J^+}\rangle\langle U_{J^+}\rangle \to \mathcal{R}_2$$

by $\chi_2(u_{J^+}) = u_{J^+}$, then $\chi_2(\delta_{J^+})$ is the limit we obtained above; this gives a continuous homomorphism. We will check that this homomorphism factors through $\mathcal{R}_{1,\log}$ or $\mathcal{R}_1$. Indeed, by the recursive formula (4.3.13), which is (4.3.12) after applying χ_2, we see that

$$-B\chi_2\begin{pmatrix}\tilde{\pi}^*(P_0)-P_0\\ \vdots\\ \tilde{\pi}^*(P_m)-P_m\end{pmatrix} - B\begin{pmatrix}V_0\\ \vdots\\ V_m\end{pmatrix} = \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}.$$

We know that B has an invertible image in $\mathrm{GL}_{m+1}(\mathcal{O}_K[\![S]\!]\langle U_{J^+}/(P_{J^+})\rangle)$, and so is invertible over $\mathcal{R}_{1,\log}$ or $\mathcal{R}_1$. We must have $0 = \chi_2(\tilde{\pi}^*(P_j) - P_j) + V_j =$

$\chi_2(\tilde{\pi}^*(P_j)) + V_j - P_j = \chi_2(\tilde{\pi}^*(P_j))$ for all $j \in J^+$. This proves that χ_2 factors through $\mathcal{R}_{1,\log}$ or $\mathcal{R}_1$.

Finally, we claim that χ_2 and χ_1 are inverse to each other. One may check this from the definition directly. Alternatively, we observe that, by our definition, they are inverse to one another on a dense subset $K[S, u_{J^+}]$, the polynomial ring inside the Fréchet algebras; therefore, they have to be inverse to one another and give an isomorphism between the ring of functions on Abbes–Saito space and the ring of functions on thickening space. □

Remark 4.3.14. The isomorphisms constructed in Theorem 4.3.6 are canonical in the sense that they match up U_{J^+} on both sides. However, slight perturbations of the isomorphisms will continue to be isomorphic. This point will be important when studying the mixed characteristic case.

4.4. ***Comparison of conductors.*** In this subsection, we will prove the comparison between the arithmetic conductors and the differential conductors. As a reminder, we do not impose Hypotheses 2.3.2 and 3.3.1 in this subsection.

Theorem 4.4.1. *Let k be a complete discretely valued field of equal characteristic $p > 0$ and let G_k be its absolute Galois group. For a p-adic representation $\rho : G_k \to \mathrm{GL}(V_\rho)$ of finite local monodromy, the arithmetic Artin conductor $\mathrm{Art}_{\mathrm{ar}}(\rho)$ of ρ coincides with the differential Artin conductor $\mathrm{Art}_{\mathrm{dif}}(\rho)$; the arithmetic Swan conductor $\mathrm{Swan}_{\mathrm{ar}}(\rho)$ coincides with the differential Swan conductor $\mathrm{Swan}_{\mathrm{dif}}(\rho)$.*

Proof. It suffices to prove this for irreducible representations, as all the conductors are additive. All the conductors remain the same if we pass to the completion of the unramified closure of k, by Proposition 4.1.7(4) and Theorem 2.4.1(2). Thus we may assume that the residue field κ_k is separably closed; hence ρ factors through the Galois group of a finite totally ramified extension l/k as $\rho : G_k \twoheadrightarrow \mathrm{Gal}(l/k) \hookrightarrow \mathrm{GL}(V_\rho)$ with the second map injective. Moreover, we may assume that l/k is wildly ramified because the theorem is known when l/k is tamely ramified, by Proposition 4.1.7(6) and Theorem 2.4.1(3). To sum up, we may assume Hypothesis 3.3.1. In particular, $b_{\mathrm{ar}}(l/k) > 1$ and $b_{ar,\log}(l/k) > 0$.

Next, we want to reduce to the case when the p-basis of k is finite. In view of Construction 3.3.5, one can choose a p-basis of l so that all but a finite number of elements are actually in k. Let $(c_i)_{i\in I}$ be a subset of those elements in the p-basis which lie in k. Set $\tilde{k} = k(c_i^{1/p^n} \mid i \in I, n \in \mathbb{N})^\wedge$ and $\tilde{l} = l\tilde{k}$. We claim that $\mathcal{O}_{\tilde{l}} = \mathcal{O}_l \otimes_{\mathcal{O}_k} \mathcal{O}_{\tilde{k}}$. Indeed, after base change to $\tilde{k}$, the valued groups do not change: $|\tilde{k}^\times| = |k^\times|$. Thus, $[|\tilde{l}^\times| : |\tilde{k}^\times|] \geq [|l^\times| : |k^\times|]$. On the other hand, the residue field extension of $\tilde{l}/\tilde{k}$ has degree at least the same as κ_l/κ_k because $\bar{c}_{J\setminus I}$ are not in the residue field of $\tilde{k}$. But we know that the degree of the extension does not increase. Therefore, we have equality on both naïve ramification degrees and degrees of residue field extension. It is then clear that $\mathbb{O}_{\tilde{l}} = \mathbb{O}_l \otimes_{\mathbb{O}_k} \mathbb{O}_{\tilde{k}}$, as the right-hand side contains the uniformizer of the left-hand side and both sides are isomorphic modulo that uniformizer. Therefore, by Proposition 4.1.7(4), $b_{\mathrm{ar}}(\tilde{l}/\tilde{k}) = b_{\mathrm{ar}}(l/k)$.

On the differential conductors side, [Kedlaya 2007, Lemma 3.5.4] shows for the log case (the nonlog case follows by a similar argument) that we can consider only a finite number of elements in the p-basis and the differential conductors are unchanged after taking an inseparable field extension with respect to other elements in the p-basis.

To sum up, we can make an inseparable extension so that all conductors do not change, and we are reduced to the case where Hypothesis 2.3.2 holds.

Now, we will prove the comparison theorem for the Swan conductors and the proof for the Artin conductors follows verbatim, except replacing Swan by Art, replacing $a > 0$ by $a > 1$, and dropping all the logs in the subscripts.

Since ρ is irreducible, $\mathrm{Swan}_{\mathrm{ar}}(\rho) = b_{ar,\log}(l/k) \cdot \dim V_\rho$. Recall from Section 2.3, we can associate with ρ a differential module $\mathscr{E}_\rho$ over $\mathscr{R}_K^{\eta_0} \otimes_{\mathbb{Q}_q} F$ for some $\eta_0 \in (0, 1)$. As the representation ρ is irreducible, $\mathscr{E}_\rho$ has a unique ramification break $b_{\mathrm{dif},\log}(\mathscr{E}_\rho)$. So the differential Swan conductor of ρ is $\mathrm{Swan}_{\mathrm{dif}}(\rho) = b_{\mathrm{dif},\log}(\mathscr{E}_\rho) \cdot \dim V_\rho$. Therefore, to conclude, it suffices to show that $b_{ar,\log}(l/k) = b_{\mathrm{dif},\log}(\mathscr{E}_\rho)$.

We do this by means of a chain of equivalences. By the equivalence (a) $\Longleftrightarrow$ (d) in Theorem 3.4.12, the inequality $a > b_{\mathrm{dif},\log}(\mathscr{E}_\rho)$ is equivalent to this condition:

For any (or some) extension l'/l with naïve ramification degree e',
$$\pi_0^{\mathrm{geom}}\big(Z_{\bar{l}'}^{\geq \eta_0^{1/ee'}} \times_{Z_l^{\geq \eta_0^{1/e}}} TS_{l/k\backslash l,\log}^{a,\geq \eta_0}\big) = [l:k], \text{ when } \eta_0 \to 1^-. \qquad (*)$$

By Theorem 4.2.4, the condition $(*)$ is equivalent to $\pi_0^{\mathrm{geom}}(as_{l/k,\log}^a) = [l:k]$, where a is a rational number. But this is the same as $a > b_{ar,\log}(l/k)$. ☐

Remark 4.4.2. In an early version of this paper, Theorem 4.4.1 is stated for representations with finite image. Andrea Pulita pointed out that this could be extended to the finite local monodromy case by a standard argument as in the proof.

Corollary 4.4.3. (a) (Hasse–Arf Theorem) *Let k be a complete discretely valued field of equal characteristic $p > 0$, let G_k be its absolute Galois group, and let $\rho : G_k \to \mathrm{GL}(V_\rho)$ be a p-adic representation of finite local monodromy. Then the arithmetic Artin conductor $\mathrm{Art}_{\mathrm{ar}}(\rho)$ and the arithmetic Swan conductor $\mathrm{Swan}_{\mathrm{ar}}(\rho)$ are integers.*

(b) *Let k be a complete discretely valued field of equal characteristic $p > 0$. Then the subquotients $\mathrm{Fil}^a G_k/\mathrm{Fil}^{a+} G_k$ (resp. $\mathrm{Fil}^a_{\log} G_k/\mathrm{Fil}^{a+}_{\log} G_k$) of the arithmetic ramification filtrations are elementary p-abelian groups if $a \in \mathbb{Q}_{>1}$ (resp. $a \in \mathbb{Q}_{>0}$) and are trivial if $a \notin \mathbb{Q}$.*

Proof. This follows from Theorems 2.4.1 and 4.4.1. ☐

5. Applications

In this section, we give two applications of the comparison Theorem 4.4.1. The first is to deduce an integrality result concerning the ramification filtration of finite flat group schemes, introduced in [Abbes and Mokrane 2004]. The other is to compare the arithmetic and differential Artin conductors to the Artin conductor defined by Borger [2004].

Remark 5.0.4. All applications in this section can be carried over to the mixed characteristic case if there is a good theory of differential conductors. For the application to finite flat group schemes, one needs the Hasse–Arf theorem of arithmetic Artin conductors; for the comparison with Borger's Artin conductor, one needs a mixed characteristic version of Proposition 5.4.1. In the absence of these statements, we only focus on the equal characteristic p case throughout this section.

5.1. ***Hasse–Arf theorem for finite flat group schemes.*** We first recall some definitions and basic properties from [Abbes and Mokrane 2004; Hattori 2008]. Then, we use a theorem by Raynaud [Berthelot et al. 1982, théorème 3.1.1] to reduce the integrality result to the case of finite Galois extension of complete discretely valued fields.

Keep the notation as in previous sections. We do not assume any hypothesis on k (and there will be no l in this subsection).

Convention 5.1.1. All finite flat groups schemes are commutative.

The construction of the canonical filtration on a generically étale finite flat group scheme is similar to that of the arithmetic ramification filtration.

Definition 5.1.2. Let A be a finite flat $\mathbb{O}_k$-algebra. Write $A = \mathbb{O}_k[x_1, \dots, x_n]/\mathcal{I}$ with $\mathcal{I}$ an ideal generated by $f_1, \dots, f_r$. For $a \in \mathbb{Q}_{>0}$, define the rigid space

$$X^a = \left\{(x_1, \dots, x_n) \in A^n_K[0, 1] \,\middle|\, |f_\alpha(x_1, \dots, x_n)| \leq \theta^a, \alpha = 1, \dots, r\right\},$$

where $\theta = |s|$ as in Notation 4.1.1. The *highest break* $b(A/\mathbb{O}_k)$ is the smallest number such that $\pi_0^{\mathrm{geom}}(X^a) = \mathrm{rank}_{\mathbb{O}_k} A$ for all $a > b(A/\mathbb{O}_k)$. This is the same as Definition 4.1.3 if $A = \mathbb{O}_l$, except here we use the ring of integers instead of the fields in the notation.

Notation 5.1.3. A finite flat group scheme $G = \operatorname{Spec} A$ is *generically étale* if $G \times_{\mathbb{O}_k} k$ is étale over k; it is *generically trivial* if $G \times_{\mathbb{O}_k} k$ is a disjoint union of copies of $\operatorname{Spec} k$.

Definition 5.1.4. For a geometrically étale finite flat group scheme $G = \operatorname{Spec} A$, we have a natural map of points $G(k^{\mathrm{alg}}) \hookrightarrow X^a(k^{\mathrm{alg}})$; further composing with the map for geometric connected components, we obtain a map

$$\sigma^a : G(k^{\mathrm{alg}}) \hookrightarrow X^a(k^{\mathrm{alg}}) \to \pi_0^{\mathrm{geom}}(X^a).$$

Define G^a to be the closure of $\ker \sigma^a$. We use $b(G/\mathbb{O}_k)$ to denote the highest break $b(A/\mathbb{O}_k)$; then for $a > b(G/\mathbb{O}_k)$, $G^a = \operatorname{Spec} \mathbb{O}_k$.

Proposition 5.1.5 [Abbes and Mokrane 2004, lemme 2.3.2]. *Let*

$$0 \to G' \to G \to G'' \to 0$$

be an exact sequence of finite flat group schemes. For $a > 0$,

$$0 \to G'^a \to G^a \to G''^a \to 0$$

is exact.

Caution 5.1.6. For a subgroup scheme $H \subset G$ and $a \geq 0$, we do not know how to link H^a with $H \times_G G^a$.

The following question was first raised in [Hattori 2008], and the result is essentially due to Hattori. The author thanks him for clarifying this and for permission to include the proof here.

Theorem 5.1.7. *Let $\mathbb{O}_k$ be a complete discrete valuation ring of equal characteristic p. For any generically trivial finite flat groups scheme G over $\mathbb{O}_k$, $b(G/\mathbb{O}_k)$ is a nonnegative integer.*

Proof. We may assume that G is connected by taking the connected component of the identity. By a theorem of Raynaud [Berthelot et al. 1982, théorème 3.1.1], we may realize G as the kernel of an isogeny $f : \mathfrak{B} \to \mathfrak{A}$ of two abelian schemes over $\operatorname{Spec} \mathbb{O}_k$. Let α and β be generic points of the special fibers of $\mathfrak{A}$ and $\mathfrak{B}$, respectively. Then by [Abbes and Mokrane 2004, lemme 2.1.6], $b(\mathbb{O}^\wedge_{\mathfrak{B},\beta}/\mathbb{O}^\wedge_{\mathfrak{A},\alpha}) = b(G/\mathbb{O}_k)$.

Since the generic fiber of G is a disjoint union of copies of $\operatorname{Spec} k$, we know that $\mathbb{O}^\wedge_{\mathfrak{B},\beta}/\mathbb{O}^\wedge_{\mathfrak{A},\alpha}$ is a generically étale finite Galois extension of complete discrete valuation rings, with Galois group $G(k)$; in particular, all irreducible representations of this Galois group over an algebraically closed field are one-dimensional. By Hasse–Arf Theorem 4.4.1, $b(\mathbb{O}^\wedge_{\mathfrak{B},\beta}/\mathbb{O}^\wedge_{\mathfrak{A},\alpha}) = b(G/\mathbb{O}_k)$ is an integer. □

5.2. *Generic p^∞-th roots.* In this subsection, we introduce the notation of generic p^∞-th roots. This idea was first introduced in [Borger 2004] as a key ingredient of Borger's Artin conductor.

Keep the notation as in previous sections. We assume Hypothesis 2.3.2, that k has a finite p-basis b_J.

Notation 5.2.1. Let $x_1, \dots, x_m$ be transcendental over k. Define k' to be the completion of $k(x_1, \dots, x_m)$ with respect to the $(1, \dots, 1)$-Gauss norm. Set $l' = k'l$. Clearly, l' is the completion of $l(x_1, \dots, x_m)$ with respect to the $(1, \dots, 1)$-Gauss norm. We call $x_1, \dots, x_m$ *dummy variables*.

Definition 5.2.2. We use *adding generic p^∞-th roots* to refer to the following procedure. Consider

$$k \hookrightarrow \tilde{k} = k'\big((b_j + x_j s)^{1/p^n};\ j \in J, n \in \mathbb{N}\big)^\wedge,$$

instead of k; namely, put all p-power roots of $b_j + x_j s$ for all $j \in J$ into k' and then take the completion. We provide $\tilde{k}$ with the p-basis x_J, i.e., replacing b_j by x_j for all $j \in J$. For a finite field extension l/k, we replace it by the extension of the composite $\tilde{l} = l\tilde{k}/\tilde{k}$. Note that $\mathrm{Gal}(\tilde{l}/\tilde{k}) = \mathrm{Gal}(l/k)$ as $\tilde{k}$ is linearly independent from l.

The proof of the following proposition is essentially the same as [Kedlaya 2007, Lemma 3.5.4]. It is also implicitly contained in Borger's construction of Artin conductors (Section 5.3).

Proposition 5.2.3. *Let l/k be a finite Galois extension of complete discretely valued fields of equal characteristic p and with finite p-basis. Then, after a finite number of operations of adding generic p^∞-th roots, the field extension has separable residue field extension.*

Proof. First, the tamely ramified part is always preserved under these operations. So, we can assume that l/k is totally wildly ramified and hence the Galois group $G_{l/k}$ is a p-group. We can filter the extension l/k as $k = k_0 \subset \cdots \subset k_n = l$, where k_i/k_{i-1} is a (wildly ramified) $\mathbb{Z}/p\mathbb{Z}$-Galois extension and k_i/k is Galois for each $i = 1, \dots, n$. Each of these subextensions

(a) either has inseparable residue field extension (and so has naïve ramification degree 1), or

(b) has separable residue field extension (and so has naïve ramification degree p).

Let i_0 be the maximal number such that k_i/k_{i-1} has separable residual extension for $i = 1, \dots, i_0$. Obviously adding generic p^∞-th roots does not decrease i_0 because after adding generic p^∞-th roots, the naïve ramification degree of $\tilde{k}_{i_0}/\tilde{k}$ still equals the degree p^{i_0}. It then suffices to show that after a finite number of operations of adding generic p^∞-th roots, k_{i_0+1}/k_{i_0} has separable residue field extension. Suppose the contrary.

Let $g \in G_{k_{i_0+1}/k_{i_0}} \simeq \mathbb{Z}/p\mathbb{Z}$ be a generator. We claim that

$$\gamma = \min_{w \in \mathbb{O}_{k_{i_0+1}}} \big(v_{k_{i_0+1}}(g(w) - w)\big)$$

decreases by at least 1 after adding p^∞-th roots. This would conclude the proposition, as γ is always a nonnegative integer, which would lead to a contradiction.

Let z be a generator of $\mathbb{O}_{k_{i_0+1}}$ as an $\mathbb{O}_{k_{i_0}}$-algebra. It satisfies an equation

$$z^p + a_1 z^{p-1} + \cdots + a_p = 0, \tag{5.2.4}$$

where $a_1, \dots, a_{p-1} \in \mathfrak{m}_{k_{i_0}}$ and $a_p \in \mathbb{O}_{k_{i_0}}^\times$ with $\bar{a}_p \in \kappa_{k_{i_0}}^\times \backslash (\kappa_{k_{i_0}}^\times)^p = \kappa_k^\times \backslash (\kappa_k^\times)^p$. It is easy to see that $\gamma = v_{k_{i_0}}(g(z) - z)$.

Adding generic p^∞-th roots to k gives us the field $\tilde{k}$. Now, the field extension $\tilde{k}k_{i_0+1}/\tilde{k}k_{i_0}$ is also generated by z as above. But we can write $a_p = \alpha^p + \beta$ for $\alpha \in \mathbb{O}_{\tilde{k}k_{i_0}}$ and $\beta \in \mathfrak{m}_{\tilde{k}k_{i_0}}$. Hence if we substitute $z' = z + \alpha$ into (5.2.4), we get $z'^p + a'_1 z'^{p-1} + \cdots + a'_p = 0$, with $a'_1, \dots, a'_p \in \mathfrak{m}_{\tilde{k}k_{i_0}}$. Hence, $v_{\tilde{k}k_{i_0+1}}(z') > 0$. By assumption that the extension $\tilde{k}k_{i_0+1}/\tilde{k}k_{i_0}$ has naïve ramification degree 1, a uniformizer $\pi_{k_{i_0}}$ of k_{i_0} is also a uniformizer for $\tilde{k}k_{i_0+1}$ and hence $z'/\pi_{k_{i_0}}$ lies in $\mathbb{O}_{\tilde{k}k_{i_0+1}}$. Thus,

$$\begin{aligned}\gamma' &= \min_{w \in \mathbb{O}_{\tilde{k}k_{i_0+1}}} \big(v_{\tilde{k}k_{i_0+1}}(g(w) - w)\big)\\ &\leq v_{\tilde{k}k_{i_0+1}}\big(g(z'/\pi_{k_{i_0}}) - z'/\pi_{k_{i_0}}\big) = v_{k_{i_0+1}}(g(z) - z) - 1 = \gamma - 1.\end{aligned}$$

This proves the claim and hence the proposition. □

5.3. ***Borger's Artin conductors.*** We start with reviewing Borger's definition of Artin conductors following [Borger 2004]. Then, we prove the comparison theorem linking this to arithmetic and differential conductors.

Keep the notation as above. Let k be a complete discretely valued field of equal characteristic p, with no further hypothesis added. In fact, Borger's construction works in the mixed characteristic case, but we only focus on the equal characteristic case (see Remark 5.0.4).

Definition 5.3.1. An $\mathbb{F}_p$-algebra R is called *perfect* if $F : x \mapsto x^p$ is an isomorphism. For an $\mathbb{F}_p$-algebra R, we use $R^{\mathrm{pf}} = \bigcup_{n \in \mathbb{N}} R^{1/p^n}$ to denote its *perfection*. Let $\mathtt{CRP}_{\mathbb{O}_k}$ be the subcategory of the category of $\mathbb{O}_k$-algebras consisting of flat $\mathbb{O}_k$-algebras A, complete with respect to the $\mathfrak{m}_k$-adic topology and for which $A/\mathfrak{m}_k A$ is perfect.

Proposition 5.3.2 [Borger 2004, Theorem 1.4]. *This category $\mathtt{CRP}_{\mathbb{O}_k}$ has an initial object $\mathbb{O}_k^u$, the* universal residual perfection *of $\mathbb{O}_k$. We have an equivalence of categories*

$$\mathtt{CRP}_{\mathbb{O}_k} \xrightarrow{\sim} \mathtt{PerfAlg}_{\overline{\mathbb{O}_k^u}}, \quad A \mapsto A/\mathfrak{m}_k A, \tag{5.3.3}$$

where $\mathtt{PerfAlg}_{\overline{\mathbb{O}_k^u}}$ is the category of perfect $\mathbb{O}_k^u/\mathfrak{m}_k\mathbb{O}_k^u$-algebras.

Definition 5.3.4. Let $\mathbb{O}_k^g$ be the inverse image of $\mathrm{Frac}(\mathbb{O}_k^u/\mathfrak{m}_k\mathbb{O}_k^u)$ under (5.3.3), called the *generic residual perfection* of $\mathbb{O}_k$. Let

$$k^g = \mathrm{Frac}(\mathbb{O}_k^g).$$

By Proposition 5.3.2, $\mathbb{O}_k^g$ is a complete discrete valuation ring with perfect residue field.

We have a homomorphism of Galois groups $G_{k^g} \to G_k$. Given a representation ρ of G_k with finite image, we define the *Borger's Artin conductor* $\mathrm{Art}_B(\rho)$ to be $\mathrm{Art}(\rho_{G_{k^g}})$, where the latter term is as in the classical definition [Serre 1979].

Remark 5.3.5. Borger [2004] only defined Artin conductors for representations of finite image. We expect his definition can be extended to representations of finite local monodromy. However, this additional freedom is not essential, so we stick to the finite image case to ease the argument.

Obviously, Borger's Artin conductors have a Hasse–Arf property naturally inherited from that of k^g, a complete discretely valued field with perfect residue field.

Proposition 5.3.6 [Borger 2004, Theorem A]. *Borger's Artin conductor* $\mathrm{Art}_B(\rho)$ *is a nonnegative integer and it coincides with the classical definition when the residue field κ_k is perfect.*

[Borger 2004, Proposition 2.3] *Furthermore*, $\mathrm{Art}_B(\rho)$ *is unchanged after a finite unramified extension of k.*

Moreover, Borger proved that his definition coincides with a variant of arithmetic Artin conductor Art_K for characters using the definition of Kato [1989]. (As we will not use Kato's definition, we just mention the following proposition as a fact.)

Proposition 5.3.7 [Borger 2004, Theorem B]. *Let χ be a class in $H^1(G_k, \mathbb{Q}/\mathbb{Z})$ and χ' its image in $H^1(G_{k^g}, \mathbb{Q}/\mathbb{Z})$. Then* $\mathrm{Art}_K(\chi) = \mathrm{Art}_K(\chi')$. *In particular, for a rank-one representation ρ of G_k with finite image*, $\mathrm{Art}_K(\rho) = \mathrm{Art}_B(\rho)$.

Borger gave the following explicit descriptions of k^u and k^g.

Proposition 5.3.8. *We have $k^u = (\kappa_k[v_{i,j} \mid j \in J, i \in \mathbb{N}])^{\mathrm{pf}}((\pi_{k^u}))$. The homomorphism $k \hookrightarrow k^u$ is determined by $s \mapsto \pi_{k^u}$ and $b_j \mapsto b_j + \sum_{i>0} v_{i,j}\pi_{k^u}^i$. Also, $k^g = \mathrm{Frac}(\kappa_k[v_{i,j};\, j \in J, i \in \mathbb{N}]^{\mathrm{pf}})((\pi_{k^u}))$ and the homomorphism $k \to k^g$ is given by composing $k \hookrightarrow k^u$ with the natural morphism $k^u \hookrightarrow k^g$.*

5.4. ***Comparison with Borger's conductors.*** The key to proving the comparison between Borger's Artin conductors and the arithmetic Artin conductors is to study how the arithmetic Artin conductors behave under the operations of adding generic p^∞-th roots.

In this subsection, we do not impose any hypothesis on k.

Proposition 5.4.1. *Assume Hypothesis 2.3.2. For representations of finite image, the differential Artin conductor for a representation of finite image is unchanged after adding generic p^∞-th roots.*

Proof. Since the operation of adding p^∞-th roots does not change the Galois group of the finite Galois extension, we may assume that the representation is irreducible and totally and wildly ramified. Hence it suffices to consider the differential ramification break of a totally and wildly ramified finite Galois extension l/k.

Recall that we have a differential module $\mathscr{E}$ over $Z_k^{\geq\eta_0} = A_K^1[\eta_0, 1)$ for some $\eta_0 \in (0, 1)$ with differential operators ∂_{B_J} and ∂_S, associated with the regular representation of $\mathrm{Gal}(l/k)$ over $\mathbb{Q}_p$. The base change $k \hookrightarrow k' = k(x_J)^\wedge$ is translated into the base change of $\mathscr{E}$ into $\mathscr{E}'$, from $Z_k^{\geq\eta_0}$ to $Z_{k'}^{\geq\eta_0} = A^1_{K(X_J)^\wedge}[\eta_0, 1)$, where $K' = K(X_J)^\wedge$ is the completion of $K(X_J)$ with respect to the $(1, \dots, 1)$-Gauss norm; $\mathscr{E}'$ has differential operators ∂_{B_J}, ∂_{X_J}, and ∂_S.

Consider the rotation $f : Z_{k'}^{\geq\eta_0} \to Z_{k'}^{\geq\eta_0}$ by $f^*(B_J) = B_J + X_J S$, $f^*(X_J) = X_J$, and $f^*(S) = S$; write ∂'_{B_J}, ∂'_{X_J}, and ∂'_S for the action of differential operators on $f^*\mathscr{E}'$. Then

$$\partial'_{B_J} = \partial_{B_J}, \qquad \partial'_{X_J} = S \cdot \partial_{B_J} + \partial_{X_J}, \qquad \partial'_S = \sum_{j\in J} X_j \cdot \partial_{B_j} + \partial_S.$$

Since X_J are transcendental over K, we have

$$\begin{aligned}\max\{|\partial_{B_J}|_{\mathscr{E}_\eta,\mathrm{sp}}, |\partial_S|_{\mathscr{E}_\eta,\mathrm{sp}}, |\partial_{X_J}|_{\mathscr{E}_\eta,\mathrm{sp}}\} &= |\partial'_S|_{\mathscr{E}'_\eta,\mathrm{sp}} \\ &= \max\{|\partial'_{X_J}|_{\mathscr{E}'_\eta,\mathrm{sp}}, |\partial'_S|_{\mathscr{E}'_\eta,\mathrm{sp}}\} \qquad (5.4.2)\end{aligned}$$

for all $\eta \in [\eta_0, 1)$. Note that adding generic p^∞-th roots to k corresponds exactly to replacing $\mathscr{E}$ by $f^*\mathscr{E}'$ and *forgetting* the differential operators B_J. By (5.4.2), the differential nonlogarithmic ramification break of $\tilde{l}/\tilde{k}$ is the same as that of l/k. □

Theorem 5.4.3. *For a complete discretely valued field k of equal characteristic p and a representation ρ of its Galois group G_k with finite image, the arithmetic Artin conductors* $\mathrm{Art}_{\mathrm{ar}}(\rho)$ *as well as the differential Artin conductors* $\mathrm{Art}_{\mathrm{dif}}(\rho)$ *are the same as Borger's Artin conductors* $\mathrm{Art}_B(\rho)$.

Proof. First we may assume that ρ is irreducible and it factors exactly through the Galois group $G_{l/k}$ of a totally ramified Galois extension l/k because all conductors are additive and remain the same under a (finite) unramified extension (Theorem 2.4.1(c) and Propositions 4.1.7(d) and 5.3.6). As k^g has a perfect residue field, $\mathrm{Art}_B(\rho) = \mathrm{Art}_B(\rho|_{G_{k^g}}) = \mathrm{Art}_{\mathrm{dif}}(\rho|_{G_{k^g}})$ are the same as in the classical definition. It suffices to show $\mathrm{Art}_{\mathrm{dif}}(\rho) = \mathrm{Art}_{\mathrm{dif}}(\rho|_{G_{k^g}})$.

Similarly to the proof of Theorem 4.4.1, one may add the p^∞-th roots of all but a finite number of elements of the p-basis into k without changing the differential Artin conductors. In other words, there exists $k \hookrightarrow k_1 = k(b_j^{p^{-n}} \mid j \in J \backslash J_0, n \in \mathbb{N})^\wedge$ for some finite set $J_0 \subset J$, such that $\mathrm{Art}_{\mathrm{dif}}(\rho) = \mathrm{Art}_{\mathrm{dif}}(\rho|_{\mathrm{Gal}_{k_1}})$. Since the residue field of k^g is perfect, there exists $k_1 \hookrightarrow k^g$ extending $k \hookrightarrow k^g$. Hence, we may assume Hypothesis 2.3.2, i.e., k has a finite p-basis.

By Proposition 5.2.3, we can do a finite number of operations of adding generic p^∞-th roots and make the resulting field extension k_2l/k_2 not fiercely ramified and $\mathrm{Art}_{\mathrm{dif}}(\rho|_{G_{k_1}}) = \mathrm{Art}_{\mathrm{dif}}(\rho|_{G_{k_2}})$. In order to link k_2 with k^g, we need to show that we have a homomorphism $k_2 \hookrightarrow k^g$ extending $k_1 \hookrightarrow k^g$, for which we return to the proof of Proposition 5.2.3 and construct the homomorphism step by step.

The r-th ($1 \leq r \leq r_0$) step of adding generic p^∞-th roots is to construct

$$k_1^{(r)} = \Big(k_1^{(r-1)}(x_{r,J})\big((x_{r-1,j} + x_{r,j}\pi_k)^{1/p^n};\ j \in J, n \in \mathbb{N}\big)\Big)^\wedge,$$

where $x_{0,j} = b_j$ for $j \in J$ and $k_1^{(0)} = k_1$. One checks that the map given by

$$x_{r,j} \mapsto \sum_{r' \geq r} v_{r',j}\pi_{k^g}^{r'-r}$$

for all $j \in J$ and $r = 1, \ldots, r_0$, gives the desired homomorphism $k_2 \hookrightarrow k^g$.

Now, k_2l/k_2 has naïve ramification degree $[k_2l : k_2]$, so $\mathbb{O}_{k^gl} = \mathbb{O}_{k^g} \otimes_{\mathbb{O}_{k_2}} \mathbb{O}_{k_2l}$. Hence we have

$$\mathrm{Art}_{\mathrm{dif}}(\rho|_{G_{k_2}}) = \mathrm{Art}_{\mathrm{ar}}(\rho|_{G_{k_2}}) = \mathrm{Art}_{\mathrm{ar}}(\rho|_{G_{k^g}}) = \mathrm{Art}_{\mathrm{dif}}(\rho|_{G_{k^g}})$$

via Theorem 4.4.1 and Proposition 4.1.7(d). □

Acknowledgments. Many thanks are due to my advisor, Kiran Kedlaya, for introducing me to the problem, for generating ideas, for constantly encouraging and supporting, and for spending many hours reviewing early drafts. He also helped me fix a gap in an early version of this paper by providing the argument in Section 1.

The author owes many thanks to the referee of this paper; this paper was greatly improved in presentation by his or her invaluable suggestions.

Thanks to Ahmed Abbes and Takeshi Saito for organizing the great conference on vanishing cycles; it provided us with a great opportunity to learn about this field.

Thanks to Christopher Davis for helping me review early drafts, correct the grammar, and smooth the argument. Thanks to Shin Hattori for helping me clarify Section 5.1. Thanks to Shun Ohkubo for pointing out two errors in an early version of this paper and their link to the work of Sweedler. Thanks to Brian Conrad for continuous encouragement and support. Thanks also to Michael Artin, Johan de Jong, Ivan Fesenko, Xuhua He, Ruochuan Liu, Christian Kappen, Andrea Pulita, Yichao Tian, and Wei Zhang for interesting discussions and helping review early drafts.

Financial support was provided by the MIT Department of Mathematics. While writing the paper, the author enjoyed a research assistantship funded by Kedlaya's NSF CAREER grant DMS-0545904.

References

[Abbes and Mokrane 2004] A. Abbes and A. Mokrane, "Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes", *Publ. Math. Inst. Hautes Études Sci.* 99 (2004), 117–162. MR 2005f:14090 Zbl 1062.14057

[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

[Abbes and Saito 2009] A. Abbes and T. Saito, "Analyse micro-locale l-adique en caractéristique $p > 0$: Le cas d'un trait", *Publ. Res. Inst. Math. Sci.* **45**:1 (2009), 25–74. MR 2009m:11197 Zbl 05551347

[Berkovich 1990] V. G. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Math. Surveys and Monographs **33**, Amer. Math. Soc., Providence, RI, 1990. MR 91k:32038 Zbl 0715.14013

[Berthelot 1996] P. Berthelot, "Cohomologie rigide et cohomologie rigide à support propre", preprint, IRMAR Université de Rennes, 1996, Available at http://tinyurl.com/2fr9nsm.

[Berthelot et al. 1982] P. Berthelot, L. Breen, and W. Messing, *Théorie de Dieudonné cristalline, II*, Lecture Notes in Math. **930**, Springer, Berlin, 1982. MR 85k:14023 Zbl 0516.14015

[Borger 2004] J. M. Borger, "Conductors and the moduli of residual perfection", *Math. Ann.* **329**:1 (2004), 1–30. MR 2005c:11146 Zbl 1096.11040

[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

[Chiarellotto and Pulita 2009] B. Chiarellotto and A. Pulita, "Arithmetic and differential Swan conductors of rank one representations with finite local monodromy", *Amer. J. Math.* **131**:6 (2009), 1743–1794. MR 2567506 Zbl 05656521

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: With a view toward algebraic geometry*, Graduate Texts in Math. **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001

[Grothendieck 1964] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, I", *Inst. Hautes Études Sci. Publ. Math.* 20 (1964), 259. MR 30 #3885

[Hattori 2008] S. Hattori, "Tame characters and ramification of finite flat group schemes", *J. Number Theory* **128**:5 (2008), 1091–1108. MR 2009a:14060 Zbl 05268132

[Kato 1989] K. Kato, "Swan conductors for characters of degree one in the imperfect residue field case", pp. 101–131 in *Algebraic K-theory and algebraic number theory* (Honolulu, 1987), edited by M. R. Stein and R. K. Dennis, Contemp. Math. **83**, Amer. Math. Soc., Providence, RI, 1989. MR 90g:11164 Zbl 0716.12006

[Kedlaya 2005] K. S. Kedlaya, "Local monodromy of p-adic differential equations: An overview", *Int. J. Number Theory* **1**:1 (2005), 109–154. MR 2006g:12013 Zbl 1107.12005

[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, New York, 2010. Zbl 05765055

[Matsuda 2002] S. Matsuda, "Katz correspondence for quasi-unipotent overconvergent isocrystals", *Compositio Math.* **134**:1 (2002), 1–34. MR 2003j:12007 Zbl 1101.14021

[Matsuda 2004] S. Matsuda, “Conjecture on Abbes–Saito filtration and Christol–Mebkhout filtration”, pp. 845–856 in *Geometric aspects of Dwork theory*, vol. 2, edited by A. Adolphson et al., de Gruyter, Berlin, 2004. MR 2005g:11233 Zbl 1174.11406

[Saito 2009] T. Saito, “Wild ramification and the characteristic cycle of an l-adic sheaf”, *J. Inst. Math. Jussieu* **8**:4 (2009), 769–829. MR 2540880 Zbl 1177.14044

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. MR 82e:12016 Zbl 0423.12016

[Sweedler 1968] M. E. Sweedler, “Structure of inseparable extensions”, *Ann. of Math.* (2) **87** (1968), 401–410. MR 36 #6391 Zbl 0168.29203

[Tsuzuki 2002] N. Tsuzuki, “Morphisms of F-isocrystals and the finite monodromy theorem for unit-root F-isocrystals”, *Duke Math. J.* **111**:3 (2002), 385–418. MR 2003b:14026 Zbl 1055.14022

[Whitney 2002] W. A. Whitney, *Functorial Cohen rings*, Ph.D. thesis, University of California, Berkeley, 2002, Available at http://tinyurl.com/2ugguq6. MR 2707613

Communicated by Brian Conrad
Received 2009-05-14 Revised 2010-05-25 Accepted 2010-06-22

lxiao@math.uchicago.edu University of Chicago, 321 Eckhart Hall,
5734 S University Avenue, Chicago, IL 60637, United States

ALGEBRA AND NUMBER THEORY 4:8(2010)

Exponential generation and largeness for compact p-adic Lie groups

Michael Larsen

Given a fixed integer n, we consider closed subgroups $\mathcal{G}$ of $\mathrm{GL}_n(\mathbb{Z}_p)$, where p is sufficiently large in terms of n. Assuming that the identity component of the Zariski closure G of $\mathcal{G}$ in $\mathrm{GL}_{n,\mathbb{Q}_p}$ does not admit any nontrivial torus as quotient group, we give a condition on the (mod p) reduction of $\mathcal{G}$ which guarantees that $\mathcal{G}$ is of bounded index in $\mathrm{GL}_n(\mathbb{Z}_p) \cap G(\mathbb{Q}_p)$.

Nori [1987] considered a special class of subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$, namely groups which are generated by elements of order p or, as we shall say, *p-generated groups*. He showed that if p is sufficiently large in terms of n, there is a correspondence between p-generated groups and a certain class of connected algebraic groups which he called *exponentially generated*. In particular, every p-generated group Γ is a subgroup of $G(\mathbb{F}_p)$ for the corresponding algebraic group G, and $[G(\mathbb{F}_p) : \Gamma]$ is bounded by a constant depending only on n. The p-generated groups are admittedly rather special, but on the other hand, every finite subgroup $\Gamma \subset \mathrm{GL}_n(\mathbb{F}_p)$ contains a p-generated normal subgroup, Γ^+, of prime-to-p index, which shows that every Γ can be related to a connected algebraic group in a weak sense. This construction can serve in some measure as a substitute for the (identity component of the) Zariski closure in the setting of finite linear groups, where the actual identity component of the Zariski closure of Γ is always trivial.

In this paper we consider closed subgroups $\mathcal{G}$ of the compact p-adic Lie group $\mathrm{GL}_n(\mathbb{Z}_p)$. In this setting, of course, Zariski closure behaves well, so we do not need a substitute. Nevertheless, it turns out that there is an interesting class of groups $\mathcal{G}$ for which we can prove a bounded index result analogous to that of Nori: see Theorem 7. We intend to give an application of this result to geometric monodromy of nonsingular projective varieties over function fields in finite characteristic.

Throughout the paper, n will denote a positive integer and F a field. If F is of characteristic $p > 0$, we assume $p \geq n$, so $i!$ is nonzero for $i < n$. As every

The author was partially supported by NSF grants DMS-0354772 and DMS-0800705.

MSC2000: primary 20G25; secondary 20G40.

Keywords: exponentially generated, Nori's theorem, p-adic Lie group.

nilpotent element $x \in M_n(F)$ satisfies $x^n = 0$, the truncated exponential function

$$\exp(x) := \sum_{i=0}^{n-1} \frac{x^i}{i!}$$

satisfies $\exp(x+y) = \exp(x)\exp(y)$ for every pair x, y of commuting nilpotent matrices. Moreover $\exp(x) - 1$ is nilpotent, so $\exp(x)$ is unipotent. Conversely, if u is unipotent, $1 - u$ is nilpotent, so

$$\log(u) := -\sum_{i=1}^{n-1} \frac{(1-u)^i}{i}$$

is nilpotent, and log and exp set up mutually inverse bijections between the unipotent and nilpotent $n \times n$ matrices over F. In the positive characteristic case, every unipotent element $u \neq 1$ is of order p, and conversely, every element of order p is unipotent (because this is true for every Jordan block of order $\leq p$).

For every nilpotent element $x \in M_n(F)$, there exists a morphism of algebraic groups $\phi_x : \mathbb{A}^1 \to \mathrm{GL}_n$ defined by

$$\phi_x(t) := \exp(tx).$$

If $x \neq 0$, this morphism is injective, and its image is isomorphic to $\mathbb{A}^1$. If N is a set of nilpotent elements of $M_n(F)$, let G_N denote the subgroup of GL_n generated by $\phi_x(\mathbb{A}^1)$ for all $x \in N$, i.e., the intersection of all algebraic subgroups of GL_n which contain

$$\bigcup_{x \in N} \phi_x(\mathbb{A}^1).$$

Following Nori we say that an algebraic subgroup of GL_n over a field F is *exponentially generated* if it is of the form G_N for some $N \subset M_n(F)$.

Proposition 1. *Over a perfect field, every exponentially generated group is the extension of a semisimple group by a unipotent group.*

Proof. It is clear that every quotient group of an exponentially generated group G must be generated by subgroups isomorphic to the additive group. In particular exponentially generated groups must be connected, and every reductive exponentially generated group must be semisimple since no nontrivial torus is generated by additive groups. As long as F is perfect, the (geometric) unipotent radical N is actually defined over F, so G is an extension of the semisimple group G/N by the unipotent group N. □

In general, the converse of Proposition 1 is not true. For example, if $F = \mathbb{R}$, GL_n contains F-anisotropic connected semisimple subgroups which have no nontrivial unipotent elements. If F is of positive characteristic, even if it is algebraically closed, the image of SL_2 under the 4-dimensional representation which is the direct sum of the standard representation and its Frobenius twist fails to be exponentially generated. In characteristic zero, we have a precise criterion for exponential generation.

Proposition 2. *Let F be a field of characteristic zero. An algebraic subgroup G of GL_n defined over F is exponentially generated if and only if it has no nontrivial finite, toric, or anisotropic quotient group.*

Proof. As there is no nontrivial homomorphism from an additive group to a finite, toric, or anisotropic group, one direction is clear. For the other, let U denote a unipotent F-subgroup of G. Thus U has a composition series

$$U = U_0 \supset U_1 \supset \cdots \supset U_s = \{e\},$$

with each U_i/U_{i+1} isomorphic to the additive group. By Steinberg's theorem [1965], $H^1(F, U_i) = 0$ for all i, so for each $1 \le i \le s$ we have a short exact sequence

$$0 \to U_i(F) \to U_{i-1}(F) \to F \to 0,$$

and there exists $u_{i-1} \in U_{i-1}(F) \setminus U_i(F)$. As F is of characteristic zero,

$$\langle u_i \rangle \subset U_{i-1}(F) \cap \phi_{\log(u_i)}(F)$$

is isomorphic to $\mathbb{Z}$, so $\phi_{\log(u_i)}(\mathbb{A}^1) \cap U_{i-1}$ has dimension 1, which means $\phi_{\log(u_i)}(\mathbb{A}^1) \subset U_{i-1}$. It follows that

$$\phi_{\log(u_i)}(\mathbb{A}^1) U_i = U_{i-1}.$$

Thus, by descending induction,

$$U = \prod_{i=1}^{s} \phi_{\log(u_{i-1})}(\mathbb{A}^1).$$

Let H denote the quotient of $G = G^\circ$ by its unipotent radical N. As H is isotropic, the set $\mathcal{P}$ of its proper parabolic F-subgroups is nonempty. For each $P \in \mathcal{P}$, let U_P denote the inverse image in G of the unipotent radical of P. Thus each U_P is a unipotent F-subgroup of G containing N. Each is therefore exponentially generated. Let $K \subset G$ be the (exponentially generated group) generated by all U_P. Thus K is normalized by the inverse image of $H(F)$ in G. By a theorem of [Chevalley 1954], $H(F)$ is Zariski-dense in H, so K is normal in G. Thus G/K is isomorphic to a quotient $H/(K/N)$, which is isotropic. It follows that $\mathcal{P}$ contains a proper parabolic F-subgroup not contained in K/N, contrary to assumption. Thus $K = G$, and G is exponentially generated. $\square$

We say that a Lie algebra is *nilpotently generated* if it is spanned by its nilpotent elements. By [Nori 1987, Theorem A], if F is of characteristic zero or characteristic p sufficiently large in terms of n, the log and exp maps give mutually inverse bijections, described more explicitly below, between exponentially generated F-subgroups of GL_n and nilpotently generated F-subalgebras of the Lie algebra $M_n = \mathfrak{gl}_n$.

The following proposition allows us to put all exponentially generated subgroups (as well, possibly, as other subvarieties of GL_n) into a family over a base of finite type. It is convenient to work projectively, by embedding GL_n into $\mathbb{P}^{n^2}$. For any scheme Z and any closed subvariety K of $\mathrm{GL}_{n,Z}$, we denote by $\bar{K}$ the closed subset $Z \cup (\mathbb{P}^{n^2}_Z \setminus \mathrm{GL}_{n,Z})$ endowed with its reduced induced scheme structure.

Proposition 3. *For every positive integer n there exists an integer N and a finite set S of polynomials such that for every field F over $\mathbb{Z}[1/N]$ and every exponentially generated subgroup $G_F \subset \mathrm{GL}_{n,F}$, the Hilbert polynomial of $\bar{G}_F$ belongs to S.*

Proof. We prove that there exists a positive integer N and a morphism $Y' \to X'$ of schemes of finite type over $\mathbb{Z}$ such that for all F whose characteristic does not divide N and all exponentially generated $G_F \subset \mathrm{GL}_{n,F}$, there exists $x' \in X'(F)$ with $Y'_{x'} = \bar{G}_F$. By [Grothendieck 1961, §2], the set of Hilbert polynomials for the $\bar{G}_F$ is therefore finite.

We begin by trying to parametrize nilpotently generated Lie algebras. The set of k-tuples of nilpotent $n \times n$ matrices which span a Lie subalgebra of $n \times n$ matrices is constructible because Lie algebra closure can be expressed as the existence of a set of k^3 structure constants for the Lie bracket. Let $N_n/\mathbb{Z}$ denote the scheme of nilpotent $n \times n$ matrices and $W \subset N_n^{n^2}$ the constructible set of ordered n^2-tuples of nilpotent matrices spanning a Lie algebra. Replacing W with the disjoint union X of the strata of a suitable stratification, we get a scheme indexing n^2-tuples of nilpotent matrices which span nilpotent Lie algebras. Thus, for every field F of characteristic zero or characteristic p sufficiently large and every nilpotently generated Lie algebra $L \subset \mathfrak{gl}_n$ over F, there exists $x \in X(F)$ which indexes a spanning set of L.

We choose N sufficiently divisible that outside of characteristics dividing N, there is a bijection between exponentially generated subgroups G of GL_n and nilpotently generated Lie subalgebras L of $\mathfrak{gl}_n$, given by the mutually inverse maps sending G to its Lie algebra and L to the group generated by $\phi_x(\mathbb{A}^1)$ for all nilpotent $x \in L$. In particular, $\phi_{x_i}(\mathbb{A}^1)$ generates G whenever $x_1, \ldots, x_{n^2}$ is a nilpotent spanning set of L. From the scheme X indexing all possible n^2-tuples, we would like to obtain a scheme of finite type over $\mathbb{Z}[1/N]$ indexing all $\bar{G}_F$, where G_F ranges over exponentially generated groups and F ranges over fields over $\mathbb{Z}[1/N]$.

Recall (from [Borel 1991, Proposition 2.2], for example) that if $V \subset G \subset \mathrm{GL}_n$ is any connected generating subvariety of an algebraic group G, the image of V^{n^2} under the multiplication map is dense in G, and the image of V^{2n^2} is exactly G. This implies

$$\bigl(\phi_{x_1}(\mathbb{A}^1)\dots\phi_{x_{n^2}}(\mathbb{A}^1)\bigr)^{2n^2} \twoheadrightarrow G.$$

Let $Y := \mathbb{P}^{n^2}_X$ and

$$Z := (\mathbb{P}^{n^2}_X \setminus \mathrm{GL}_{n,X}) \coprod (X \times \mathbb{A}^{2n^4}).$$

We define $\xi\colon Z \to Y$ by extending the obvious inclusion map on the first component of Z by

$$\xi\bigl((x_1,\dots,x_{n^2}),(t_{1,1},\dots,t_{n^2,2n^2})\bigr) := \Bigl((x_1,\dots,x_{n^2}), \prod_{j=1}^{2n^2}\prod_{i=1}^{n^2}\phi_{x_i}(t_{i,j})\Bigr).$$

For each F and each $x \in X(F)$, the image of the map of fibers $Z_x \to Y_x = \mathbb{P}^{n^2}_F$ is the union of $\mathbb{P}^{n^2}_F \setminus \mathrm{GL}_{n,F}$ and the exponential subgroup of $\mathrm{GL}_{n,F}$ in correspondence with the nilpotently generated Lie subalgebra of $\mathfrak{gl}_n(F)$ associated to x. The following lemma now implies the proposition. $\square$

Lemma 4. *Let m be a positive integer, X a scheme of finite type over $\mathbb{Z}$, Y a closed subscheme of $\mathbb{P}^m_X$, and $\xi\colon Z \to Y$ a morphism of finite type such that $\xi(Z_x)$ is a closed subset of Y_x for all $x \in X$. There exists $N \in \mathbb{N}$, a morphism $\psi\colon X' \to X$, and a closed subscheme $Y' \subset \mathbb{P}^m_{X'}$ such that for every field F over $\mathbb{Z}[1/N]$ and every $x \in X(F)$, there exists $x' \in X'_x(F)$ such that $Y'_{x'} = \xi(Z_x)^{\mathrm{red}}$.*

Proof. We use Noetherian induction on X. If the image of $Z \to X$ has Zariski closure $C \subsetneq X$, we can replace X and Y by C and Y_C respectively. We therefore assume without loss of generality that $Z \to X$ has dense image. Replacing Z by Z^{red}, without loss of generality we may assume Z is reduced. We choose N divisible by every prime which is the characteristic of a generic point of X.

Let η denote a generic point of X. As any localization of a reduced ring is reduced, Z_η is reduced. Either η lies over a prime p dividing N or η is of characteristic zero. In the former case, let U_1 denote any neighborhood of η which lies over $\operatorname{Spec}\mathbb{F}_p$. In the latter case, Z_η is geometrically reduced [Grothendieck 1965, Proposition 4.6.1 on p. 68], so Z_x is geometrically reduced for all x in some neighborhood U_1 of η [Grothendieck 1966, Theorem 9.7.7(iii) on p. 79]. Let W denote the Zariski closure of $\overline{\xi(Z)} \setminus \xi(Z)$ in Y, endowed with its reduced induced scheme structure. As $\xi(Z_\eta)$ is closed in Y_η, the η-fibers of $\xi(Z)$ and $\overline{\xi(Z)}$ are the same, so W_η is empty. Let U_2 denote a neighborhood of η which does not meet the image of $W \to X$. Finally, let $U = U_1 \cap U_2$, $X_1 = X \setminus U$, $Y_1 = Y \times_X X_1$, and $Z_1 = Z \times_X X_1$.

By the induction hypothesis, if N is sufficiently divisible, the lemma holds for X_1, Y_1, and Z_1. Let X_1', Y_1', and ψ_1 be chosen suitably. Let $X' = U \coprod X_1'$ and $Y' = W_U \coprod Y_1'$, and let ψ denote the extension of ψ_1 which is given on W_U by the composition of the obvious maps $W_U \to Y \to \mathbb{P}^m_X \to X$. If $x \in X(F)$ belongs to $X_1(F)$, we are done already. If not, it belongs to $U(F)$. Let x' denote the image of $x \in U(F)$ under the inclusion $U \to X'$. As $U \subset U_2$, at the set level, the fiber $Y'_{x'}$ coincides with $\xi(Z_x)$. As $U \subset U_1$, if F is a $\mathbb{Z}[1/N]$-algebra, then $Y'_{x'}$ is reduced. $\square$

We now specialize to the case $F = \mathbb{F}_p$, where $p \geq n$. If Γ is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, we write Γ^+ for the subgroup of Γ generated by all elements of order p. Let $N(\Gamma) = N(\Gamma^+)$ denote the set $\{\log u \mid u^p = 1, u \in \Gamma\}$, and let $G := G_{N(\Gamma)}$. Then $\Gamma^+ \subset G(\mathbb{F}_p)$.

Definition 5. If Γ is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ we define the *Nori dimension*, $\mathrm{Ndim}\,\Gamma$, to be $\dim G_{N(\Gamma)}$. Likewise if $\mathcal{G}$ is a subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ its Nori dimension, $\mathrm{Ndim}\,\mathcal{G}$, is the Nori dimension of its reduction (mod p).

Lemma 6. *Let $p \geq 2n$, let x be a nilpotent $n \times n$ matrix over $\mathbb{F}_p$, and let $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ be a p-adic lift of* $\exp(x)$. *For all positive integers k,*

$$A^{p^k} \equiv 1 + p^k M \pmod{p^{k+1}},$$

where M reduces (mod p) *to x.*

Proof. It suffices to prove the lemma when $k = 1$. Without loss of generality, we may assume that M is nilpotent, so $M^p = 0$. Let $N = \exp(M) - 1$. As N reduces (mod p) to the nilpotent element $\exp(x) - 1$, N^n is divisible by p in $M_n(\mathbb{Z}_p)$, and we can write A as $1 + N + pB$ for some $B \in M_n(\mathbb{Z}_p)$. Expanding,

$$\begin{aligned} A^p = (1 + N + pB)^p &= \sum_{m=0}^{p} \binom{p}{m} (N + pB)^m \\ &\equiv \sum_{m=0}^{p} \binom{p}{m} \Bigl(N^m + p \sum_{i+j=m-1} N^i B N^j \Bigr) \\ &\equiv \sum_{m=0}^{p} \binom{p}{m} N^m = (1+N)^p = \exp(pM) \equiv 1 + pM \pmod{p^2}. \qquad \square \end{aligned}$$

Theorem 7. *For every positive integer n there exist constants A_n, B_n, and C_n such that if $p > A_n$ is prime, $\mathcal{G}$ is a closed subgroup of* $\mathrm{GL}_n(\mathbb{Z}_p)$, *and G is the Zariski closure of $\mathcal{G}$ in* $\mathrm{GL}_{n,\mathbb{Q}_p}$, *then* $\mathrm{Ndim}\,\mathcal{G} \leq \dim G$. *If* $\mathrm{Ndim}\,\mathcal{G} = \dim G$, *then*:

(1) *$\mathcal{G}$ is an open subgroup of $G(\mathbb{Q}_p)$.*

(2) *G/G° is of prime-to-p order and has a normal abelian subgroup of index $\leq B_n$.*

(3) *If, in addition, the radical of* G° *is unipotent, then*

$$[G(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p) : \mathscr{G}] \le C_n.$$

Proof. We fix $A_n \ge 2n$ large enough for Proposition 3 to apply.

Let $\mathscr{H} = G(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$. Let $F_m\mathscr{H}$ denote the subgroup of $\mathscr{H}$ consisting of elements congruent to 1 (mod p^m). We identify $F_m\mathscr{H}/F_{m+1}\mathscr{H}$ with a subspace of M_n over the field $\mathbb{F}_p$. As

$$(1 + p^m A)^p \equiv 1 + p^{m+1} A \pmod{p^{m+2}},$$

we have that

$$F_m\mathscr{H}/F_{m+1}\mathscr{H} \subset F_{m+1}\mathscr{H}/F_{m+2}\mathscr{H}$$

for all $m \ge 1$. It follows that

$$\dim F_m\mathscr{H}/F_{m+1}\mathscr{H} \le \dim G$$

for all $m \ge 1$. Indeed, otherwise, the quotient $\mathscr{H}/F_m\mathscr{H}$ would grow at least as fast as $cp^{m(1+\dim G)}$, which is impossible [Serre 1981, Theorem 8].

As $\mathscr{G} \subset \mathscr{H}$, we have

$$F_m\mathscr{G}/F_{m+1}\mathscr{G} \subset F_m\mathscr{H}/F_{m+1}\mathscr{H}.$$

By the preceding lemma the dimension of $F_m\mathscr{G}/F_{m+1}\mathscr{G}$ is at least the dimension of the vector space spanned by the logarithms of elements of order p in the (mod p) reduction of $\mathscr{G}$. By the correspondence between exponentially generated groups and nilpotently generated Lie algebras this dimension is the Nori dimension of $\mathscr{G}$. In summary, for all $m \ge 1$,

$$\operatorname{Ndim} \mathscr{G} \le F_m\mathscr{G}/F_{m+1}\mathscr{G} \le F_m\mathscr{H}/F_{m+1}\mathscr{H} \le \dim G.$$

This proves the first claim of the theorem.

If the Nori dimension of $\mathscr{G}$ equals $\dim G$, we have further that

$$\dim F_m\mathscr{G}/F_{m+1}\mathscr{G} = \dim F_m\mathscr{H}/F_{m+1}\mathscr{H},$$

for all $m \ge 1$. As $\mathscr{G}$ and $\mathscr{H}$ are closed subgroups of $\mathrm{GL}_n(\mathbb{Z}_p)$, this implies $F_1\mathscr{G} = F_1\mathscr{H}$, which implies (1).

If G is any closed subgroup of GL_n, there exists a finite central extension of G/G° which can be realized as a subgroup of $G(\mathbb{Q}_p)$. (See, e.g., the proof of [Khare et al. 2008, Proposition 6.2].) Jordan's theorem implies the existence of a normal abelian subgroup of bounded index.

For $n < p - 1$, $\mathrm{GL}_n(\mathbb{Q}_p)$ has no element of order p, since the p-th cyclotomic polynomial is irreducible over $\mathbb{Q}_p$. On the other hand, every extension of a group containing an element of order p again has an element of order p. This gives (2).

For (3), we note first that since $\mathcal{G}$ meets every component of G, it suffices to prove that

$$\mathcal{G}^\circ := \mathcal{G} \cap G^\circ(\mathbb{Q}_p)$$

is of bounded index in $G^\circ(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$. As $[\mathcal{G}:\mathcal{G}^\circ]$ is prime to p, the (mod p) reduction of $\mathcal{G}^\circ$ is of prime-to-p index in that of $\mathcal{G}$. It follows that $\operatorname{Ndim}\mathcal{G}^\circ = \operatorname{Ndim}\mathcal{G}$. Replacing $\mathcal{G}$ with $\mathcal{G}^\circ$ if necessary, we may assume without loss of generality that G is connected.

Let F denote any finite extension of $\mathbb{Q}_p$ over which G has no nontrivial anisotropic quotient. We may take F to be totally ramified over $\mathbb{Q}_p$ since the anisotropic simple groups over $\mathbb{Q}_p$ are all central quotients of groups of the form $\mathrm{SL}_1(D)$, where D is a division algebra over $\mathbb{Q}_p$ [Kneser 1965], and every degree n division algebra over $\mathbb{Q}_p$ splits over $\mathbb{Q}_p(p^{1/n})$. We denote by $\mathbb{O}$ the ring of elements of nonnegative valuation in F. Thus, the residue field of $\mathbb{O}$ is $\mathbb{F}_p$. By Proposition 2, G_F is exponentially generated.

Let $\bar{G}_F$ denote $G_F \cup (\mathbb{P}_F^{n^2} \setminus \mathrm{GL}_{n,F})$, regarded as a reduced subscheme of $\mathbb{P}_F^{n^2}$ and $\bar{G}_{\mathbb{O}}$ denote the schematic closure of $\bar{G}_F \subset \mathbb{P}_F^{n^2}$ in $\mathbb{P}_{\mathbb{O}}^{n^2}$, i.e., the unique $\mathbb{O}$-flat closed subscheme of $\mathbb{P}_{\mathbb{O}}^{n^2}$ having generic fiber $\bar{G}_F$ [Grothendieck 1965, Proposition 2.8.5 on p. 35]. Thus, $\mathcal{H} \subset \bar{G}_{\mathbb{O}}(\mathbb{O})$.

Let X denote the union of Hilbert schemes of the polynomials in S over $\mathbb{Z}[1/N]$, where N and S are given by Proposition 3. Let Y be the universal closed subscheme of $\mathbb{P}_X^{n^2}$ with Hilbert polynomials in S. If A_n is sufficiently large, for every $p > A_n$, every p-adic field F, and every exponentially generated $G_F \subset \mathrm{GL}_{n,F}$, there exists an F-point $x \in X(F)$ such that $G_F = Y_x \cap \mathrm{GL}_{n,F}$. By the valuative criterion of properness, x extends to a morphism $\operatorname{Spec}\mathbb{O} \to X$, where $\mathbb{O}$ is the ring of integers in F. Pulling back Y by this morphism, we obtain an $\mathbb{O}$-flat subscheme of $\mathrm{GL}_{n,\mathbb{O}}$ whose generic point is $\bar{G}_F$. This must be isomorphic to $\bar{G}_{\mathbb{O}}$ by uniqueness of flat extension over $\mathbb{O}$. Let $G_{\mathbb{O}}$ denote the intersection of $\bar{G}_{\mathbb{O}}$ with $\mathrm{GL}_{n,\mathbb{O}} \subset \mathbb{P}_{\mathbb{O}}^{n^2}$. Thus $G_{\mathbb{O}}$ is flat over $\mathbb{O}$ and the generic fiber of $G_{\mathbb{O}}$ is $\bar{G}_F \cap \mathrm{GL}_{n,F} = G_F$. The fiber $G_{\mathbb{F}_p}$ has no more irreducible components than the fiber $\bar{G}_{\mathbb{F}_p}$, which can be regarded as a fiber of $Y \to X$. By the local constructibility of the function giving the number of irreducible components of geometric fibers [Grothendieck 1966, Corollary 9.7.9 on p. 82] and Noetherian induction, this gives an upper bound d_n on $G_{\mathbb{F}_p}/G^\circ_{\mathbb{F}_p}$ independent of G and $p > A_n$.

By the flatness of $G_{\mathbb{O}}$, the special fiber $G_{\mathbb{F}_p}$ has dimension equal to that of G_F, which is $\operatorname{Ndim}\mathcal{G}$. We claim that the number of $\mathbb{F}_p$-points of a connected d-dimensional algebraic group over $\mathbb{F}_p$ is at least $(p-1)^d$ and at most $(p+1)^d$. This is obvious for additive groups (where the number of points is p^d) and tori (where the number of points is $Q(p)$, Q being the characteristic polynomial of Frobenius on the character group), and it is well-known in the semisimple case. It follows in the general case from the structure theory of connected linear algebraic groups. The upper bound implies

$$G_{\mathbb{F}_p}(\mathbb{F}_p) \leq |G_{\mathbb{F}_p}/G^\circ_{\mathbb{F}_p}|(p+1)^{\mathrm{N}\dim \mathcal{G}} \leq d_n(3/2)^{n^2} p^{\mathrm{N}\dim \mathcal{G}}.$$

The kernel $F_1 G_{\mathbb{O}}(\mathbb{O})$ of the reduction map

$$G_{\mathbb{O}}(\mathbb{O}) \to G_{\mathbb{O}}(\mathbb{F}_p) = G_{\mathbb{F}_p}(\mathbb{F}_p)$$

consists of elements of $F_1\,\mathrm{GL}_n(\mathbb{O})$, i.e., elements of $\mathrm{GL}_n(\mathbb{O})$ congruent to 1 modulo the maximal ideal of $\mathbb{O}$. Thus,

$$\mathcal{H} \cap F_1 G_{\mathbb{O}}(\mathbb{O}) \subset \mathrm{GL}_n(\mathbb{Z}_p) \cap F_1\,\mathrm{GL}_n(\mathbb{O}) = F_1\,\mathrm{GL}_n(\mathbb{Z}_p).$$

It follows that

$$|\mathcal{H}/F_1\mathcal{H}| \leq d_n(3/2)^{n^2} p^{\mathrm{N}\dim \mathcal{G}}.$$

On the other hand, by Nori's theorem [1987], $(\mathcal{G}/F_1\mathcal{G})^+$ is of bounded index e_n in $G_{N(\mathcal{G}/F_1\mathcal{G})}(\mathbb{F}_p)$. The lower bound for points on a connected group implies

$$|\mathcal{G}/F_1\mathcal{G}| \geq |(\mathcal{G}/F_1\mathcal{G})^+| \geq e_n^{-1}(p-1)^{\mathrm{N}\dim \mathcal{G}} \geq e_n^{-1} 2^{-n^2} p^{\mathrm{N}\dim \mathcal{G}}.$$

Combining these estimates, we obtain

$$\frac{|\mathcal{H}/F_1\mathcal{H}|}{|\mathcal{G}/F_1\mathcal{G}|} \leq 3^{n^2} d_n e_n.$$

As $F_1\mathcal{G} = F_1\mathcal{H}$, setting $C_n = 3^{n^2} d_n e_n$, we obtain (3). □

Acknowledgements. The impetus to write this paper came from correspondence with N. Katz regarding these monodromy questions. It gives me great pleasure to thank him. I would also like to thank B. Conrad for a number of helpful comments on an earlier draft of this paper.

References

[Borel 1991] A. Borel, *Linear algebraic groups*, 2nd ed., Graduate Texts in Mathematics **126**, Springer, New York, 1991. MR 92d:20001 Zbl 0726.20030

[Chevalley 1954] C. Chevalley, "On algebraic group varieties", *J. Math. Soc. Japan* **6** (1954), 303–324. MR 16,672g Zbl 0057.26301

[Grothendieck 1961] A. Grothendieck, "Techniques de construction et théorèmes d'existence en géométrie algébrique, IV: les schémas de Hilbert", in *Séminaire Bourbaki,* 1960/61, fasc. 3, exposé 221, Secrétariat mathématique, Paris, 1961. Reprinted W. A. Benjamin, Amsterdam, 1966, and Soc. Mat. de France, Paris, 1995, pp. 249–276.

[Grothendieck 1965] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 1–231. MR 33 #7330 Zbl 0135.39701

[Grothendieck 1966] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, III", *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 1–255. MR 36 #178 Zbl 0144.19904

[Khare et al. 2008] C. Khare, M. Larsen, and G. Savin, "Functoriality and the inverse Galois problem", *Compos. Math.* **144**:3 (2008), 541–564. MR 2009m:11076 Zbl 1194.11062

[Kneser 1965] M. Kneser, "Galois-Kohomologie halbeinfacher algebraischer Gruppen über $\mathfrak{p}$-adischen Körpern, II", *Math. Z.* **89** (1965), 250–272. MR 32 #5658 Zbl 0143.04702

[Nori 1987] M. V. Nori, "On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$", *Invent. Math.* **88**:2 (1987), 257–275. MR88d:20068 Zbl 0632.20030

[Serre 1981] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 123–201. MR 83k:12011 Zbl 0496.12011

[Steinberg 1965] R. Steinberg, "Regular elements of semisimple algebraic groups", *Inst. Hautes Études Sci. Publ. Math.* **25** (1965), 49–80. MR 31 #4788 Zbl 0136.30002

Communicated by Bjorn Poonen
Received 2009-05-15 Revised 2010-07-21 Accepted 2010-07-21

mjlarsen@indiana.edu Department of Mathematics, Rawles Hall, Indiana University, Bloomington, IN 47405-5701, United States
http://mlarsen.math.indiana.edu/~larsen/

ALGEBRA AND NUMBER THEORY 4:8(2010)

On the (non)rigidity of the Frobenius endomorphism over Gorenstein rings

Hailong Dao, Jinjia Li and Claudia Miller

It is well-known that for a large class of local rings of positive characteristic, including complete intersection rings, the Frobenius endomorphism can be used as a test for finite projective dimension. In this paper, we exploit this property to study the structure of such rings. One of our results states that the Picard group of the punctured spectrum of such a ring R cannot have p-torsion. When R is a local complete intersection, this recovers (with a purely local algebra proof) an analogous statement for complete intersections in projective spaces first given by Deligne in SGA and also a special case of a conjecture by Gabber. Our method also leads to many simply constructed examples where rigidity for the Frobenius endomorphism does not hold, even when the rings are Gorenstein with isolated singularity. This is in stark contrast to the situation for complete intersection rings. A related length criterion for modules of finite length and finite projective dimension is discussed towards the end.

1. Introduction

The Frobenius endomorphism for rings of positive characteristic has been one of the central objects of study in homological commutative algebra over the past decades. Not only is it a useful tool in proofs of homological conjectures, but also its intrinsic homological properties have been shown to have strong connections with the structure of the ring or of modules over it. In this article we provide several surprising connections, for example, the relationship between the ability of the Frobenius to detect the finite projective dimension of modules and the torsion part of the divisor class group.

We review some history and notation. In [Kunz 1969, Theorem 2.1] regular local rings are characterized as those for which the Frobenius endomorphism $f : R \to R$ (or equivalently some iteration of it) is flat. Since then, a list of papers has yielded further similar homological results for f, each analogous to a classical homological

Miller gratefully acknowledges partial financial support from NSA grant #H98230-06-1-0035. Dao is partially supported by NSF grant 0834050.

MSC2000: primary 13A35; secondary 13D07, 14A05, 13C20.

Keywords: Frobenius endomorphism, rigidity, Tor, Picard group, isolated singularity.

result concerning the residue field k (viewed as an R-module via $\pi : R \to k$); for further details see the survey [Miller 2003], as well as [Avramov et al. 2006; Iyengar and Sather-Wagstaff 2004]. We will use the notation ${}^{f^n}\!R$ for R viewed as an R-module via the n-th iteration f^n of f.

For their celebrated proof of the Intersection Theorem, Peskine and Szpiro [1969, Corollary 2; 1972, Theorem 1.7] generalized one direction of Kunz's result, and shortly thereafter Herzog [1974, Theorem 3.1] proved the converse, yielding the following equivalence:

$$M \text{ has finite projective dimension} \Leftrightarrow \operatorname{Tor}_i^R(M, {}^{f^n}\!R) = 0 \text{ for all } i > 0 \text{ and all } n > 0.$$

This leads one to ask to what extent the module ${}^{f^n}\!R$ could function as a test module for finite projective dimension: is the vanishing of $\operatorname{Tor}_i^R(M, {}^{f^n}\!R)$ for just *one* value each of $i > 0$ and $n > 0$ sufficient? In particular, this would imply that the R-module ${}^{f^n}\!R$ is *rigid*, that is, that

$$\operatorname{Tor}_i^R(M, {}^{f^n}\!R) = 0 \implies \operatorname{Tor}_{i+1}^R(M, {}^{f^n}\!R) = 0.$$

Several steps toward these goals have been made in recent years. In the general setting, [Koh and Lee 1998, Proposition 2.6] proved a *finiteness* result: there is a constant $c(R)$, depending only on the ring R, such that vanishing of $\operatorname{Tor}_i^R(M, {}^{f^n}\!R)$ for any depth $R + 1$ consecutive values of $i > 0$ and any one value of $n \geq c(R)$ implies that M has finite projective dimension. In fact, it showed that depth R consecutive values of i suffice if R is Cohen–Macaulay of positive dimension. The best possible result however, occurs in the setting of complete intersection rings:

Theorem 1.1 [Avramov and Miller 2001; Dutta 2003]. *Let R be a local complete intersection and M a finitely generated R-module. Then the vanishing of* $\operatorname{Tor}_i^R(M, {}^{f^n}\!R)$ *for* one *value each of $i > 0$ and $n > 0$ implies that M has finite projective dimension.*

Phenomena like this can occur over noncomplete intersection rings as well. In such a case, we call the corresponding ${}^{f^n}\!R$ strongly rigid (which is equivalent to being rigid when $n \geq c(R)$ by Koh and Lee's result above). See Definition 2.1 and Example 2.2 for known examples.

In Section 2, we study the properties of Gorenstein local rings whose corresponding ${}^{f^n}\!R$ is strongly rigid. We show that if R is Gorenstein such that ${}^{f^n}\!R$ is locally strongly rigid (i.e., strongly rigid at the localization at every prime ideal), then the minimal infinite projective dimension locus of a module M (see Definition 2.3) must be contained in the set of associated primes of $F^n(M)$ (see Theorem 2.5). One consequence of this result is the following characterization for modules of finite projective dimension:

Corollary 2.6. *Let R be a Gorenstein local ring such that ${}^{f^n}R$ is locally strongly rigid for some $n > 0$ and M an R-module. Then M has finite projective dimension if and only if $\operatorname{Ass} F^n(M)$ is contained in the finite projective dimension locus of M.*

Note that the class of rings such that ${}^{f^n}R$ is locally strongly rigid for all $n > 0$ includes, but is strictly bigger than, the class of all local complete intersections; see Example 2.2.

We also apply Theorem 2.5 to prove that the divisor class groups of certain Gorenstein domains have no p-torsion.

Theorem 2.9. *Let R be a Gorenstein local ring such that ${}^{f^n}R$ is locally strongly rigid for some $n > 0$. Let I be a reflexive ideal such that I is locally free in codimension 2. Furthermore, assume that $\operatorname{Hom}_R(I, I) \cong R$. Let $q = p^n$. Then if $I^{(q)}$ satisfies Serre's condition (S_3), I must be principal. In particular, the Picard group of the punctured spectrum of R has no p-torsion. If, furthermore, R satisfies condition (R_2), $\operatorname{Cl}(R)$ has no p-torsion.*

This theorem shows that the Picard groups of the punctured spectrum of complete intersection rings cannot have p-torsion. For complete intersections in projective spaces, such a result was first proved in [Deligne 1973, Theorem 1.8] using sophisticated geometric machinery. We also note that this particular case confirms the positive characteristic case of the following conjecture:

Conjecture 1.2 [Gabber 2004]. *Let $(R, \mathfrak{m})$ be a local complete intersection ring of dimension 3. Let $U_R = \operatorname{Spec}(R) - \{\mathfrak{m}\}$ be the punctured spectrum of R. Then $\operatorname{Pic}(U_R)$ is torsion-free.*

It was implied in [Gabber 2004] that the positive characteristic case is known, but we cannot find a precise reference. In any case, it is worth noting that our proof is purely homological and quite simple.

In Section 3, we push the ideas in the previous section further to construct many examples of Gorenstein local rings R such that ${}^{f^n}R$ is not strongly rigid. In other words, the vanishing of $\operatorname{Tor}_i^R(M, {}^{f^n}R)$ for just one value each of $i > 0$ and $n > 0$ is *not* sufficient to conclude that M has finite projective dimension. Two different approaches are used in these constructions. The first approach boils down to finding an isolated Gorenstein singularity with torsion class group and applying Theorem 2.9; see Example 3.2. The second approach takes a different route, via Lemma 3.3. Obtaining an actual example requires some explicit computations on the determinantal ring of 2×2 minors in 9 variables and hence is less general than the first approach; see Example 3.5. The bonus is, however, that these have a torsion-free class group.

In Section 4, we study the connection between (strong) rigidity and numerical rigidity (see Definitions 4.1 and 4.2) of the Frobenius endomorphism. The main result we prove there is this:

Theorem 4.6. *Let R be a Cohen–Macaulay local ring with isolated singularity and of positive dimension. Fix $n > 0$. If ${}^{f^n}(R/yR)$ is numerically rigid for every nonzerodivisor $y \in R$, then ${}^{f^n}R$ is strongly rigid against modules of dimension up to one.*

The rest of the introduction contains a review of the notation and definitions used throughout the paper. We assume throughout that R is a commutative Noetherian local ring of prime characteristic $p > 0$ and that all R-modules M and N are finitely generated. The Frobenius endomorphism $f : R \to R$ is defined by $f(r) = r^p$ for $r \in R$; its self-compositions are given by $f^n(r) = r^{p^n}$. Restriction of scalars along each iteration f^n endows R with a new R-module structure, denoted by ${}^{f^n}R$.

The Frobenius functor, introduced in [Peskine and Szpiro 1972], is given by base change along the Frobenius endomorphism:

$$F_R(M) = M \otimes_R {}^{f}R$$

for any R-module M. Its compositions are given by $F_R^n(M) = M \otimes_R {}^{f^n}R$, namely base change along the compositions f^n of f. We omit the subscript R if there is no ambiguity about R. Note particularly that the module structure on $F^n(M)$ is via usual multiplication in R on the right hand factor of the tensor product. The values of the derived functors $\operatorname{Tor}_i^R(M, {}^{f^n}R)$ are similarly viewed as R-modules via the target of the base change map f^n.

It is easy to verify that $F^n(R) \cong R$ and that for cyclic modules $F^n(R/I) \cong R/I^{[q]}$, where $q = p^n$ and $I^{[q]}$ denotes the ideal generated by the q-th powers of the generators of I. We frequently use q to denote the power p^n, which may vary.

In the sequel, $\ell(M)$ will denote the *length* and $\operatorname{pd} M$ the *projective dimension* of the module M. By the *codimension* of M we mean $\dim R - \dim M$. We use the notation $\boldsymbol{x}$ for a sequence of elements of R and often write simply $R/\boldsymbol{x}$ for $R/(\boldsymbol{x})$ to save space. Likewise, $\boldsymbol{x}^q$ denotes the ideal generated by the q-th powers of the sequence $\boldsymbol{x}$, *not* the q-th power of the ideal $\boldsymbol{x}$.

2. Strong rigidity of Frobenius and torsion elements in divisor class groups

We now investigate the consequences of the phenomenon that over certain rings the Frobenius map can be used to test for finite projective dimension (e.g., over complete intersection rings). This work enables us to prove strong results about torsion elements in the class groups of complete intersection rings and also allows us to construct counterexamples to such phenomena over noncomplete intersection rings. We begin with some convenient definitions to facilitate the discussion.

Definition 2.1. An R-module N is called *strongly rigid* if for any integer i and any finitely generated R-module M, $\operatorname{Tor}_i^R(M, N) = 0$ implies $\operatorname{pd}_R M < \infty$. The module N is called *locally strongly rigid* if $N_{\mathfrak{p}}$ is strongly rigid for all $\mathfrak{p} \in \operatorname{Spec} R$.

Example 2.2. If R is a local complete intersection ring, then ${}^{f^n}\!R$ is locally strongly rigid for all n; see Theorem 1.1. For any local Cohen–Macaulay ring R of dimension at most 1, there is a number $c(R)$ such that for any $n \geq c(R)$, ${}^{f^n}\!R$ is strongly rigid by virtue of [Koh and Lee 1998, Proposition 2.6], already mentioned on page 1040. In particular, when $(R, \mathfrak{m})$ is Artinian and $\mathfrak{m}^{[p]} = 0$, then ${}^{f^n}\!R$ is (locally) strongly rigid for all n [Miller 2003, 2.2.8].

Definition 2.3 [Dao 2010]. Let M be an R-module. One defines the infinite projective dimension locus of M as

$$\mathrm{IPD}(M) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \operatorname{pd}_{R_\mathfrak{p}} M_\mathfrak{p} = \infty\}.$$

Similarly, define $\mathrm{FPD}(M)$ to be the finite projective dimension locus of M. Finally, we define the n-strong rigidity locus of R as

$$\mathrm{SR}_n(R) = \{\mathfrak{p} \in \operatorname{Spec} R \mid {}^{f^n}\!R_\mathfrak{p} \text{ is strongly rigid}\}.$$

The following standard facts, which we state without proof, will be used often:

Fact 2.4. *Let $f : R \to S$ be a ring homomorphism and $\mathfrak{p}$ a prime ideal of S. Then for each $i \geq 0$ and R-module M there is a natural isomorphism*

$$\operatorname{Tor}_i^R(M, S)_\mathfrak{p} \cong \operatorname{Tor}_i^{R_{f^{-1}(\mathfrak{p})}}(M_{f^{-1}(\mathfrak{p})}, S_\mathfrak{p}).$$

Furthermore, if f is the Frobenius endomorphism of R, then $f^{-1}(\mathfrak{p}) = \mathfrak{p}$ and $R_{f^{-1}(\mathfrak{p})} \to S_\mathfrak{p}$ is the Frobenius endomorphism of $R_\mathfrak{p}$.

Theorem 2.5. *Let R be a Gorenstein local ring and M an R-module. Then*

$$\min \mathrm{IPD}(M) \cap \mathrm{SR}_n(R) \subseteq \operatorname{Ass} F^n(M).$$

In particular, if ${}^{f^n}\!R$ is locally strongly rigid, then

$$\min \mathrm{IPD}(M) \subseteq \operatorname{Ass} F^n(M).$$

Proof. Since R is Gorenstein, by the Cohen–Macaulay approximation due to [Auslander and Buchweitz 1989, 1.8], there is a short exact sequence

$$0 \to M \to Q \to N \to 0,$$

where $\operatorname{pd} Q < \infty$ and N is maximal Cohen–Macaulay. Tensoring with the Frobenius endomorphism, we have an embedding

$$0 \to \operatorname{Tor}_1^R(N, {}^{f^n}\!R) \to F^n(M). \tag{2-1}$$

Take any $\mathfrak{p} \in \min \mathrm{IPD}(M) \cap \mathrm{SR}_n(R)$; then $\operatorname{pd}_{R_\mathfrak{p}} M_\mathfrak{p} = \infty$ and ${}^{f^n}\!R_\mathfrak{p}$ is strongly rigid. It follows that $\operatorname{pd}_{R_\mathfrak{p}} N_\mathfrak{p} = \infty$ and therefore that $\operatorname{Tor}_1^{R_\mathfrak{p}}(N_\mathfrak{p}, {}^{f^n}\!R_\mathfrak{p}) \neq 0$. On the other hand, since $\mathfrak{p}$ is minimal in the infinite projective dimension locus of M,

$\operatorname{pd}_{R_\mathfrak{q}} M_\mathfrak{q} < \infty$ for any prime $\mathfrak{q} \subsetneq \mathfrak{p}$, whence $\operatorname{pd}_{R_\mathfrak{q}} N_\mathfrak{q} < \infty$ and so $\operatorname{Tor}_1^{R_\mathfrak{q}}(N_\mathfrak{q}, {}^{f^n}R_\mathfrak{q}) = 0$. Therefore, the length of $\operatorname{Tor}_1^{R_\mathfrak{p}}(N_\mathfrak{p}, {}^{f^n}R_\mathfrak{p})$ must be finite.

Localizing (2-1) at $\mathfrak{p}$, we have an exact sequence

$$0 \to \operatorname{Tor}_1^{R_\mathfrak{p}}(N_\mathfrak{p}, {}^{f^n}R_\mathfrak{p}) \to F^n(M)_\mathfrak{p}.$$

This implies that depth $F^n(M)_\mathfrak{p} = 0$. Hence $\mathfrak{p} \in \operatorname{Ass} F^n(M)$. □

Corollary 2.6. *Let R be a Gorenstein local ring such that ${}^{f^n}R$ is locally strongly rigid for some $n > 0$ and M an R-module. Then M has finite projective dimension if and only if* $\operatorname{Ass} F^n(M) \subseteq \operatorname{FPD}(M)$.

As an immediate consequence, we obtain the following special case with simpler hypotheses. Here, $\operatorname{Sing}(R)$ denotes the singular locus of R. Note particularly that the hypothesis that $\min \operatorname{Supp} M$ and $\operatorname{Sing}(R)$ are disjoint holds, for example, when $\dim M > \dim \operatorname{Sing}(R)$.

Corollary 2.7. *Let R be a Gorenstein local ring such that ${}^{f^n}R$ is locally strongly rigid for some $n > 0$ (e.g., if R is a local complete intersection) and M an R-module such that* $(\min \operatorname{Supp} M) \cap \operatorname{Sing}(R) = \varnothing$. *If $F^n(M)$ has no embedded primes, then M has finite projective dimension. In particular, if $F^n(M)$ is Cohen–Macaulay, then M is perfect.*

Proof. It suffices to note that

$$\operatorname{Ass} F^n(M) = \min \operatorname{Supp} F^n(M) = \min \operatorname{Supp} M \subseteq \operatorname{Spec} R \setminus \operatorname{Sing}(R) \subseteq \operatorname{FPD}(M),$$

where the first equality is by the assumption that $F^n(M)$ has no embedded primes, the second is well-known (see [Peskine and Szpiro 1972], for example) and the first containment follows from the hypothesis. □

Remark 2.8. If R is reduced, we do not know if the disjointness of $\min \operatorname{Supp} M$ and $\operatorname{Sing}(R)$ in Corollary 2.7 can be replaced by the simpler condition $\dim M > 0$. However, this is impossible when R is not reduced (see [Miller 2003, 2.1.7], for example).

We now give an application of Theorem 2.5 to divisor class groups. In the sequel, we use $\operatorname{Cl}(R)$ to denote the divisor class group of R. We refer to [Fossum 1973] for the definition and basic facts about $\operatorname{Cl}(R)$ and the Picard groups and to [Bruns and Herzog 1993] for Serre's conditions (R_n) and (S_n).

Theorem 2.9. *Let R be a Gorenstein local ring such that ${}^{f^n}R$ is locally strongly rigid for some $n > 0$. Let I be a reflexive ideal such that I is locally free in codimension 2. Furthermore, assume that* $\operatorname{Hom}_R(I, I) \cong R$. *Let $q = p^n$. Then if $I^{(q)}$ satisfies Serre's condition (S_3), I must be principal. In particular, the Picard group of the punctured spectrum of R has no p-torsion. If, furthermore, R satisfies condition (R_2), then* $\operatorname{Cl}(R)$ *has no p-torsion.*

Proof. We may assume $\dim R \geq 3$. Assume that I is not principal, then it follows that $\operatorname{pd} I = \infty$ (see [Braun 2004, Corollary 11] and [Bourbaki 1965, Chapter VII, §4, no. 7, Corollary 2]). We claim that one can always write $I = (a) : (b)$ for $a, b \in R$. Here is a quick proof: choose a such that a generates I at the minimal primes of I. Pick an irredundant primary decomposition of (a); it can be written as $I \cap J$ (if $I = (a)$ we are done). Choosing b in J but not in any minimal prime of I, one can show that $I = (a) : (b)$. By the short exact sequence

$$0 \to R/(a:b) \xrightarrow{b} R/(a) \to R/(a,b) \to 0$$

we obtain $\operatorname{IPD}(I) = \operatorname{IPD}(R/(a,b))$. Thus we have $\mathfrak{p} \in \min \operatorname{IPD}(R/(a,b))$ for any $\mathfrak{p} \in \min \operatorname{IPD}(I)$, and so by Theorem 2.5,

$$\mathfrak{p} \in \operatorname{Ass}\big(F^n(R/(a,b))\big) = \operatorname{Ass}(R/(a^q, b^q)).$$

Localize the short exact sequence

$$0 \to R/(a^q : b^q) \to R/(a^q) \to R/(a^q, b^q) \to 0$$

at $\mathfrak{p}$, and observe that $(a^q : b^q) = I^{(q)}$. From the fact that $\operatorname{depth}(R/(a^q, b^q))_{\mathfrak{p}} = 0$ we get $\operatorname{depth} I_{\mathfrak{p}}^{(q)} \leq 2$. On the other hand, since I is locally free in codimension 2, $\dim R_{\mathfrak{p}} \geq 3$. So, $I^{(q)}$ does not satisfy (S_3), and our first assertion is proved. The last two statements follow immediately (note that if R is (R_2) then R is automatically normal). □

As a corollary we can recover a notable result about torsion elements in the Picard groups of complete intersections.

Corollary 2.10. *Let R be an equicharacteristic local complete intersection ring of dimension at least* 3. *Then the Picard group of the punctured spectrum of R is torsion-free. If, furthermore, R satisfies condition* (R_2), *then the class group of R is torsion-free.*

Let X be a complete intersection variety of dimension at least 2 *in the projective space over a field. The Picard group of X modulo the hyperplane section is torsion-free.*

Proof. Let p be the characteristic exponent of R (so it is 1 if the characteristic of R is 0). The fact that neither the Picard group nor $\operatorname{Cl}(R)$ has an element whose order is relatively prime to p was well-known [Robbiano 1976]. Theorem 2.9 takes care of the p-torsion elements. The second half of the corollary follows by applying the first to the local ring at the origin of the affine cone over X. □

Remark 2.11. The second half of the corollary was first proved in [Deligne 1973]. Another proof was given in [Bădescu 1978, Theorem B]. As far as we know, ours is the first algebraic proof.

Example 2.12. The conditions $\dim R \geq 3$ and (R_2) in the corollary cannot be weakened. Let $R = k[[x, y, z]]/(xy - z^2)$, where k is an algebraically closed field of characteristic other than 2. Then $\dim R = 2$ and R is regular in codimension 1, but $\mathrm{Cl}(R) \cong \mathbb{Z}/(2)$ (see, for example, [Fossum 1973, Proposition 11.4]).

3. Examples of nonrigidity

In this section we construct plenty of examples of a Gorenstein ring R in positive characteristic such that ${}^{f^n}\!R$ is not (strongly) rigid. This is in stark contrast to the situation for complete intersection rings, where the strong rigidity of ${}^{f^n}\!R$ is known to hold. Our constructions take two completely different approaches. The first approach (see Example 3.2) provides the desired examples with torsion divisor class groups. This can be viewed as a natural consequence of Theorem 2.9. The second approach (see Example 3.5), on the contrary, provides the desired examples with torsion-free divisor class groups.

First we isolate a consequence of Theorem 2.9:

Corollary 3.1. *Let R be a local, Gorenstein domain with isolated singularity. Suppose that $\dim R \geq 3$ and $\mathrm{Cl}(R)$ has a torsion element of order l that satisfies (S_3). Then ${}^{f^n}\!R$ is not strongly rigid for any n such that $p^n \equiv 1$ or 0 modulo l. In particular, if $l = 2$, then ${}^{f^n}\!R$ is not strongly rigid for any n and not rigid for $n \gg 0$.*

Proof. Let I be a reflexive ideal which represents an l-torsion element in $\mathrm{Cl}(R)$ and $q = p^n$. Then the ideal $J = I^{(q)}$ is isomorphic to I or R, both of which satisfy (S_3), contradicting Theorem 2.9. When $l = 2$, for any n, $q = p^n$ is congruent to 0 or 1 modulo 2. The last statement follows from Example 2.2. ☐

Example 3.2. It is not hard to find examples of isolated Gorenstein singularities with torsion class group. Let $S = k[x_1, \dots, x_d]$ and l be an integer. Let T be the l-Veronese subring of S and R be the local ring at the homogeneous maximal ideal of T. Then one can show that $\mathrm{Cl}(R) = \mathrm{Cl}(T) = \mathbb{Z}/(l)$ using [Watanabe 1981, Theorem 1.6]. The ring R obviously has an isolated singularity, as it is the local ring at the origin of the cone over a smooth projective variety. Also, R will be Gorenstein as long as l divides d. Finally, let I represent the generator of $\mathrm{Cl}(T)$. It is easy to see that the cyclic cover of T corresponding to I is S, so I, and therefore the generator of $\mathrm{Cl}(R)$, is Cohen–Macaulay. In particular, it will be (S_3). So all of the conditions of Corollary 3.1 can be satisfied easily.

For the rest of this section we will take another approach to construct examples of nonrigidity in which the rings have *torsion-free* divisor class groups. The following result gives a general technique for finding such examples:

Lemma 3.3. *Let $(R, \mathfrak{m})$ be a Gorenstein ring with isolated singularity and positive dimension. The following are equivalent*:

(1) ${}^{f^n}R$ *is strongly rigid.*

(2) *For any R-module L with infinite projective dimension*, depth $F^n(L) = 0$.

Proof. That (1) implies (2) is a consequence of Corollary 2.6. Now assume (2). Let L be a module of infinite projective dimension. It is enough to prove that $\operatorname{Tor}_1^R(L, {}^{f^n}R) \neq 0$. Consider the exact sequence

$$0 \to L_1 \to Q \to L \to 0$$

where Q is free and L_1 is the first syzygy of L. If $\operatorname{Tor}_1^R(L, {}^{f^n}R) = 0$, then by tensoring with ${}^{f^n}R$ one gets

$$0 \to F^n(L_1) \to Q \to F^n(L) \to 0.$$

But since $\operatorname{pd}_R L = \operatorname{pd}_R L_1 = \infty$, one has depth $F^n(L_1) =$ depth $F^n(L) = 0$. Since depth $Q = \dim Q > 0$, this is a contradiction. □

We also need the following crucial observation.

Lemma 3.4. *Let k be a field of characteristic $p > 0$. Let A denote the determinantal ring $k[X]/I_2$ where $X = (X_{ij})$ is a 3×3 matrix of indeterminates and I_2 is the ideal of $k[X]$ generated by all the 2×2 minors of X. Let x_{ij} denote the images of X_{ij} in A. Let $L = A/(x_{11}, x_{12})$. Then* depth $F^n(L) > 0$ *for all $n > 0$ and* pd $L = \infty$.

Proof. Let δ_{ij} denote the minor of X corresponding to X_{ij} and I be the ideal of $k[X]$ generated by X_{11}^n, X_{12}^n, and all the δ_{ij}. We prove that for any field k (we do not need to assume that k has prime characteristic!) and any $n \geq 2$, x_{33} is a nonzerodivisor for $A/(x_{11}^n, x_{12}^n) \cong k[X]/I$. In the following paragraph, we refer the reader to [Eisenbud 1995, 15.2–4] for notation and terminology (some of it italicized) regarding Gröbner bases.

We fix a *reverse lexicographic order* $>$ on the monomials such that

$$X_{11} > X_{12} > X_{13} > X_{21} > X_{22} > X_{23} > X_{31} > X_{32} > X_{33}.$$

Using *Buchberger's algorithm*, one can produce a Gröbner basis for I consisting of all the δ_{ij}, X_{11}^n, X_{12}^n, and all the monomials of the form $X_{11}^l X_{12}^{n-l} X_{22}^s X_{32}^t$, where l runs from 1 through $n-1$ and s, t run through all positive integers such that $s + t = l$. Therefore the *initial ideal* of I (henceforth $\operatorname{in}(I)$) does not contain any monomial divisible by X_{33}. Assume for some $g \in k[X]$, $X_{33}g \in I$. Let g_0 be the *remainder* of g (with respect to the generators of I) in a *standard expression* obtained by performing the *division algorithm*. If $g_0 \neq 0$, then $X_{33}g_0 \neq 0$ since $k[X]$ is a domain. On the other hand, since $X_{33}g_0 \in I$, at least one of the monomials of $X_{33}g_0$ is in $\operatorname{in}(I)$. Thus, at least one of the monomials of g_0 is in $\operatorname{in}(I)$. This contradicts the fact that g_0 is a nonzero remainder. Thus $g_0 = 0$ and $g \in I$. It follows that x_{33} is a nonzerodivisor for $k[X]/I$.

Finally, we show $\operatorname{pd} L = \infty$. Assume that $\operatorname{pd} L < \infty$, i.e., the ideal (x_{11}, x_{12}) is of finite projective dimension. By [MacRae 1963, Corollary 4.4], two-generated ideals of finite projective dimension have the form $a(b, c)$, where a is a nonzero-divisor and b, c form a regular sequence. But if $(x_{11}, x_{12}) = a(b, c)$ for such a, b, and c, since the degree of x_{11} is one, a is forced to be a unit (otherwise, (x_{11}, x_{12}) would be a principal ideal which is impossible). Therefore $(x_{11}, x_{12}) = (b, c)$. But since $x_{11}x_{22} - x_{21}x_{12} = 0$, (x_{11}, x_{12}) cannot be an ideal generated by a regular sequence of two elements. This is a contradiction. □

Combining the two lemmas above, we get the following example. Note that the divisor class group of the ring in this example is isomorphic to $\mathbb{Z}$ [Bruns and Herzog 1993, 7.3.5], which is torsion-free.

Example 3.5. Let R be the localization of the determinantal ring A as in Lemma 3.4 with respect to the maximal ideal (X). Then ${}^{f^n}\!R$ is not strongly rigid for any n.

Remark 3.6. In view of the theorem of Koh and Lee mentioned in Section 1, Example 3.5 immediately yields the nonrigidity of ${}^{f^n}\!R$ for any $n \geq c(R)$ (see Example 2.2). But in fact, with a little further computation, the reader can check that this example yields nonrigidity for *all* $n > 0$: indeed, the module N of infinite projective dimension constructed in Theorem 2.5 by taking for the module M the module L of Lemma 3.4 satisfies $\operatorname{Tor}_1^R(N, {}^{f^n}\!R) = 0$ by the argument in the proof. But it can be shown that in fact $\operatorname{Tor}_2^R(N, {}^{f^n}\!R) \neq 0$.

We point out that we do not know of any example showing that ${}^{f^n}\!R$ is not (strongly) rigid when $\dim R = 0$ or against a module M of finite length. See, however, the discussion at the end of Section 4.

4. Some further observations

Throughout this section, d will always be the dimension of the ring and n always denotes some positive integer. We know from the previous section that R could fail to be strongly rigid when R is no longer a complete intersection ring. However, we still hope that to some extent such a property could hold over noncomplete intersection rings. In particular, we do not know any example showing that ${}^{f^n}\!R$ is not rigid when $\dim R = 0$ or against a module M of finite length.

We first make two more definitions, the first of which is just a refinement of the definition of strong rigidity of ${}^{f^n}\!R$.

Definition 4.1. Let h be a nonnegative integer. ${}^{f^n}\!R$ is called *strongly rigid against modules of dimension at most* h if, for any integer i and any finitely generated module M of dimension at most h, $\operatorname{Tor}_i^R(M, {}^{f^n}\!R) = 0$ implies $\operatorname{pd}_R M < \infty$.

Definition 4.2. ${}^{f^n}\!R$ is called *numerically rigid* if for any R-module M of finite length, $\ell(F^n(M)) = p^{nd}\ell(M)$ implies $\operatorname{pd}_R M < \infty$.

The latter definition is motivated by the following characterization for modules of finite projective dimension and finite length over complete intersection rings.

Theorem [Dutta 1983; Miller 2003]. *Let R be a complete intersection ring in characteristic p and M an R-module of finite length. Then the following are equivalent*:

(1) *M has finite projective dimension*,

(2) *$\ell(F^n(M)) = p^{nd}\ell(M)$ for all $n > 0$*,

(3) *$\ell(F^n(M)) = p^{nd}\ell(M)$ for some $n > 0$.*

The implication (3) ⇒ (1) simply says that if R is a complete intersection ring, then ${}^{f^n}R$ is numerically rigid for any n. When R is no longer a complete intersection ring, it is an open question whether ${}^{f^n}R$ could still be numerically rigid.[1] In fact, such a question is closely related to the rigidity question discussed earlier. The goal of this section is to explore the connections between them.

The following technical result plays a crucial role here. Recall that if $\ell(M \otimes N)$ and $\operatorname{pd} N$ are finite, then

$$\chi(M, N) \overset{\text{def}}{=} \sum_{j=0}^{\operatorname{pd} N} (-1)^j \ell(\operatorname{Tor}_j^R(M, N)).$$

Proposition 4.3. *Let R be a Noetherian local Cohen–Macaulay ring of positive dimension and of characteristic $p > 0$. Let M be an R-module of codimension c. Suppose* $\dim M > 0$ *and $R_{\mathfrak{p}}$ is a complete intersection ring for every minimal prime $\mathfrak{p}$ of M. Then*

$$\ell(F^n_{R/\boldsymbol{x}}(M/\boldsymbol{x}M)) \geq q^c \chi(M, R/\boldsymbol{x}) \tag{$*$}$$

for all $n > 0$ and for any system of parameters $\boldsymbol{x}$ of $F^n(M)$ which is also R-regular. Given $n > 0$, equality holds in $(*)$ if and only if $F^n(M)$ is Cohen–Macaulay and $\operatorname{pd}_{R_{\mathfrak{p}}} M_{\mathfrak{p}}$ *is finite for every minimal prime $\mathfrak{p}$ of M.*

For the proof the properties of the higher Euler characteristics of Koszul complexes are used in an essential way. We recall some terms and results here.

For a pair of modules M and N such that $\ell(M \otimes N) < \infty$ and $\operatorname{pd} N < \infty$, the *$i$-th higher Euler characteristic* is defined by the formula

$$\chi_i(M, N) = \sum_{j=i}^{\operatorname{pd} N} (-1)^{j-i} \ell(\operatorname{Tor}_j^R(M, N)).$$

By convention, $\chi(M, N) = \chi_0(M, N)$. Some standard facts about χ and χ_i can be found in [Lichtenbaum 1966; Serre 1975]. In this paper, we particularly need the following two well-known results:

[1] The implication (1) ⇒ (2) in the theorem fails even over Gorenstein rings [Miller and Singh 2000].

Lemma 4.4 [Lichtenbaum 1966, Lemma 1]. *Let M be an R-module and $\boldsymbol{x} = \{x_1, x_2, \dots, x_c\}$ an R-sequence such that $\ell(M/\boldsymbol{x}M) < \infty$. Then $\chi(M, R/\boldsymbol{x}) \geq 0$, with the equality holding if and only if* $\dim M < c$.

Theorem 4.5 [Lichtenbaum 1966, Theorem 1]. *Let M be an R-module and $\boldsymbol{x}$ an R-sequence such that $\ell(M/\boldsymbol{x}M) < \infty$. Then for any $i > 0$, $\chi_i(M, R/\boldsymbol{x}) \geq 0$, with the equality holding if and only if* $\operatorname{Tor}_i(M, R/\boldsymbol{x}) = 0$ (*and hence* $\operatorname{Tor}_j(M, R/\boldsymbol{x}) = 0$ *for all $j \geq i$*).

Proof of Proposition 4.3. We have $\min \operatorname{Supp} F^n(M) = \min \operatorname{Supp} M$, since $\operatorname{Supp} M$ and $\operatorname{Supp} F^n(M)$ coincide [Peskine and Szpiro 1972]. Now write

$$\begin{aligned}
\ell(F^n_{R/\boldsymbol{x}}(M/\boldsymbol{x}M)) &= \ell(F^n(M) \otimes_R R/\boldsymbol{x}) \\
&\geq \chi(F^n(M), R/\boldsymbol{x}) \\
&= \sum_{\mathfrak{p} \in \min \operatorname{Supp} M} \ell(F^n(M)_{\mathfrak{p}}) \chi(R/\mathfrak{p}, R/\boldsymbol{x}) \\
&= \sum_{\mathfrak{p} \in \min \operatorname{Supp} M} \ell(F^n_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})) \chi(R/\mathfrak{p}, R/\boldsymbol{x}) \\
&\geq \sum_{\mathfrak{p} \in \min \operatorname{Supp} M} q^c \ell(M_{\mathfrak{p}}) \chi(R/\mathfrak{p}, R/\boldsymbol{x}) \\
&= q^c \chi(M, R/\boldsymbol{x}),
\end{aligned}$$

where the first inequality holds since $\chi_1(F^n(M), R/\boldsymbol{x}) \geq 0$ by Theorem 4.5, the second and last equalities hold by Lemma 4.4, and the second inequality is a result over complete intersection rings [Dutta 1983, Theorem 1.9] (note that $R_{\mathfrak{p}}$ is complete intersection by the hypotheses).

Therefore, furthermore, equality holds if and only if $\chi_1(F^n(M), R/\boldsymbol{x}) = 0$ and $\ell(F^n_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})) = q^c \ell(M_{\mathfrak{p}})$ for every minimal prime $\mathfrak{p}$ of M. The former is equivalent to $F^n(M)$ being Cohen–Macaulay by Theorem 4.5 and the latter is equivalent to $M_{\mathfrak{p}}$ having finite projective dimension over $R_{\mathfrak{p}}$ by [Miller 2003, Theorem 5.2.2], since $R_{\mathfrak{p}}$ is a complete intersection ring. □

Theorem 4.6. *Let R be a Cohen–Macaulay local ring with isolated singularity and of positive dimension. Fix some $n > 0$. If for every nonzerodivisor $y \in R$, ${}^{f^n}(R/yR)$ is numerically rigid, then ${}^{f^n}R$ is strongly rigid against modules of dimension at most one.*

Proof. Let M be an R-module of dimension at most one. Assume ${}^{f^n}(R/yR)$ is numerically rigid for every nonzerodivisor $y \in R$. We want to prove that for any $i > 0$, $\operatorname{Tor}_i(M, {}^{f^n}R) = 0$ implies $\operatorname{pd} M < \infty$. Let $\boldsymbol{x} = \{x_1, \dots, x_{d-1}\}$ be an R-sequence contained in $\operatorname{Ann} M$. We may assume that $i = 1$ by replacing M by its $(i-1)$-th syzygy over the ring $R/(x_1, \dots, x_{d-1})$ and using that $\operatorname{Tor}_i(R/(x_1, \dots, x_{d-1}), {}^{f^n}R)$ vanishes for all $i > 0$, since $\operatorname{pd}_R R/(x_1, \dots, x_{d-1}) < \infty$.

Letting K be the first syzygy of M as an $R/(x_1, \dots, x_{d-1})$-module, we get a short exact sequence:

$$0 \to F^n(K) \to F^n\big((R/(x_1, \dots, x_{d-1}))^t\big) \to F^n(M) \to 0.$$

It follows that $F^n(K)$ is a Cohen–Macaulay module of dimension one. Hence by Proposition 4.3 (note that R has an isolated singularity), one has $\ell(F^n_{R/yR}(K/yK)) = q^{d-1}\chi(K, R/yR)$ for every $y \in R$ which is regular on both K and R. Therefore, $\ell(F^n_{R/yR}(K/yK)) = q^{d-1}\ell(K/yK)$. Since we assume ${}^{f^n}(R/yR)$ is numerically rigid, K/yK has finite projective dimension over R/yR. Thus K has finite projective dimension over R, whence M does too by the long exact sequence of Tors against the residue field k. □

Remark 4.7. For the determinantal ring $R = k[X]/I_2$ used in Section 3, it was shown there that ${}^{f^n}R$ is not strongly rigid against modules of dimension at most 5 for any n. In fact, we can also modify the example a little bit to show that it is not strongly rigid against modules of dimension at most 3. For k of arbitrary characteristic, though, we do not know if ${}^{f^n}R$ is strongly rigid against modules of dimension at most 0, 1, or 2. However, in characteristic 2 we have an example which shows that ${}^{f^1}R$ is not strongly rigid against modules of dimension 1. In fact, if we set $k = \mathbb{Z}/2\mathbb{Z}$ and take the module $N = R/(x_{12}, x_{13}, x_{21}, x_{23}, x_{31}, x_{32})$, then it is easy to check that $\dim N = 1$, depth $F(N) = 1$, and pd $N = \infty$. Taking an R-sequence x_1, x_2, x_3, x_4 contained in the annihilator of N and embedding N into a module of finite projective dimension over $R/(x_1, x_2, x_3, x_4)$ (via the Auslander–Buchweitz short exact sequence again), the cokernel of this embedding gives such an example. Therefore, by Theorem 4.6, we also obtain an example of a Gorenstein ring R in characteristic 2 for which the corresponding R-module ${}^{f^1}R$ is not numerically rigid.

Acknowledgements. We thank Craig Huneke for crucial remarks which connected our works, and Srikanth Iyengar, who carefully read an earlier version of this manuscript and suggested a better statement for Corollary 2.6. We also thank the anonymous referee for many helpful comments.

References

[Auslander and Buchweitz 1989] M. Auslander and R.-O. Buchweitz, "The homological theory of maximal Cohen–Macaulay approximations", pp. 5–37 Mém. Soc. Math. France (N.S.) **38**, Soc. Math. de France, Paris, 1989. MR 91h:13010 Zbl 0697.13005

[Avramov and Miller 2001] L. L. Avramov and C. Miller, "Frobenius powers of complete intersections", *Math. Res. Lett.* **8**:1-2 (2001), 225–232. MR 2002b:13022 Zbl 1034.13006

[Avramov et al. 2006] L. L. Avramov, S. Iyengar, and C. Miller, "Homology over local homomorphisms", *Amer. J. Math.* **128**:1 (2006), 23–90. MR 2007e:13027 Zbl 1102.13011

[Bădescu 1978] L. Bădescu, "A remark on the Grothendieck–Lefschetz theorem about the Picard group", *Nagoya Math. J.* **71** (1978), 169–179. MR 80g:14012 Zbl 0358.14026

[Bourbaki 1965] N. Bourbaki, *Algèbre commutative, ch. 7: diviseurs*, Actualités Scientifiques et Industrielles **1314**, Hermann, Paris, 1965. Translated as part of *Commutative algebra*, Hermann, Paris, 1972. MR 41 #5339

[Braun 2004] A. Braun, "On a question of M. Auslander", *J. Algebra* **276**:2 (2004), 674–684. MR 2005a:13020 Zbl 1084.13004

[Bruns and Herzog 1993] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, 1993. MR 95h:13020 Zbl 0788.13005

[Dao 2010] H. L. Dao, "Decency and Tor-rigidity for modules over hypersurfaces", preprint, 2010. arXiv math/0611568v3

[Deligne 1973] P. Deligne, "Cohomologie des intersections completes", pp. 39–61 in *SGA 7 XI* (Séminaire de Géométrie Algébrique du Bois Marie 1967–1969), Lect. Notes Math. **340**, Springer, Berlin, 1973. Zbl 0265.14007

[Dutta 1983] S. P. Dutta, "Frobenius and multiplicities", *J. Algebra* **85**:2 (1983), 424–448. MR 85f:13022 Zbl 0527.13014

[Dutta 2003] S. P. Dutta, "On modules of finite projective dimension over complete intersections", *Proc. Amer. Math. Soc.* **131**:1 (2003), 113–116. MR 2003j:13016 Zbl 1007.13006

[Eisenbud 1995] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001

[Fossum 1973] R. M. Fossum, *The divisor class group of a Krull domain*, Ergebnisse der Math. **74**, Springer, New York, 1973. MR 52 #3139 Zbl 0256.13001

[Gabber 2004] O. Gabber, "On purity for the Brauer group", pp. 1975–1977 in *Arithmetic Algebraic Geometry*, Oberwolfach Report **37**, 2004.

[Herzog 1974] J. Herzog, "Ringe der Charakteristik p und Frobeniusfunktoren", *Math. Z.* **140** (1974), 67–78. MR 50 #4569 Zbl 0278.13006

[Iyengar and Sather-Wagstaff 2004] S. Iyengar and S. Sather-Wagstaff, "G-dimension over local homomorphisms: applications to the Frobenius endomorphism", *Illinois J. Math.* **48**:1 (2004), 241–272. MR 2005c:13016 Zbl 1103.13009

[Koh and Lee 1998] J. Koh and K. Lee, "Some restrictions on the maps in minimal resolutions", *J. Algebra* **202**:2 (1998), 671–689. MR 99d:13017 Zbl 0909.13008

[Kunz 1969] E. Kunz, "Characterizations of regular local rings for characteristic p", *Amer. J. Math.* **91** (1969), 772–784. MR 40 #5609 Zbl 0188.33702

[Lichtenbaum 1966] S. Lichtenbaum, "On the vanishing of Tor in regular local rings", *Illinois J. Math.* **10** (1966), 220–226. MR 32 #5688 Zbl 0139.26601

[MacRae 1963] R. E. MacRae, "On the homological dimension of certain ideals", *Proc. Amer. Math. Soc.* **14** (1963), 746–750. MR 28 #5103

[Miller 2003] C. Miller, "The Frobenius endomorphism and homological dimensions", pp. 207–234 in *Commutative algebra* (Grenoble/Lyon, 2001), edited by L. L. Avramov et al., Contemp. Math. **331**, Amer. Math. Soc., Providence, RI, 2003. MR 2004j:13020 Zbl 1085.13502

[Miller and Singh 2000] C. M. Miller and A. K. Singh, "Intersection multiplicities over Gorenstein rings", *Math. Ann.* **317**:1 (2000), 155–171. MR 2001h:13031 Zbl 0970.13007

[Peskine and Szpiro 1969] C. Peskine and L. Szpiro, "Sur la topologie des sous-schémas fermés d'un shéma localement noethérien, définis comme support d'un faisceau cohérent localement de dimension projective finie", *C. R. Acad. Sci. Paris Sér. A* **269** (1969), 49–51. MR 40 #1385 Zbl 0184.29001

[Peskine and Szpiro 1972] C. Peskine and L. Szpiro, "Dimension projective finie et cohomologie locale. Applications à la démonstration de conjectures de M. Auslander, H. Bass et A. Grothendieck", *Inst. Hautes Études Sci. Publ. Math.* 42 (1972), 47–119. MR 51 #10330 Zbl 0268.13008

[Robbiano 1976] L. Robbiano, "Some properties of complete intersections in "good" projective varieties", *Nagoya Math. J.* **61** (1976), 103–111. MR 53 #13222 Zbl 0309.14043

[Serre 1975] J.-P. Serre, *Algèbre locale: multiplicités*, 3e ed., Lecture Notes in Math. **11**, Springer, Berlin, 1975. Zbl 0296.13018

[Watanabe 1981] K. Watanabe, "Some remarks concerning Demazure's construction of normal graded rings", *Nagoya Math. J.* **83** (1981), 203–211. MR 83g:13016 Zbl 0518.13003

Communicated by Kei-Ichi Watanabe
Received 2009-09-11 Revised 2010-05-09 Accepted 2010-06-11

hdao@math.ku.edu — *Department of Mathematics, University of Kansas, Lawrence, KS 66045-7523, United States*

jinjia.li@louisville.edu — *Department of Mathematical Sciences, Middle Tennessee State University, Murfreesboro, TN 37132, United States*

Current address: *Department of Mathematics, University of Louisville, 328 Natural Sciences Building, Louisville, KY 40292, United States*

clamille@syr.edu — *Mathematics Department, Syracuse University, Syracuse, NY 13244-1150, United States*

ALGEBRA AND NUMBER THEORY 4:8(2010)

A lower bound on the essential dimension of simple algebras

Alexander S. Merkurjev

Let p be a prime integer and F a field of characteristic different from p. We prove that the essential p-dimension $\operatorname{ed}_p(\mathsf{CSA}(p^r))$ of the class $\mathsf{CSA}(p^r)$ of central simple algebras of degree p^r is at least $(r-1)p^r+1$. The integer $\operatorname{ed}_p(\mathsf{CSA}(p^r))$ measures complexity of the class of central simple algebras of degree p^r over field extensions of F.

1. Introduction

The essential dimension of an *algebraic structure* is a numerical invariant that measures its complexity. Informally, the essential dimension of an algebraic structure over a field F is the smallest number of algebraically independent parameters required to define the structure over a field extension of F [Berhuy and Favi 2003; Merkurjev 2009].

Let $\mathcal{F} : \mathit{Fields}/F \to \mathit{Sets}$ be a functor (an algebraic structure) from the category Fields/F of field extensions of F and field homomorphisms over F to the category of sets. Let $K \in \mathit{Fields}/F$, $\alpha \in \mathcal{F}(K)$, and K_0 be a subfield of K over F. We say that α is *defined over* K_0 (and K_0 is called a *field of definition of* α) if there exists an element $\alpha_0 \in \mathcal{F}(K_0)$ such that the image $(\alpha_0)_K$ of α_0 under the map $\mathcal{F}(K_0) \to \mathcal{F}(K)$ coincides with α. The *essential dimension of* α, denoted $\operatorname{ed}^{\mathcal{F}}(\alpha)$, is the least transcendence degree $\operatorname{tr.deg}_F(K_0)$ over all fields of definition K_0 of α. The *essential dimension of the functor* $\mathcal{F}$ is

$$\operatorname{ed}(\mathcal{F}) = \sup\{\operatorname{ed}^{\mathcal{F}}(\alpha)\},$$

where the supremum is taken over fields $K \in \mathit{Fields}/F$ and all $\alpha \in \mathcal{F}(K)$.

Let p be a prime integer and $\alpha \in \mathcal{F}(K)$. The *essential p-dimension* $\operatorname{ed}_p^{\mathcal{F}}(\alpha)$ *of* α is the minimum of $\operatorname{ed}^{\mathcal{F}}(\alpha_{K'})$ over all finite field extensions K'/K of degree prime to p. The *essential p-dimension* $\operatorname{ed}_p(\mathcal{F})$ *of* $\mathcal{F}$ is the supremum of $\operatorname{ed}_p^{\mathcal{F}}(\alpha)$ over all

The work has been supported by the NSF grant DMS #0652316.
MSC2000: primary 16K50; secondary 14L30, 20G15.
Keywords: essential dimension, Brauer group, algebraic tori.

fields $K \in \mathit{Fields}/F$ and all $\alpha \in \mathcal{F}(K)$ [Reichstein and Youssin 2000, §6]. Clearly, $\operatorname{ed}^{\mathcal{F}}(\alpha) \geq \operatorname{ed}^{\mathcal{F}}_p(\alpha)$ and $\operatorname{ed}(\mathcal{F}) \geq \operatorname{ed}_p(\mathcal{F})$ for all p.

Let $\mathit{CSA}(n)$ be the functor taking a field extension K/F to the set of isomorphism classes $\mathit{CSA}_K(n)$ of central simple K-algebras of degree n. Let p be a prime integer and let p^r be the highest power of p dividing n. Then $\operatorname{ed}_p\bigl(\mathit{CSA}(n)\bigr) = \operatorname{ed}_p\bigl(\mathit{CSA}(p^r)\bigr)$ [Reichstein and Youssin 2000, Lemma 8.5.5]. Every central simple algebra of degree p is cyclic over a finite field extension of degree prime to p, and hence $\operatorname{ed}_p\bigl(\mathit{CSA}(p)\bigr) = 2$ [Reichstein and Youssin 2000, Lemma 8.5.7]. It was proven in [Merkurjev 2010] that $\operatorname{ed}_p\bigl(\mathit{CSA}(p^2)\bigr) = p^2 + 1$ and in general, $2p^{2r-2} - p^r + 1 \geq \operatorname{ed}_p\bigl(\mathit{CSA}(p^r)\bigr) \geq 2r$ for all $r \geq 2$ [Meyer and Reichstein 2009b, Theorem 1; Reichstein and Youssin 2000, Theorem 8.6].

We improve the lower bound for $\operatorname{ed}_p\bigl(\mathit{CSA}(p^r)\bigr)$ as follows:

Theorem 6.1. *Let F be a field and p a prime integer different from* $\operatorname{char}(F)$. *Then*

$$\operatorname{ed}_p\bigl(\mathit{CSA}(p^r)\bigr) \geq (r-1)p^r + 1.$$

Let G be an algebraic group over F. The *essential dimension* $\operatorname{ed}(G)$ (resp. *essential p-dimension* $\operatorname{ed}_p(G)$) of G is the essential dimension (resp. essential p-dimension) of the functor $G\text{-}\mathit{torsors}$ taking a field K to the set of isomorphism classes of all G-torsors (principal homogeneous G-spaces) over K.

If $G = \mathbf{PGL}(n)$ is the projective linear group over F, the functor $G\text{-}\mathit{torsors}$ is isomorphic to the functor $\mathit{CSA}(n)$. Therefore, the theorem yields the following lower bound for the essential dimension of $\mathbf{PGL}(p^r)$:

$$\operatorname{ed}\bigl(\mathbf{PGL}(p^r)\bigr) \geq \operatorname{ed}_p\bigl(\mathbf{PGL}(p^r)\bigr) \geq (r-1)p^r + 1.$$

2. Preliminaries

Characters. Let F be a field, let F_{sep} be a separable closure of F, and let

$$\Gamma = \operatorname{Gal}(F_{\mathrm{sep}}/F)$$

be the *absolute Galois group* of F. For a Γ-module M, we write $H^n(F, M)$ for the cohomology group $H^n(\Gamma, M)$.

The *character group* $\operatorname{Ch}(F)$ of F is defined as

$$\operatorname{Hom}_{\mathrm{cont}}(\Gamma, \mathbb{Q}/\mathbb{Z}) = H^1(F, \mathbb{Q}/\mathbb{Z}) \simeq H^2(F, \mathbb{Z}).$$

For a character $\chi \in \operatorname{Ch}(F)$, set $F(\chi) = (F_{\mathrm{sep}})^{\operatorname{Ker}(\chi)}$. Then $F(\chi)/F$ is a cyclic field extension of degree $\operatorname{ord}(\chi)$. If $\Phi \subset \operatorname{Ch}(F)$ is a finite subgroup, we set

$$F(\Phi) = (F_{\mathrm{sep}})^{\cap \operatorname{Ker}(\chi)},$$

where the intersection is taken over all $\chi \in \Phi$. The Galois group $G = \mathrm{Gal}(F(\Phi)/F)$ is abelian and Φ is canonically isomorphic to the character group $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ of G.

If $F' \subset F$ is a subfield and $\chi \in \mathrm{Ch}(F')$, we write χ_F for the image of χ under the natural map $\mathrm{Ch}(F') \to \mathrm{Ch}(F)$ and $F(\chi)$ for $F(\chi_F)$. If $\Phi \subset \mathrm{Ch}(F)$ is a finite subgroup, then the character $\chi_{F(\Phi)}$ is trivial if and only if $\chi \in \Phi$.

Lemma 2.1. *Let $\Phi, \Phi' \subset \mathrm{Ch}(F)$ be two finite subgroups. Suppose that for a field extension K/F, we have $\Phi_K = \Phi'_K$ in $\mathrm{Ch}(K)$. Then there is a finite subextension K'/F in K/F such that $\Phi_{K'} = \Phi'_{K'}$ in $\mathrm{Ch}(K')$.*

Proof. Choose a set of characters $\{\chi_1, \dots, \chi_m\}$ generating Φ and a set of characters $\{\chi'_1, \dots, \chi'_m\}$ generating Φ' such that $(\chi_i)_K = (\chi'_i)_K$ for all i. Let $\eta_i = \chi_i - \chi'_i$. Since all η_i vanish over K, the finite field extension $K' := F(\eta_1, \dots, \eta_m)$ of F can be viewed as a subextension in K/F. Now $\Phi_{K'} = \Phi'_{K'}$ since $(\chi_i)_{K'} = (\chi'_i)_{K'}$. □

Brauer groups. We write $\mathrm{Br}(F)$ for the *Brauer group* $H^2(F, F^\times_{\mathrm{sep}})$ of a field F. If $a \in \mathrm{Br}(F)$ and K/F is a field extension, then we write a_K for the image of a under the natural homomorphism $\mathrm{Br}(F) \to \mathrm{Br}(K)$. We write $\mathrm{Br}(K/F)$ for the *relative Brauer group* $\mathrm{Ker}\big(\mathrm{Br}(F) \to \mathrm{Br}(K)\big)$. We say that K is a splitting field of a if $a_K = 0$, that is, $a \in \mathrm{Br}(K/F)$. The *index* $\mathrm{ind}(a)$ of a is the smallest degree of a splitting field of a.

The cup product

$$\mathrm{Ch}(F) \otimes F^\times = H^2(F, \mathbb{Z}) \otimes H^0(F, F^\times_{\mathrm{sep}}) \to H^2(F, F^\times_{\mathrm{sep}}) = \mathrm{Br}(F)$$

takes $\chi \otimes a$ to the class $\chi \cup (a)$ in $\mathrm{Br}(F)$ that is split by $F(\chi)$.

For a finite subgroup $\Phi \subset \mathrm{Ch}(F)$, write $\mathrm{Br}_{\mathrm{dec}}\big(F(\Phi)/F\big)$ for the *subgroup of decomposable elements* in $\mathrm{Br}\big(F(\Phi)/F\big)$ generated by the elements $\chi \cup (a)$ for all $\chi \in \Phi$ and $a \in F^\times$. The *indecomposable relative Brauer group* $\mathrm{Br}_{\mathrm{ind}}\big(F(\Phi)/F\big)$ is the factor group $\mathrm{Br}\big(F(\Phi)/F\big)/\mathrm{Br}_{\mathrm{dec}}\big(F(\Phi)/F\big)$.

Complete fields. Let E be a complete field with respect to a discrete valuation v, and let K be its residue field.

Let p be a prime integer different from $\mathrm{char}(K)$. There is a natural injective homomorphism $\mathrm{Ch}(K)\{p\} \to \mathrm{Ch}(E)\{p\}$ of the p-primary components of the character groups that identifies $\mathrm{Ch}(K)\{p\}$ with the character group of an unramified field extension of E. For a character $\chi \in \mathrm{Ch}(K)\{p\}$, we write $\hat{\chi}$ for the corresponding character in $\mathrm{Ch}(E)\{p\}$.

By [Garibaldi et al. 2003, §7.9], there is an exact sequence

$$0 \to \mathrm{Br}(K)\{p\} \xrightarrow{i} \mathrm{Br}(E)\{p\} \xrightarrow{\partial_v} \mathrm{Ch}(K)\{p\} \to 0. \tag{2-1}$$

If $a \in \mathrm{Br}(K)\{p\}$, we write $\hat{a}$ for the element $i(a)$ in $\mathrm{Br}(E)\{p\}$. For example, if $a = \chi \cup (\bar{u})$ for some $\chi \in \mathrm{Ch}(K)\{p\}$ and a unit $u \in E$, then $\hat{a} = \hat{\chi} \cup (u)$.

Proposition 2.2 [Tignol 1978, Proposition 2.4; Jacob and Wadsworth 1990, Theorem 5.15(a); Garibaldi et al. 2003, Proposition 8.2]. *Let E be a complete field with respect to a discrete valuation v, and let K be its residue field of characteristic different from p. Then*:

(i) $\mathrm{ind}(\hat{a}) = \mathrm{ind}(a)$ *for any* $a \in \mathrm{Br}(K)\{p\}$.

(ii) *Let* $b = \hat{a} + \big(\hat{\chi} \cup (x)\big)$ *for an element* $a \in \mathrm{Br}(K)\{p\}$, $\chi \in \mathrm{Ch}(K)\{p\}$ *and* $x \in E^\times$. *Then* $\partial_v(b) = v(x)\chi$. *Also, if $v(x)$ is not divisible by p, we have*

$$\mathrm{ind}(b) = \mathrm{ind}(a_{K(\chi)}) \cdot \mathrm{ord}(\chi).$$

(iii) *Let E'/E be a finite field extension and v' the discrete valuation on E' extending v with residue field K'. Then for any* $b \in \mathrm{Br}(E)\{p\}$, *we have*

$$\partial_{v'}(b_{E'}) = e \cdot \partial_v(b)_{K'},$$

where e is the ramification index of E'/E.

The choice of a prime element π in E provides us with a splitting of the sequence (2-1) by sending a character χ to the class $\hat{\chi} \cup (\pi)$ in $\mathrm{Br}(E)\{p\}$. Thus, any $b \in \mathrm{Br}(E)\{p\}$ can be written in the form

$$b = \hat{a} + \big(\hat{\chi} \cup (\pi)\big), \tag{2-2}$$

for $\chi = \partial_v(b)$ and a unique $a \in \mathrm{Br}(K)\{p\}$.

The homomorphism

$$s_\pi : \mathrm{Br}(E)\{p\} \to \mathrm{Br}(K)\{p\},$$

defined by $s_\pi(b) = a$, where a is given by (2-2), is called a *specialization* map. For example, $s_\pi(\hat{a}) = a$ for any $a \in \mathrm{Br}(K)\{p\}$ and $s_\pi\big(\hat{\chi} \cup (x)\big) = \chi \cup (\bar{u})$, where $\chi \in \mathrm{Ch}(K)\{p\}$, $x \in E^\times$ and u is the unit in E such that $x = u\pi^{v(x)}$.

If v is trivial on a subfield $F \subset E$ and $\Phi \subset \mathrm{Ch}(F)\{p\}$ a finite subgroup, then

$$s_\pi\big(\mathrm{Br}_{\mathrm{dec}}(E(\Phi)/E)\big) \subset \mathrm{Br}_{\mathrm{dec}}\big(K(\Phi)/K\big). \tag{2-3}$$

We shall need the following technical lemma. For an abelian group A we write ${}_pA$ for the subgroup of all elements in A of exponent dividing p.

Lemma 2.3. *Let (E, v) be a complete discrete valued field with the residue field K of characteristic different from p containing a primitive p^2-th root of unity. Let $\eta \in \mathrm{Ch}(E)$ be a character of order p^2 such that $p \cdot \eta$ is unramified, that is, $p \cdot \eta = \hat{\nu}$ for some $\nu \in \mathrm{Ch}(K)$ of order p. Let $\chi \in {}_p\mathrm{Ch}(K)$ be a character linearly independent from ν. Let $a \in \mathrm{Br}(K)$ and set $b = \hat{a} + \big(\hat{\chi} \cup (x)\big) \in \mathrm{Br}(E)$, where $x \in E^\times$ is an element such that $v(x)$ is not divisible by p. Then*:

(i) *If η is unramified, that is, $\eta = \hat{\mu}$ for some $\mu \in \mathrm{Ch}(K)$ of order p^2, then* $\mathrm{ind}(b_{E(\eta)}) = p \cdot \mathrm{ind}(a_{K(\mu,\chi)})$.

(ii) *If η is ramified, then there exists a unit $u \in E^\times$ such that $K(\nu) = K(\bar{u}^{1/p})$ and* $\mathrm{ind}(b_{E(\eta)}) = \mathrm{ind}\big(a - (\chi \cup (\bar{u}^{1/p}))\big)_{K(\nu)}$.

Proof. (i) If $\eta = \hat{\mu}$ for some $\mu \in \mathrm{Ch}(K)$, then $K(\mu)$ is the residue field of $E(\eta)$ and we have

$$b_{E(\eta)} = \hat{a}_{K(\mu)} + \big(\hat{\chi}_{K(\mu)} \cup (x)\big).$$

Since χ and ν are linearly independent, the character $\chi_{K(\mu)}$ is nontrivial. The first statement follows from Proposition 2.2(ii).

(ii) Since $p \cdot \eta$ is unramified, the ramification index of $E(\eta)/E$ is equal to p, and hence $E(\eta) = E\big((ux^p)^{1/p^2}\big)$ for some unit $u \in E$. Note that $K(\nu) = K(\bar{u}^{1/p})$ is the residue field of $E(\eta)$. Since $u^{1/p}x$ is a pth power in $E(\eta)$, the class

$$b_{E(\eta)} = \hat{a}_{K(\nu)} - \big(\hat{\chi}_{K(\nu)} \cup (u^{1/p})\big) = \hat{a}_{K(\nu)} - \big(\widehat{\chi_{K(\nu)} \cup (\bar{u}}^{1/p})\big)$$

is unramified. It follows from Proposition 2.2(i) that the elements $b_{E(\eta)}$ in $\mathrm{Br}\big(E(\eta)\big)$ and $a_{K(\nu)} - \big(\chi_{K(\nu)} \cup (\bar{u}^{1/p})\big)$ in $\mathrm{Br}\big(K(\nu)\big)$ have the same indices. □

3. Brauer group and algebraic tori

Torsors. Let G be an algebraic group over F and let K/F be a field extension. The set of isomorphism classes of G-torsors (principal homogeneous spaces) over K is bijective to $H^1(K, G)$ [Serre 1997].

Example 3.1. Let A be a central simple F-algebra of degree n and $G = \mathbf{Aut}(A)$. Then $H^1(K, G)$ is the set of isomorphism classes of central simple K-algebras of degree n, or equivalently, the set of elements in $\mathrm{Br}(K)$ of index dividing n. If $A = M_n(F)$ is the split algebra, then $G = \mathbf{PGL}(n)$.

Example 3.2. Let L be an étale F-algebra of dimension n. Consider the algebraic torus $U = R_{L/F}(\mathbb{G}_{m,L})/\mathbb{G}_m$ over F. The exact sequence

$$1 \to \mathbb{G}_m \to R_{L/F}(\mathbb{G}_{m,L}) \to U \to 1$$

and Hilbert Theorem 90 yield an isomorphism $\theta : H^1(F, U) \xrightarrow{\sim} \mathrm{Br}(L/F)$. Note that if L is a subalgebra of a central simple F-algebra A of degree n, then U is a maximal torus in the group $\mathbf{Aut}(A)$.

Let $\alpha : G \to \mathbf{GL}(W)$ be a finite dimensional representation over F. Suppose that α is *generically free*, that is, there is a nonempty open subset $W' \subset W$ and a G-torsor $\beta : W' \to X$ for a variety X over F. The torsor β is *versal*, that is, every G-torsor over a field extension K/F is the pull-back of β with respect to a K-point of X. The generic fiber of β is called a *generic* G-torsor. It is a torsor over the function field $F(X)$ [Garibaldi et al. 2003; Reichstein 2000].

Example 3.3. Let S be an algebraic torus over F. We embed S into the quasitrivial torus $P = R_{L/F}(\mathbb{G}_{m,L})$, where L is an étale F-algebra [Colliot-Thélène and Sansuc 1977]. Then S acts on the vector space L by multiplication, so that the action on the open subset P is regular. If T is the factor torus P/S, then the S-torsor $P \to T$ is versal.

The tori P^Φ, S^Φ, T^Φ, U^Φ and V^Φ. Let F be a field, Φ be a subgroup of ${}_p\operatorname{Ch}(F)$ of rank r, and $L = F(\Phi)$. Let $G = \operatorname{Gal}(L/F)$. Choose a basis $\chi_1, \chi_2, \dots, \chi_r$ for Φ. We can view each χ_i as a character of G, that is, as a homomorphism $\chi_i : G \to \mathbb{Q}/\mathbb{Z}$. Let $\sigma_1, \sigma_2, \dots, \sigma_r$ be the dual basis for G, that is,

$$\chi_i(\sigma_j) = \begin{cases} (1/p) + \mathbb{Z} & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Let R be the group ring $\mathbb{Z}[G]$. Consider the surjective homomorphism of G-modules $k : R^r \to R$ taking the ith basis element e_i of R^r to $\sigma_i - 1$. The image of k is the *augmentation ideal* $I = \operatorname{Ker}(\varepsilon)$ in R, where $\varepsilon : R \to \mathbb{Z}$ is defined by $\varepsilon(\rho) = 1$ for all $\rho \in G$.

Write $N_i = 1 + \sigma_i + \sigma_i^2 + \cdots + \sigma_i^{p-1} \in R$.

Set $N := \operatorname{Ker}(k)$. Consider the following elements in N:

$$e_{ij} := (\sigma_i - 1)e_j - (\sigma_j - 1)e_i \quad \text{and} \quad f_i = N_i e_i, \quad i, j = 1, \dots r.$$

Lemma 3.4. *The G-module N is generated by e_{ij} and f_i.*

Proof. Let $\overline{R} = \mathbb{Z}[t_1, \dots, t_r]$ be the polynomial ring. Acyclicity of the Koszul complex for the homomorphism $\bar{k} : (\overline{R})^r \to \overline{R}$, taking the ith basis element $\bar{e}_i$ to $t_i - 1$ [Matsumura 1980, Theorem 43] implies that $\operatorname{Ker}(\bar{k})$ is generated by $\bar{e}_{ij} := (t_i - 1)\bar{e}_j - (t_j - 1)\bar{e}_i$.

The kernel J of the surjective homomorphism $\overline{R} \to R$, taking t_i to σ_i, is generated by $t_i^p - 1$.

Let $x := \sum x_i e_i \in \operatorname{Ker}(k)$. Lift every x_i to a polynomial $\bar{x}_i \in \overline{R}$ and consider $\bar{x} := \sum \bar{x}_i \bar{e}_i \in (\overline{R})^r$. We have $\bar{k}(\bar{x}) \in J$, and hence

$$\bar{k}(\bar{x}) = \sum (t_i - 1)\bar{x}_i = \sum (t_i^p - 1)h_i = \sum (t_i - 1)\overline{N}_i h_i,$$

for some polynomials $h_i \in \overline{R}$, where $\overline{N}_i = 1 + t_i + t_i^2 + \cdots + t_i^{p-1} \in R$. Hence the element $\sum (\bar{x}_i - h_i \overline{N}_i)\bar{e}_i$ belongs to the kernel of $\bar{k}$ and therefore is a linear combination of $\bar{e}_{ij}$. It follows that $\bar{x}$ is a linear combination of $\bar{e}_{ij}$ and $\overline{N}_i \bar{e}_i$, and hence x is a linear combination of e_{ij} and f_i. $\square$

Let $\varepsilon_i : R^r \to \mathbb{Z}$ be the ith projection followed by the augmentation map ε. It follows from Lemma 3.4 that $\varepsilon_i(N) = p\mathbb{Z}$ for every i. Moreover, the G-homomorphism

$$l : N \to \mathbb{Z}^r, \quad m \mapsto \big(\varepsilon_1(m)/p, \dots, \varepsilon_r(m)/p\big)$$

is surjective. Set $M = \mathrm{Ker}(l)$ and $Q = R^r/M$.

Lemma 3.5. *The G-module M is generated by e_{ij}.*

Proof. Let M' be the submodule of N generated by e_{ij}. Clearly, $M' \subset M$. Note also that $(\sigma_j - 1) f_i = N_i e_{ij} \in M'$, and hence $I f_i \subset M'$.

Suppose that $m \in M$. By Lemma 3.4, modifying m by an element in M', we can assume that $m = \sum_{i=1}^r x_i f_i$ for some $x_i \in R$. Since $l(m) = 0$, we have $\varepsilon(x_i) = 0$, that is, $x_i \in I$ for all i, and hence $m \in \sum I f_i \subset M'$. □

Let P^Φ, S^Φ, T^Φ, U^Φ and V^Φ be the algebraic tori over F with the character G-modules R^r, Q, M, I and N, respectively. The diagram of homomorphisms of G-modules with exact columns and rows

$$\begin{tikzcd} M \arrow[r, equal] \arrow[d, hook] & M \arrow[d, hook] & \\ N \arrow[r, hook] \arrow[d, two heads, "l"'] & R^r \arrow[r, two heads, "k"] \arrow[d, two heads] & I \arrow[d, equal] \\ \mathbb{Z}^r \arrow[r, hook] & Q \arrow[r, two heads] & I \end{tikzcd} \tag{3-1}$$

yields the following diagram of homomorphisms of the tori:

$$\begin{tikzcd} U^\Phi \arrow[r, hook] \arrow[d, equal] & S^\Phi \arrow[r, two heads] \arrow[d, hook] & \mathbb{G}_m^r \arrow[d, hook] \\ U^\Phi \arrow[r, hook] & P^\Phi \arrow[r, two heads] \arrow[d, two heads] & V^\Phi \arrow[d, two heads] \\ & T^\Phi \arrow[r, equal] & T^\Phi \end{tikzcd} \tag{3-2}$$

Let K/F be a field extension. Set $KL := K \otimes_F L$. The exact sequence of G-modules

$$0 \to I \to R \to \mathbb{Z} \to 0 \tag{3-3}$$

gives an exact sequence of the tori

$$1 \to \mathbb{G}_m \to R_{L/F}(\mathbb{G}_{m,L}) \to U \to 1,$$

and then an exact sequence

$$0 \to H^1(K, U^\Phi) \to H^2(K, \mathbb{G}_m) \to H^2(KL, \mathbb{G}_m).$$

Hence

$$H^1(K, U^\Phi) \simeq \mathrm{Br}(KL/K). \tag{3-4}$$

Lemma 3.6. *The homomorphism $(K^\times)^r \to H^1(K, U^\Phi) \simeq \mathrm{Br}(KL/K)$ induced by the first row of the diagram (3-2) takes $(x_1, \ldots, x_r)$ to $\sum_{i=1}^r \big((\chi_i)_K \cup (x_i)\big)$.*

Proof. Consider the composition

$$h : \mathrm{Hom}_G(\mathbb{Z}^r, \mathbb{Z}) \to \mathrm{Ext}^1_G(I, \mathbb{Z}) \to \mathrm{Ext}^2_G(\mathbb{Z}, \mathbb{Z}) = H^2(G, \mathbb{Z}) = \mathrm{Ch}(G), \tag{3-5}$$

where the first homomorphism is induced by the bottom row of the diagram (3-1), and the second one by the exact sequence (3-3).

We claim that for any k, the image of the kth projection $p_k : \mathbb{Z}^r \to \mathbb{Z}$ under the composition (3-5) coincides with χ_k. Consider the G-homomorphism $R^r \to \mathbb{Q}$, taking e_k to $1/p$ and e_i to 0 for all $i \neq k$. By Lemma 3.5, this homomorphism vanishes on M, and hence it factors through a map $Q \to \mathbb{Q}$. Thus, we have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}^r \arrow[r] \arrow[d, "p_k"'] & Q \arrow[r] \arrow[d] & I \arrow[r] \arrow[d, "f_k"'] & 0 \\ 0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Q} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \end{tikzcd} \tag{3-6}$$

for the map f_k defined by $f_k(\sigma_k - 1) = 1/p + \mathbb{Z}$ and $f_k(\sigma_i - 1) = 0$ for all $i \neq k$.

Let α be the image of the class of the top row of (3-6) under the map $p_k^* : \mathrm{Ext}^1_G(I, \mathbb{Z}^r) \to \mathrm{Ext}^1_G(I, \mathbb{Z})$. Then $h(p_k)$ is the image of α under the second map in the composition (3-5). Hence $h(p_k)$ is also the image of the class β of the sequence (3-3) under the connecting map

$$H^1(G, I) = \mathrm{Ext}^1_G(\mathbb{Z}, I) \to \mathrm{Ext}^2_G(\mathbb{Z}, \mathbb{Z}) = H^2(G, \mathbb{Z})$$

induced by the exact sequence representing the class α.

The diagram (3-6) yields a commutative diagram

$$\begin{tikzcd} H^1(G, I) \arrow[r, "\partial"] \arrow[d, "f_k^*"'] & H^2(G, \mathbb{Z}^r) \arrow[d, "p_k^*"'] \\ H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r, equal] & H^2(G, \mathbb{Z}) \end{tikzcd}$$

As we have shown, $p_k^*\big(\partial(\beta)\big) = h(p_k)$. Therefore, it suffices to prove that $f_k^*(\beta) = \chi_k$. The cocycle β satisfies $\beta(\sigma_i) = \sigma_i - 1$. It follows that $f_k^*(\beta)(\sigma_k) = f_k(\sigma_k - 1) = 1/p + \mathbb{Z}$ and $f_k^*(\beta)(\sigma_i) = 0$ for all $i \neq k$. This proves the claim.

Consider the commutative diagram

$$\begin{tikzcd} (K^\times)^r = \mathrm{Hom}_G(\mathbb{Z}^r, \mathbb{Z}) \otimes K^\times \arrow[r] \arrow[d, equal] & \mathrm{Ext}^1_G(I, \mathbb{Z}) \otimes K^\times \arrow[r] \arrow[d] & \mathrm{Ext}^2_G(\mathbb{Z}, \mathbb{Z}) \otimes K^\times \arrow[d] \\ (K^\times)^r = \mathrm{Hom}_G(\mathbb{Z}^r, KL^\times) \arrow[r] & \mathrm{Ext}^1_G(I, KL^\times) \arrow[r] & \mathrm{Ext}^2_G(\mathbb{Z}, KL^\times), \end{tikzcd}$$

where the vertical homomorphisms are given by the cup products. By the claim, the image of the tuple $(x_1, \dots, x_r)$ under the diagonal composition is equal to

$\sum_{i=1}^{r}\big((\chi_i)_K \cup (x_i)\big)$. On the other hand, the bottom composition coincides with

$$(K^\times)^r \to H^1(K, U^\Phi) \simeq \mathrm{Br}(KL/K). \qquad \square$$

Corollary 3.7. *The map $H^1(K, U^\Phi) \to H^1(K, S^\Phi)$ induces an isomorphism*

$$H^1(K, S^\Phi) \simeq \mathrm{Br}_{\mathrm{ind}}(KL/K).$$

It follows from Corollary 3.7 and the triviality of the group $H^1(K, P^\Phi)$ that we have a commutative diagram

$$\begin{tikzcd}
V^\Phi(K) \arrow[r] \arrow[d] & H^1(K, U^\Phi) \arrow[r, equal] \arrow[d] & \mathrm{Br}(KL/K) \arrow[d] \\
T^\Phi(K) \arrow[r] & H^1(K, S^\Phi) \arrow[r, equal] & \mathrm{Br}_{\mathrm{ind}}(KL/K)
\end{tikzcd} \tag{3-7}$$

with surjective homomorphisms.

3.1. ***The element a.*** Let a' be the image of the generic point of V^Φ over $K = F(V^\Phi)$ in $\mathrm{Br}\big(L(V^\Phi)/F(V^\Phi)\big)$ in the diagram (3-7). Choose also an element $a \in \mathrm{Br}\big(L(T^\Phi)/F(T^\Phi)\big)$ corresponding to the generic point of T^Φ over $F(T^\Phi)$. The field $F(T^\Phi)$ is a subfield of $F(V^\Phi)$ and the classes $a_{F(V^\Phi)}$ and a' are equal in $\mathrm{Br}_{\mathrm{ind}}\big(L(V^\Phi)/F(V^\Phi)\big)$. It follows that $pa_{F(V^\Phi)} = pa'$ in $\mathrm{Br}\, F(V^\Phi)$.

The exact sequence of G-modules

$$0 \to L^\times \oplus N \to L(V^\Phi)^\times \to \mathrm{Div}(V_L^\Phi) \to 0$$

induces an exact sequence

$$H^1\big(G, \mathrm{Div}(V_L^\Phi)\big) \to H^2(G, L^\times) \oplus H^2(G, N) \to H^2\big(G, L(V^\Phi)^\times\big).$$

Since $\mathrm{Div}(V_L^\Phi)$ is a permutation G-module, the first term in the sequence is trivial. Therefore, we get an injective homomorphism

$$\varphi : H^2(G, N) \to \mathrm{Br}\, F(V^\Phi)/\,\mathrm{Br}(F).$$

Then (3-1) and (3-3) yield

$$H^2(G, N) \simeq H^1(G, I) \simeq \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/p^r\mathbb{Z};$$

thus, $H^2(G, N)$ has a canonical generator ξ of order p^r.

Lemma 3.8 [Merkurjev 2010, Lemma 2.4]. *We have $\varphi(\xi) = -a' + \mathrm{Br}(F)$.*

Proof. Consider the diagram

$$\begin{tikzcd}
 & & \mathrm{Hom}_G(\mathbb{Z},\mathbb{Z}) \arrow[d] \\
 & \mathrm{Hom}_G(I,I) \arrow[r] \arrow[d] & \mathrm{Ext}^1_G(\mathbb{Z},I) \arrow[d] \\
\mathrm{Hom}_G(N,N) \arrow[r] \arrow[d] & \mathrm{Ext}^1_G(I,N) \arrow[r] \arrow[d, "l"'] & \mathrm{Ext}^2_G(\mathbb{Z},N) \arrow[d] \\
\mathrm{Hom}_G\big(N, L(V^\Phi)^\times\big) \arrow[r] & \mathrm{Ext}^1_G\big(I, L(V^\Phi)^\times\big) \arrow[r] & \mathrm{Ext}^2_G\big(\mathbb{Z}, L(V^\Phi)^\times\big)
\end{tikzcd}$$

By [Cartan and Eilenberg 1999, Chapter XIV], the images of $1_{\mathbb{Z}}$ and -1_I agree in $\mathrm{Ext}^1_G(\mathbb{Z}, I)$, and the images of 1_N and -1_I agree in $\mathrm{Ext}^1_G(I, N)$. It follows from [Cartan and Eilenberg 1999, Chapter V, Proposition 4.1] that the upper square is anticommutative. The image of $1_{\mathbb{Z}}$ is equal to $\varphi(\xi)$, and the image of 1_N is equal to $a' + \mathrm{Br}(F)$ in the right bottom corner. □

Corollary 3.9. *If $r \geq 2$, then the class $p^{r-1}a$ in $\mathrm{Br}\, F(T^\Phi)$ does not belong to the image of $\mathrm{Br}(F) \to \mathrm{Br}\, F(T^\Phi)$.*

Proof. The image of $p^{r-1}a$ in $\mathrm{Br}\, F(V^\Phi)$ coincides with $p^{r-1}a'$. Modulo the image of the map $\mathrm{Br}(F) \to \mathrm{Br}\, F(V^\Phi)$, the class $p^{r-1}a'$ is equal to $-\varphi(p^{r-1}\xi)$ and is therefore nonzero, since φ is injective. □

4. Essential dimension of algebraic tori

Let S be an algebraic torus over F with the splitting group G. We assume that G is a p-group of order p^r. Let X be the G-module of characters of S. A *p-presentation* of X is a G-homomorphism $f : P \to X$ with P a permutation G-module and finite cokernel of order prime to p. A p-presentation with the smallest $\mathrm{rank}(P)$ is called *minimal*.

Essential p-dimension of algebraic tori was determined in [Lötscher et al. 2009, Theorem 1.4]:

Theorem 4.1. *Let S be an algebraic torus over F with the (finite) splitting group G, X the G-module of characters of S, and $f : P \to X$ a minimal p-presentation of X. Then $\mathrm{ed}_p(S) = \mathrm{rank}\big(\mathrm{Ker}(f)\big)$.*

Corollary 4.2. *Suppose that X admits a surjective minimal p-presentation $f : P \to X$. Then $\mathrm{ed}(S) = \mathrm{ed}_p(S) = \mathrm{rank}\big(\mathrm{Ker}(f)\big)$.*

Proof. As explained in Example 3.3, a surjective G-homomorphism f yields a generically free representation of S of dimension $\mathrm{rank}(P)$. In view of Section 3 of

[Reichstein 2000], we have

$$\mathrm{ed}_p(S) \le \mathrm{ed}(S) \le \mathrm{rank}(P) - \dim(S) = \mathrm{rank}\big(\mathrm{Ker}(f)\big). \qquad \square$$

In this section we derive from Theorem 4.1 an explicit formula for the essential p-dimension of algebraic tori.

Define the group $\overline{X} := X/(pX + IX)$, where I is the augmentation ideal in $R = \mathbb{Z}[G]$. For any subgroup $H \subset G$, consider the composition $X^H \hookrightarrow X \to \overline{X}$. For every k, let V_k denote the image of the homomorphism

$$\coprod_{H \subset G} X^H \to \overline{X},$$

where the coproduct is taken over all subgroups H with $[G:H] \le p^k$. We have the sequence of subgroups

$$0 = V_{-1} \subset V_0 \subset \cdots \subset V_r = \overline{X}. \tag{4-1}$$

Theorem 4.3. *The essential p-dimension of S is given by the explicit formula*

$$\mathrm{ed}_p(S) = \sum_{k=0}^{r} (\mathrm{rank}\, V_k - \mathrm{rank}\, V_{k-1})\, p^k - \dim(S).$$

Proof. Set $b_k = \mathrm{rank}(V_k)$. By Theorem 4.1, it suffices to prove that the smallest rank of the G-module P in a p-presentation of X is equal to $\sum_{k=0}^{r}(b_k - b_{k-1})p^k$.

Let $f : P \to X$ be a p-presentation of X and A a G-invariant basis of P. The set A is the disjoint union of the G-orbits A_j, so that P is the direct sum of the permutation G-modules $\mathbb{Z}[A_j]$.

The composition $\bar{f} : P \to X \to \overline{X}$ is surjective. Since G acts trivially on $\overline{X}$, the rank of the group $\bar{f}(\mathbb{Z}[A_j])$ is at most 1 for all j and $\bar{f}(\mathbb{Z}[A_j]) \subset V_k$ if $|A_j| \le p^k$. It follows that the group $\overline{X}/V_k$ is generated by the images under the composition

$$P \xrightarrow{\bar{f}} \overline{X} \to \overline{X}/V_k$$

of all $\mathbb{Z}[A_j]$ with $|A_j| > p^k$. Denote by c_k the number of such orbits A_j, so that

$$c_k \ge \mathrm{rank}(\overline{X}/V_k) = b_r - b_k.$$

Set $c'_k = b_r - c_k$, so that $b_k \ge c'_k$ for all k and $b_r = c'_r$.

Since the number of orbits A_j with $|A_j| = p^k$ is equal to $c_{k-1} - c_k$, we have

$$\begin{aligned}\mathrm{rank}(P) &= \sum_{k=0}^{r}(c_{k-1} - c_k)p^k = \sum_{k=0}^{r}(c'_k - c'_{k-1})p^k = c'_r p^r + \sum_{k=0}^{r-1} c'_k (p^k - p^{k+1}) \\ &\ge b_r p^r + \sum_{k=0}^{r-1} b_k (p^k - p^{k+1}) = \sum_{k=0}^{r}(b_k - b_{k-1})p^k.\end{aligned}$$

It remains to construct a p-presentation with P of rank $\sum_{k=0}^{r}(b_k-b_{k-1})p^k$. For every $k\geq 0$, choose a subset X_k in X of the preimage of V_k under the canonical map $X\to\overline{X}$, with the property that for any $x\in X_k$ there is a subgroup $H_x\subset G$ with $x\in X^{H_x}$, and $[G:H_x]=p^k$ such that the composition

$$X_k\to V_k\to V_k/V_{k-1}$$

yields a bijection between X_k and a basis of V_k/V_{k-1}. In particular, $|X_k|=b_k-b_{k-1}$. Consider the G-homomorphism

$$f:P:=\coprod_{k=0}^{r}\coprod_{x\in X_k}\mathbb{Z}[G/H_x]\to X,$$

taking 1 in $\mathbb{Z}[G/H_x]$ to x in X.

By construction, the composition of f with the canonical map $X\to\overline{X}$ is surjective. Since G is a p-group, the ideal $pR_{(p)}+I$ of $R_{(p)}$ is the Jacobson radical of the ring $R_{(p)}:=R\otimes\mathbb{Z}_{(p)}$. By the Nakayama Lemma, $f_{(p)}$ is surjective. Hence the cokernel of f is finite of order prime to p. The rank of the permutation G-module P is equal to

$$\sum_{k=0}^{r}\sum_{x\in X_k}p^k=\sum_{k=0}^{r}|X_k|p^k=\sum_{k=0}^{r}(b_k-b_{k-1})p^k. \qquad \square$$

Remark 4.4. In the context of finite p-groups, Theorem 4.3 was proved in [Meyer and Reichstein 2010, Theorem 1.2].

Example 4.5. Let F be a field and Φ be a subgroup of ${}_p\mathrm{Ch}(F)$ of rank r, and let $L=F(\Phi)$ and $G=\mathrm{Gal}(L/F)$. Consider the torus U^Φ with the character group the augmentation ideal I defined in Section 3.

The middle row of (3-1) yields an exact sequence

$$\overline{N}\to(\overline{R})^r\to\bar{I}\to 0.$$

It follows from Lemma 3.4 that $N\subset pR^r+I^r$, and hence the first homomorphism in the sequence is trivial. The middle group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$, and hence $\mathrm{rank}(\bar{I})=r$.

For any subgroup $H\subset G$, the Tate cohomology group $\hat{H}^0(H,I)\simeq\hat{H}^{-1}(H,\mathbb{Z})$ is trivial. It follows that the group I^H is generated by N_Hx for all $x\in I$, where $N_H=\sum_{h\in H}h\in R$. Since $\bar{I}$ is of period p with trivial G-action, the classes of the elements N_Hx in $\bar{I}$ are trivial if H is a nontrivial subgroup of G. It follows that the maps $I^H\to\bar{I}$ are trivial for all $H\neq 1$. In the notation of (4-1), $V_0=\cdots=V_{r-1}=0$ and $V_r=\bar{I}$. By Theorem 4.3,

$$\mathrm{ed}_p(U^\Phi)=rp^r-\dim(U^\Phi)=rp^r-p^r+1=(r-1)p^r+1$$

and the rank of the permutation module in a minimal p-presentation of I is equal to rp^r. Therefore, $k : R^r \to I$ is a minimal p-presentation of I that appears to be surjective. Therefore, by Corollary 4.2,

$$\mathrm{ed}(U^\Phi) = \mathrm{ed}_p(U^\Phi) = (r-1)p^r + 1. \tag{4-2}$$

Let S^Φ be the torus with the character group Q defined in Section 3. As in (3-1), the homomorphism k factors through a surjective map $R^r \to Q$ that is then necessarily a minimal p-presentation of Q. By Theorem 4.3 and Corollary 4.2,

$$\mathrm{ed}(S^\Phi) = \mathrm{ed}_p(S^\Phi) = rp^r - \dim(S^\Phi) = (r-1)p^r - r + 1. \tag{4-3}$$

5. Degeneration

In this section we study the behavior of the essential p-dimension under degeneration, that is, we compare the essential p-dimension of an object over a complete discrete valued field and its specialization over the residue field (Proposition 5.2). The iterated degeneration (Corollary 5.4) connects a class in the Brauer group degree p^r over some (large) field and the elements of the indecomposable relative Brauer group that are torsors for a certain torus.

A simple degeneration. Let F be a field, p a prime integer different from $\mathrm{char}(F)$, and $\Phi \subset {}_p\mathrm{Ch}(F)$ a finite subgroup. For an integer $k \geq 0$ and a field extension K/F, let

$$\mathcal{B}_k^\Phi(K) = \{a \in \mathrm{Br}(K)\{p\} \text{ such that } \operatorname{ind} a_{K(\Phi)} \leq p^k\}.$$

Two elements a and a' in $\mathcal{B}_k^\Phi(K)$ are *equivalent* if $a - a' \in \mathrm{Br}_{\mathrm{dec}}\big(K(\Phi)/K\big)$. Write $\mathcal{F}_k^\Phi(K)$ for the set of equivalence classes in $\mathcal{B}_k^\Phi(K)$. Abusing notation, we shall write a for the equivalence class of an element $a \in \mathcal{B}_k^\Phi(K)$ in $\mathcal{F}_k^\Phi(K)$.

We view $\mathcal{B}_k^\Phi$ and $\mathcal{F}_k^\Phi$ as functors from *Fields*$/F$ to *Sets*.

Example 5.1. (i) If Φ is the zero subgroup, then $\mathcal{F}_r^\Phi = \mathcal{B}_r^\Phi \simeq$ *CSA*$(p^r) \simeq$ $\mathbf{PGL}(p^r)$- *torsors*.

(ii) The set $\mathcal{B}_0^\Phi(K)$ is naturally bijective to $\mathrm{Br}\big(K(\Phi)/K\big)$ and

$$\mathcal{F}_0^\Phi(K) \simeq \mathrm{Br}_{\mathrm{ind}}\big(K(\Phi)/K\big).$$

By Corollary 3.7, the latter group is naturally isomorphic to $H^1(K, S^\Phi)$, where S^Φ is the torus defined in Section 3, and thus, $\mathcal{F}_0^\Phi \simeq S^\Phi$- *torsors*.

Let $\Phi' \subset \Phi$ be a subgroup of index p and $\eta \in \Phi \setminus \Phi'$; hence $\Phi = \langle \Phi', \eta \rangle$. Let E/F be a field extension such that $\eta_E \notin \Phi'_E$ in $\mathrm{Ch}(E)$. Choose an element $a \in \mathcal{B}_k^\Phi(E)$, that is, $a \in \mathrm{Br}(E)\{p\}$ and $\mathrm{ind}(a_{E(\Phi)}) \leq p^k$.

Let E' be a field extension of F that is complete with respect to a discrete valuation v' over F with residue field E, and set

$$a' = \hat{a} + \big(\hat{\eta}_E \cup (x)\big) \in \mathrm{Br}(E') \tag{5-1}$$

for some $x \in E'^{\times}$ such that $v'(x)$ is not divisible by p. By Proposition 2.2(ii), $\mathrm{ind}(a'_{E'(\Phi')}) = p \cdot \mathrm{ind}(a_{E(\Phi)}) \leq p^{k+1}$, and hence $a' \in \mathcal{B}^{\Phi'}_{k+1}(E')$.

Proposition 5.2. *Suppose that for any finite field extension N/E of degree prime to p and any character $\rho \in \mathrm{Ch}(N)$ of order p^2 such that $p \cdot \rho \in \Phi_N \setminus \Phi'_N$, we have* $\mathrm{ind}\, a_{N(\Phi',\rho)} > p^{k-1}$. *Then*

$$\mathrm{ed}_p^{\mathcal{F}^{\Phi'}_{k+1}}(a') \geq \mathrm{ed}_p^{\mathcal{F}^{\Phi}_{k}}(a) + 1.$$

Proof. Let M/E' be a finite field extension of degree prime to p, let $M_0 \subset M$ be a subfield over F, and let $a'_0 \in \mathcal{B}^{\Phi'}_{k+1}(M_0)$ be such that $(a'_0)_M = a'_M$ in $\mathcal{F}^{\Phi'}_{k+1}$ and

$$\mathrm{tr.deg}_F(M_0) = \mathrm{ed}_p^{\mathcal{F}^{\Phi'}_{k+1}}(a').$$

We have

$$a'_M - (a'_0)_M \in \mathrm{Br}_{\mathrm{dec}}\big(M(\Phi')/M\big). \tag{5-2}$$

It follows from (5-1) that

$$a'_M = \hat{a}_N + \big(\hat{\eta}_N \cup (x)\big) \tag{5-3}$$

and $\partial_{v'}(a') = q \cdot \eta_E$, where $q = v'(x)$ is relatively prime to p. We extend the discrete valuation v' on E' to a (unique) discrete valuation v on M. The ramification index e' and inertia degree are both prime to p. Thus, the residue field N of v is a finite extension of E of degree prime to p. By Proposition 2.2(iii),

$$\partial_v(a'_M) = e' \cdot \partial_{v'}(a')_N = e' q \cdot \eta_N. \tag{5-4}$$

Let v_0 be the restriction of v to M_0 and N_0 its residue field. From (5-2), we have

$$\partial_v(a'_M) - \partial_v\big((a'_0)_M\big) \in \Phi'_N. \tag{5-5}$$

Recall that $\eta_E \notin \Phi'_E$. Since $[N : E]$ is not divisible by p, it follows that

$$\eta_N \notin \Phi'_N. \tag{5-6}$$

By (5-4), (5-5) and (5-6), $\partial_v\big((a'_0)_M\big) \neq 0$, that is, $(a'_0)_M$ is ramified and therefore v_0 is nontrivial, that is, v_0 is a discrete valuation on M_0.

Let $\eta_0 := \partial_{v_0}(a'_0) \in \mathrm{Ch}(N_0)\{p\}$. By Proposition 2.2(iii),

$$\partial_v\big((a'_0)_M\big) = e \cdot (\eta_0)_N, \tag{5-7}$$

where e is the ramification index of M/M_0, and hence $(\eta_0)_N \neq 0$. It follows from (5-4), (5-5) and (5-7) that

$$e'q \cdot \eta_N - e \cdot (\eta_0)_N \in \Phi'_N. \tag{5-8}$$

Since $e'q$ is relatively prime to p,

$$\eta_N \in \langle \Phi'_N, (\eta_0)_N \rangle \quad \text{in} \quad \mathrm{Ch}(N). \tag{5-9}$$

Let p^t $(t \geq 1)$ be the order of $(\eta_0)_N$. It follows from (5-6) and (5-8) that $v_p(e) = t-1$ and

$$p^{t-1} \cdot (\eta_0)_N \in \Phi_N \setminus \Phi'_N. \tag{5-10}$$

Choose a prime element π_0 in M_0 and write

$$(a'_0)_{\widehat{M}_0} = \hat{a}_0 + \big(\hat{\eta}_0 \cup (\pi_0)\big) \tag{5-11}$$

in $\mathrm{Br}(\widehat{M}_0)$, where $a_0 \in \mathrm{Br}(N_0)\{p\}$.

Applying the specialization homomorphism $s_\pi : \mathrm{Br}(M)\{p\} \to \mathrm{Br}(N)\{p\}$ (for a prime element π in M) to (5-2), (5-3) and (5-11), using (2-3) and (5-9), we get

$$a_N - (a_0)_N \in \mathrm{Br}_{\mathrm{dec}}\big(N(\Phi', \eta_0)/N\big). \tag{5-12}$$

It follows from (5-12) that

$$a_{N(\Phi',\eta_0)} = (a_0)_{N(\Phi',\eta_0)} \tag{5-13}$$

in $\mathrm{Br}\big(N(\Phi', \eta_0)\big)$.

By (5-11),

$$(a'_0)_{\widehat{M}_0(\Phi')} = \widehat{(a_0)}_{N_0(\Phi')} + \big(\widehat{(\eta_0)}_{N_0(\Phi')} \cup (\pi_0)\big).$$

Since no nontrivial multiple of $(\eta_0)_N$ belongs to Φ'_N, by (5-10), the order of the character $(\eta_0)_{N_0(\Phi')}$ is at least p^t. It follows from Proposition 2.2(ii) that

$$\mathrm{ind}(a_0)_{N_0(\Phi',\eta_0)} = \mathrm{ind}(a'_0)_{\widehat{M}_0(\Phi')} / \mathrm{ord}(\eta_0)_{N_0(\Phi')} \leq p^{k+1}/p^t = p^{k-t+1}. \tag{5-14}$$

By (5-13) and (5-14),

$$\mathrm{ind}(a_{N(\Phi',\eta_0)}) \leq p^{k-t+1}. \tag{5-15}$$

Suppose that $t \geq 2$, and consider the character $\rho = p^{t-2} \cdot (\eta_0)_N$ of order p^2 in $\mathrm{Ch}(N)$. We have $p \cdot \rho = p^{t-1}(\eta_0)_N \in \Phi_N \setminus \Phi'_N$, by (5-10). Also, the degree of the field extension $N(\Phi', \eta_0)/N(\Phi', \rho)$ is equal to p^{t-2}. Hence, by (5-15),

$$\mathrm{ind}(a_{N(\Phi',\rho)}) \leq \mathrm{ind}(a_{N(\Phi',\eta_0)}) \cdot p^{t-2} \leq p^{k-t+1} \cdot p^{t-2} = p^{k-1}.$$

This contradicts the assumption. Therefore, $t = 1$, that is, $\mathrm{ord}(\eta_0)_N = p$. Then $(e, p) = 1$ and it follows from (5-8) that $(\eta_0)_N \in \langle \Phi'_N, \eta_N \rangle$. Moreover,

$$\langle \Phi', \eta_0 \rangle_N = \langle \Phi', \eta \rangle_N = \Phi_N. \tag{5-16}$$

There is a finite subextension N_1/N_0 of N/N_0 such that $\langle\Phi', \eta_0\rangle_{N_1} = \Phi_{N_1}$, by Lemma 2.1. Replacing N_0 by N_1 and a_0 by $(a_0)_{N_1}$, we may assume that $\langle\Phi', \eta_0\rangle_{N_0} = \Phi_{N_0}$. In particular, η_0 is of order p in $\mathrm{Ch}(N_0)$.

Since $\mathrm{ind}(a_0)_{N_0(\Phi)} = \mathrm{ind}(a_0)_{N_0(\Phi',\eta_0)} \le p^k$ by (5-14), we have $a_0 \in \mathcal{B}_k^{\Phi}(N_0)$.

It follows from (5-12) that

$$a_N - (a_0)_N \in \mathrm{Br}_{\mathrm{dec}}\big(N(\Phi)/N\big).$$

Hence the classes of a_N and $(a_0)_N$ are equal in $\mathcal{F}_k^{\Phi}(N)$. The class of a_N in $\mathcal{F}_k^{\Phi}(N)$ is then defined over N_0, and therefore

$$\mathrm{ed}_p^{\mathcal{F}_{k+1}^{\Phi'}}(a') = \mathrm{tr.deg}_F(M_0) \ge \mathrm{tr.deg}_F(N_0) + 1 \ge \mathrm{ed}_p^{\mathcal{F}_k^{\Phi}}(a) + 1. \qquad \square$$

5.1. *Multiple degeneration.* In this section we assume that the base field F contains a primitive p^2-th root of unity.

Let $\chi_1, \chi_2, \dots, \chi_r$ be linearly independent characters in ${}_p\mathrm{Ch}(F)$, and let $\Phi = \langle\chi_1, \chi_2, \dots, \chi_r\rangle$. Let E/F be a field extension such that $\mathrm{rank}(\Phi_E) = r$ and let $a \in \mathrm{Br}(E)\{p\}$ be an element that is split by $E(\Phi)$.

Let $E_0 = E, E_1, \dots, E_r$ be field extensions of F such that for any $k = 1, 2, \dots, r$, the field E_k is complete with respect to a discrete valuation v_k over F and E_{k-1} is its residue field. For any $k = 1, 2, \dots, r$, choose elements $x_k \in E_k^{\times}$ such that $v_k(x_k)$ is not divisible by p, and define the elements $a_k \in \mathrm{Br}(E_k)\{p\}$ inductively by $a_0 = a$ and

$$a_k = \widehat{a_{k-1}} + \big(\widehat{(\chi_k)}_{E_{k-1}} \cup (x_k)\big).$$

Let Φ_k be the subgroup of Φ generated by $\chi_{k+1}, \dots, \chi_r$. Thus, $\Phi_0 = \Phi$, $\Phi_r = 0$ and $\mathrm{rank}(\Phi_k) = r - k$. Note that the character $(\chi_k)_{E_{k-1}(\Phi_k)}$ is not trivial. It follows from Proposition 2.2(ii) that

$$\mathrm{ind}(a_k)_{E_k(\Phi_k)} = p \cdot \mathrm{ind}(a_{k-1})_{E_{k-1}(\Phi_{k-1})}$$

for any $k = 1, \dots, r$. Since $\mathrm{ind}\, a_{E(\Phi)} = 1$, we have $\mathrm{ind}(a_k)_{E_k(\Phi_k)} = p^k$ for all $k = 0, 1, \dots, r$. In particular, $a_k \in \mathcal{B}_k^{\Phi_k}(E_k)$.

The following lemma assures that under a certain restriction on the element a, the conditions of Proposition 5.2 are satisfied for the fields E_k, the groups of characters Φ_k, and the elements a_k.

Lemma 5.3. *Suppose that $a_{E(\Psi)} \notin \mathrm{Im}\big(\mathrm{Br}\, F(\Psi) \to \mathrm{Br}\, E(\Psi)\big)$ for any proper subgroup $\Psi \subset \Phi$. Then for every $k = 0, 1, \dots, r-1$, and any finite field extension N/E_k of degree prime to p and any character $\rho \in \mathrm{Ch}(N)$ of order p^2 such that $p \cdot \rho \in (\Phi_k)_N \setminus (\Phi_{k+1})_N$, we have*

$$\mathrm{ind}(a_k)_{N(\Phi_{k+1},\rho)} > p^{k-1}. \tag{5-17}$$

Proof. Let $k=0,1,\dots,r-1$ and N/E_k be a finite field extension of degree prime to p. We construct a new sequence of fields $\tilde{E}_0, \tilde{E}_1, \dots, \tilde{E}_r$ such that each $\tilde{E}_i$ is a finite extension of E_i of degree prime to p as follows. We set $\tilde{E}_j = N$. The fields $\tilde{E}_j$ with $j<k$ are constructed by descending induction on j. If we have constructed $\tilde{E}_j$ as a finite extension of E_j of degree prime to p, then we extend the valuation v_j to $\tilde{E}_j$ and let $\tilde{E}_{j-1}$ be its residue field. The fields $\tilde{E}_j$ with $j>k$ are constructed by induction on j. If we have constructed $\tilde{E}_j$ as a finite extension of E_j of degree prime to p, then let $\tilde{E}_{j+1}$ be an extension of E_{j+1} of degree $[\tilde{E}_j : E_j]$ with residue field $\tilde{E}_j$.

Replacing E_i by $\tilde{E}_i$ and a_i by $(a_i)_{\tilde{E}_i}$, we may assume that $N=E_k$. Let $\rho\in \operatorname{Ch}(E_k)$ be a character of order p^2. We prove the inequality (5-17) by induction on r. The case $r=1$ is obvious. Suppose first that $k<r-1$. Consider the fields $F'=F(\chi_r)$, $E'=E(\chi_r)$, $E'_i=E_i(\chi_r)$, the sequence of characters $\chi'_i=(\chi_i)_{F'}$, and the sequence of elements $a'_i := (a_i)_{E'_i}\in \operatorname{Br}(E'_i)$ for $i=0,1,\dots,r-1$. Let $\Phi' = \langle \chi'_1, \chi'_2, \dots, \chi'_{r-1}\rangle$ and let Φ'_k be the subgroup of Φ' generated by $\chi'_{k+1},\dots,\chi'_{r-1}$.

Let $\Psi'\subset\Phi'$ be a proper subgroup. Then $\Psi := \Psi' + \langle\chi_r\rangle$ is a proper subgroup of Φ. Since $F(\Psi)=F'(\Psi')$ and $E(\Psi)=E'(\Psi')$, we have

$$a_{E'(\Psi')}\notin \operatorname{Im}\bigl(\operatorname{Br} F'(\Psi')\to \operatorname{Br} E'(\Psi')\bigr).$$

By induction, the inequality (5-17) holds for the term a'_k of the new sequence. Since

$$(a'_k)_{E'_k(\Phi'_{k+1},\rho)} = (a_k)_{E_k(\Phi_{k+1},\rho)},$$

the inequality (5-17) holds for the term a_k.

Thus we can assume that $k=r-1$.

Case 1. The character ρ is unramified with respect to v_{r-1}, that is, $\rho=\hat{\mu}$ for a character $\mu\in\operatorname{Ch}(E_{r-2})$ of order p^2. By Lemma 2.3(i),

$$\operatorname{ind}(a_{r-2})_{E_{r-2}(\chi_{r-1},\mu)} = \operatorname{ind}(a_{r-1})_{E_{r-1}(\rho)}/p = \operatorname{ind}(a_{r-1})_{E_{r-1}(\Phi_r,\rho)}/p. \tag{5-18}$$

Consider the fields $F'=F(\chi_{r-1})$, $E'=E(\chi_{r-1})$, $E'_i=E_i(\chi_{r-1})$, the new sequence of characters $\chi_1,\dots,\chi_{r-2},\chi_r$ and the elements $a'_i\in\operatorname{Br}(E'_i)$ for $i=0,1,\dots,r-1$ defined by $a'_i=(a_i)_{E'_i}$ for $i\le r-2$ and $a'_{r-1}=\hat{a}_{r-2}+\bigl(\hat{\chi}_r\cup(x_{r-1})\bigr)$ over E'_{r-1}.

Let $\Phi'=\langle\chi_1,\dots,\chi_{r-2},\chi_r\rangle$ and $\Psi'\subset\Phi'$ be a proper subgroup. Then $\Psi := \Psi'+\langle\chi_{r-1}\rangle$ is a proper subgroup of Φ. Since $F(\Psi)=F'(\Psi')$ and $E(\Psi)=E'(\Psi')$, we have $a_{E'(\Psi')}\notin\operatorname{Im}\bigl(\operatorname{Br} F'(\Psi')\to\operatorname{Br} E'(\Psi')\bigr)$. By induction, the inequality (5-17) holds for the term a'_{r-2} of the new sequence, the field $N=E'_{r-2}$, and the character μ_N. Since

$$(a'_{r-2})_{E'_{r-2}(\mu)} = (a_{r-2})_{E_{r-2}(\chi_{r-1},\mu)},$$

the equality (5-18) shows that (5-17) holds for a_{r-1}.

Case 2. The character ρ is ramified. Note that $p\cdot\rho$ is a nonzero multiple of $(\chi_r)_{E_{r-1}}$. Suppose the inequality (5-17) fails for a_{r-1}, that is, we have

$$\operatorname{ind}(a_{r-1})_{E_{r-1}(\rho)} \le p^{r-2}.$$

By Lemma 2.3(ii), there exists a unit $u\in E_{r-1}$ such that $E_{r-2}(\chi_r)=E_{r-2}(\bar{u}^{1/p})$ and

$$\operatorname{ind}\bigl(a_{r-2}-(\chi_{r-1}\cup(\bar{u}^{1/p}))\bigr)_{E_{r-2}(\chi_r)} = \operatorname{ind}(a_{r-1})_{E_{r-1}(\rho)} \le p^{r-2}.$$

By descending induction on $j=0,1,\dots,r-2$, we show that there exist a unit u_j in E_{j+1} and a subgroup $\Theta_j\subset\Phi$ of rank $r-j-1$ such that $\chi_r\in\Theta_j$, $\langle\chi_1,\dots,\chi_j,\chi_{r-1}\rangle\cap\Theta_j=0$, $E_j(\chi_r)=E_j(\bar{u}_j^{1/p})$, and

$$\operatorname{ind}\bigl(a_j-(\chi_{r-1}\cup(\bar{u}_j^{1/p}))\bigr)_{E_j(\Theta_j)} \le p^j. \tag{5-19}$$

If $j=r-2$, we set $u_j=u$ and $\Theta_j=\langle\chi_r\rangle$.

($j\Rightarrow j-1$): The field $E_j(\bar{u}_j^{1/p})=E_j(\chi_r)$ is unramified over E_j, and hence $v_j(\bar{u}_j)$ is divisible by p. Modifying u_j by a p^2-th power, we may assume that $\bar{u}_j=u_{j-1}x_j^{mp}$ for a unit $u_{j-1}\in E_j$ and an integer m. Then

$$\bigl(a_j-(\chi_{r-1}\cup(\bar{u}_j^{1/p}))\bigr)_{E_j(\Theta_j)} = \hat{b}+\bigl(\hat{\eta}\cup(x_j)\bigr)_{E_j(\Theta_j)},$$

where $\eta=\chi_j-m\chi_{r-1}$ and $b=\bigl(a_{j-1}-(\chi_{r-1}\cup(\bar{u}_{j-1}^{1/p}))\bigr)_{E_{j-1}(\Theta_j)}$. Since η is not contained in Θ_j, the character $\eta_{E_{j-1}(\Theta_j)}$ is not trivial. Set $\Theta_{j-1}=\langle\Theta_j,\eta\rangle$. It follows from Proposition 2.2(ii) that

$$\operatorname{ind}(b_{E_{j-1}(\Theta_{j-1})}) = \operatorname{ind}\bigl(a_j-(\chi_{r-1}\cup(\bar{u}_j^{1/p}))\bigr)_{E_j(\Theta_j)}/p \le p^{j-1}.$$

Applying the inequality (5-19) in the case $j=0$, we get

$$a_{E(\Theta_0)} = \bigl(\chi_{r-1}\cup(w^{1/p})\bigr)_{E(\Theta_0)}$$

for an element $w\in E^\times$ such that $E(w^{1/p})=E(\chi_r)$. Since the character χ_r is defined over F, we may assume that $w\in F^\times$, and therefore

$$a_{E(\Theta_0)}\in\operatorname{Im}\bigl(\operatorname{Br}F(\Theta_0)\to\operatorname{Br}E(\Theta_0)\bigr).$$

The degree of the extension $E(\Theta_0)/E$ is equal to p^{r-1}, and hence Θ_0 is a proper subgroup of Φ, a contradiction. Thus, we have shown that the inequality (5-17) holds. □

By Example 5.1(ii), we can view a as an S^Φ-torsor over E.

Corollary 5.4. *Suppose that $p^{r-1}a\notin\operatorname{Im}\bigl(\operatorname{Br}(F)\to\operatorname{Br}(E)\bigr)$. Then*

$$\operatorname{ed}_p^{\mathit{CSA}(p^r)}(a_r) \ge \operatorname{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a)+r.$$

Proof. By iterated application of Proposition 5.2 and Example 5.1,

$$\begin{aligned}\mathrm{ed}_p^{CSA(p^r)}(a_r) &= \mathrm{ed}_p^{\mathcal{F}_r^{\Phi_r}}(a_r) \geq \mathrm{ed}_p^{\mathcal{F}_{r-1}^{\Phi_{r-1}}}(a_{r-1}) + 1 \geq \dots \\ &\geq \mathrm{ed}_p^{\mathcal{F}_1^{\Phi_1}}(a_1) + (r-1) \geq \mathrm{ed}_p^{\mathcal{F}_0^{\Phi_0}}(a_0) + r = \mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) + r. \qquad \square\end{aligned}$$

6. Proof of the main theorem

Theorem 6.1. *Let F be a field and p a prime integer different from* $\mathrm{char}(F)$. *Then*

$$\mathrm{ed}_p\big(CSA(p^r)\big) \geq (r-1)p^r + 1.$$

Proof. Since $\mathrm{ed}_p\big(CSA(p^r)\big)$ can only go down if we replace the base field F by any field extension [Merkurjev 2009, Proposition 1.5], we can replace F by any field extension. In particular, we may assume that F contains a primitive p^2-th root of unity and that there is a subgroup Φ of ${}_p\mathrm{Ch}(F)$ of rank r (replacing F by the field of rational functions in r variables over F).

Let T^Φ be the algebraic torus constructed in Section 3 for the subgroup Φ. Set $E = F(T^\Phi)$, and let $a \in \mathrm{Br}(EL/E)$ be the element defined in Section 3.1. Let $a_r \in \mathrm{Br}(E_r)$ be the element of index p^r constructed in Section 5.1. By Corollary 3.9, the class $p^{r-1}a$ in $\mathrm{Br}(E)$ does not belong to the image of $\mathrm{Br}(F) \to \mathrm{Br}(E)$. It follows from Corollary 5.4 that

$$\mathrm{ed}_p^{CSA(p^r)}(a_r) \geq \mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) + r. \tag{6-1}$$

The S^Φ-torsor a is the generic fiber of the versal S^Φ-torsor $P^\Phi \to T^\Phi$ (see Example 3.3), and hence a is a generic torsor. By [Reichstein and Youssin 2000, §6] or [Merkurjev 2009, Theorem 2.9],

$$\mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) = \mathrm{ed}_p(S^\Phi). \tag{6-2}$$

The essential p-dimension of S^Φ was calculated in (4-3):

$$\mathrm{ed}_p(S^\Phi) = (r-1)p^r - r + 1. \tag{6-3}$$

Finally, it follows from (6-1), (6-2) and (6-3) that

$$\mathrm{ed}_p\big(CSA(p^r)\big) \geq \mathrm{ed}_p^{CSA(p^r)}(a_r) \geq \mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) + r = (r-1)p^r + 1. \qquad \square$$

7. Remarks

Let K/F be a field extension and G an elementary abelian group of order p^r. Consider the subset $CSA_K(G)$ of $CSA_K(p^r)$ consisting of all classes admitting a splitting Galois K-algebra E with $\mathrm{Gal}(E/K) \simeq G$. Equivalently, $CSA_K(G)$

consists of all classes represented by crossed product algebras with the group G [Herstein 1994, §4.4].

Write $\mathit{Pair}_K(G)$ for the set of isomorphism classes of pairs (a, E), where $a \in \mathit{CSA}_K(G)$ and E is a Galois G-algebra splitting a.

Finally, fix a Galois field extension L/F with $\mathrm{Gal}(L/F) \simeq G$ and consider the subset $\mathit{CSA}_K(L/F)$ of $\mathit{CSA}_K(G)$ consisting of all classes split by the extension KL/K. Thus, $\mathit{CSA}(L/F)$ is a subfunctor of $\mathit{CSA}(G)$ and there is the obvious surjective morphism of functors $\mathit{Pair}(G) \to \mathit{CSA}(G)$.

Theorem 7.1. *Let F be a field, p a prime integer different from* $\mathrm{char}(F)$, *G an elementary abelian group of order p^r, $r \geq 2$, and L/F a Galois field extension with* $\mathrm{Gal}(L/F) \simeq G$. *Let $\mathcal{F}$ be one of the three functors $\mathit{CSA}(L/F)$, $\mathit{CSA}(G)$, $\mathit{Pair}(G)$. Then*

$$\mathrm{ed}(\mathcal{F}) = \mathrm{ed}_p(\mathcal{F}) = (r-1)p^r + 1.$$

Proof. The functor $\mathit{CSA}(L/F)$ is isomorphic to U^{Φ}-*torsors* by (3-4), where Φ is a subgroup of $\mathrm{Ch}(F)$ such that $L = F(\Phi)$. It follows from (4-2) that

$$\mathrm{ed}\big(\mathit{CSA}(L/F)\big) = \mathrm{ed}_p\big(\mathit{CSA}(L/F)\big) = (r-1)p^r + 1.$$

Let a_r be the element in $\mathrm{Br}(E_r)$ in the proof of Theorem 6.1. It satisfies

$$\mathrm{ed}_p^{\mathit{CSA}(p^r)}(a_r) \geq (r-1)p^r + 1.$$

By construction, $a_r \in \mathit{CSA}_{E_r}(G)$. Since $\mathit{CSA}(G)$ is a subfunctor of $\mathit{CSA}(p^r)$, we have

$$\mathrm{ed}_p\big(\mathit{CSA}(G)\big) \geq \mathrm{ed}_p^{\mathit{CSA}(G)}(a_r) \geq \mathrm{ed}_p^{\mathit{CSA}(p^r)}(a_r) \geq (r-1)p^r + 1.$$

The upper bound $\mathrm{ed}\big(\mathit{CSA}(G)\big) \leq (r-1)p^r + 1$ was proven in [Lorenz et al. 2003, Corollary 3 10].

The split étale F-algebra $E := \mathrm{Map}(G, F)$ has the natural structure of a Galois G-algebra over F. The group G acts on the split torus $U := R_{E/F}(\mathbb{G}_{m,E})/\mathbb{G}_m$. Let A be the split F-algebra $\mathrm{End}_F(E)$. The semidirect product $H := U \rtimes G$ acts naturally on A by F-algebra automorphisms. Moreover, by the Skolem–Noether Theorem, H is precisely the automorphism group of the pair (A, E). It follows that the functor $\mathit{Pair}_K(G)$ is isomorphic to H-*torsors*.

The character group of U is G-isomorphic to the ideal I in $R = \mathbb{Z}[G]$. By [Meyer and Reichstein 2009a, §3], the G-homomorphism $k : R^r \to I$ constructed in Section 3 yields a representation W of the group H of dimension rp^r. Since $r \geq 2$, by Lemma 3.4, G acts faithfully on the kernel N of k. By [Meyer and Reichstein 2009a, Lemma 3.3], the action of H on W is generically free, and hence

$$\mathrm{ed}\big(\mathit{Pair}(G)\big) = \mathrm{ed}(H) \leq \dim(W) - \dim(H) = (r-1)p^r + 1.$$

Since $Pair(G)$ surjects onto $CSA(G)$, we have

$$\mathrm{ed}\big(Pair(G)\big) \geq \mathrm{ed}_p\big(Pair(G)\big) \geq \mathrm{ed}_p\big(CSA(G)\big) = (r-1)p^r + 1. \qquad \square$$

Remark 7.2. The generic G-crossed product algebra D constructed in [Amitsur and Saltman 1978] is a generic element for the functor $CSA(G)$ in the sense of [Merkurjev 2009, §2], and hence

$$\mathrm{ed}(D) = \mathrm{ed}_p(D) = (r-1)p^r + 1$$

for $r \geq 2$ by Theorem 7.1.

References

[Amitsur and Saltman 1978] S. A. Amitsur and D. Saltman, "Generic Abelian crossed products and p-algebras", *J. Algebra* **51**:1 (1978), 76–87. MR 58 #10988 Zbl 0391.13001

[Berhuy and Favi 2003] G. Berhuy and G. Favi, "Essential dimension: a functorial point of view (after A. Merkurjev)", *Doc. Math.* **8** (2003), 279–330. MR 2004m:11056 Zbl 1101.14324

[Cartan and Eilenberg 1999] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, 1999. MR 2000h:18022 Zbl 0933.18001

[Colliot-Thélène and Sansuc 1977] J.-L. Colliot-Thélène and J.-J. Sansuc, "La R-équivalence sur les tores", *Ann. Sci. École Norm. Sup.* (4) **10**:2 (1977), 175–229. MR 56 #8576 Zbl 0356.14007

[Garibaldi et al. 2003] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series **28**, American Mathematical Society, Providence, RI, 2003. MR 2004f:11034 Zbl 1159.12311

[Herstein 1994] I. N. Herstein, *Noncommutative rings*, Carus Mathematical Monographs **15**, Mathematical Association of America, Washington, DC, 1994. MR 97m:16001 Zbl 0874.16001

[Jacob and Wadsworth 1990] B. Jacob and A. Wadsworth, "Division algebras over Henselian fields", *J. Algebra* **128**:1 (1990), 126–179. MR 91d:12006 Zbl 0692.16011

[Lorenz et al. 2003] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman, "Fields of definition for division algebras", *J. London Math. Soc.* (2) **68**:3 (2003), 651–670. MR 2004j:16022 Zbl 1071.16012

[Lötscher et al. 2009] R. Lötscher, M. MacDonald, A. Meyer, and R. Reichstein, "Essential p-dimension of algebraic tori", preprint, 2009. arXiv 0910.5574v1

[Matsumura 1980] H. Matsumura, *Commutative algebra*, 2nd ed., Mathematics Lecture Note Series **56**, Benjamin/Cummings, Reading, MA, 1980. MR 82i:13003 Zbl 0441.13001

[Merkurjev 2009] A. S. Merkurjev, "Essential dimension", pp. 299–325 in *Quadratic forms: algebra, arithmetic, and geometry*, edited by R. Baeza et al., Contemp. Math. **493**, Amer. Math. Soc., Providence, RI, 2009. MR 2010i:14014 Zbl 1188.14006

[Merkurjev 2010] A. S. Merkurjev, "Essential p-dimension of $\mathrm{PGL}(p^2)$", *J. Amer. Math. Soc.* **23** (2010), 693–712. Zbl 05775681

[Meyer and Reichstein 2009a] A. Meyer and Z. Reichstein, "The essential dimension of the normalizer of a maximal torus in the projective linear group", *Algebra Number Theory* **3**:4 (2009), 467–487. MR 2010h:11065 Zbl 05588054

[Meyer and Reichstein 2009b] A. Meyer and Z. Reichstein, "An upper bound on the essential dimension of a central simple algebra", preprint, 2009, Available at www.math.ubc.ca/~reichst/meyer-reichstein3.pdf. To appear in *J. Algebra*.

[Meyer and Reichstein 2010] A. Meyer and Z. Reichstein, "Some consequences of the Karpenko–Merkurjev theorem", *Docum. Math.* extra vol. (2010), 445–457. Zbl 05827449

[Reichstein 2000] Z. Reichstein, "On the notion of essential dimension for algebraic groups", *Transform. Groups* **5**:3 (2000), 265–304. MR 2001j:20073 Zbl 0981.20033

[Reichstein and Youssin 2000] Z. Reichstein and B. Youssin, "Essential dimensions of algebraic groups and a resolution theorem for G-varieties", *Canad. J. Math.* **52**:5 (2000), 1018–1056. MR 2001k:14088 Zbl 1044.14023

[Serre 1997] J.-P. Serre, *Galois cohomology*, Springer, Berlin, 1997. MR 98g:12007 Zbl 0902.12004

[Tignol 1978] J.-P. Tignol, "Sur les classes de similitude de corps à involution de degré 8", *C. R. Acad. Sci. Paris Sér. A-B* **286**:20 (1978), A875–A876. MR 58 #16605 Zbl 0374.16006

Communicated by Raman Parimala
Received 2009-11-27 Revised 2010-03-30 Accepted 2010-05-15

merkurev@math.ucla.edu *Department of Mathematics, University of California, Los Angeles, CA 90095-1555, United States*

ALGEBRA AND NUMBER THEORY 4:8(2010)

On the minimal ramification problem for semiabelian groups

Hershy Kisilevsky, Danny Neftin and Jack Sonn

It is now known that for any prime p and any finite semiabelian p-group G, there exists a (tame) realization of G as a Galois group over the rationals $\mathbb{Q}$ with exactly $d = \mathrm{d}(G)$ ramified primes, where $\mathrm{d}(G)$ is the minimal number of generators of G, which solves the minimal ramification problem for finite semiabelian p-groups. We generalize this result to obtain a theorem on finite semiabelian groups and derive the solution to the minimal ramification problem for a certain family of semiabelian groups that includes all finite nilpotent semiabelian groups G. Finally, we give some indication of the depth of the minimal ramification problem for semiabelian groups not covered by our theorem.

1. Introduction

Let G be a finite group. Let $d = \mathrm{d}(G)$ be the smallest number for which there exists a subset S of G with d elements such that the normal subgroup of G generated by S is all of G. One observes that if G is realizable as a Galois group $G(K/\mathbb{Q})$ with $K/\mathbb{Q}$ tamely ramified (e.g., if none of the ramified primes divide the order of G), then at least $\mathrm{d}(G)$ rational primes ramify in K (see, e.g., [Kisilevsky and Sonn 2010]). The *minimal ramification problem for G* is to realize G as the Galois group of a tamely ramified extension $K/\mathbb{Q}$ in which exactly $\mathrm{d}(G)$ rational primes ramify. This variant of the inverse Galois problem is open even for p-groups, and no counterexample has been found. It is known that the problem has an affirmative solution for all semiabelian p-groups, for all rational primes p [Neftin 2009; Kisilevsky and Sonn 2010]. A finite group G is *semiabelian* if and only if $G \in \mathcal{SA}$, where $\mathcal{SA}$ is the smallest family of finite groups satisfying (i) every finite abelian group belongs to $\mathcal{SA}$, (ii) if $G \in \mathcal{SA}$ and A is finite abelian, then any semidirect product $A \rtimes G$ belongs to $\mathcal{SA}$, and (iii) if $G \in \mathcal{SA}$, then every homomorphic image of G belongs to $\mathcal{SA}$. In this paper we generalize this result to arbitrary finite semiabelian groups by means of a "wreath product length" $\mathrm{wl}(G)$ of a finite semiabelian group G. When a

Kisilevsky's research was supported in part by a grant from the NSERC.
MSC2000: primary 11R32; secondary 20D15.
Keywords: Galois group, nilpotent group, ramified primes, wreath product, semiabelian group.

finite semiabelian group G is nilpotent, $\mathrm{wl}(G) = \mathrm{d}(G)$, which for nilpotent groups G equals the (more familiar) minimal number of generators of G. Thus the general result does not solve the minimal ramification problem for all finite semiabelian groups, but does specialize to an affirmative solution to the minimal ramification problem for nilpotent semiabelian groups. Note that for a nilpotent group G, $\mathrm{d}(G)$ is $\max_{p\,|\,|G|} \mathrm{d}(G_p)$ and not $\sum_{p\,|\,|G|} \mathrm{d}(G_p)$, where G_p is the p-Sylow subgroup of G. Thus, a solution to the minimal ramification problem for nilpotent groups does not follow trivially from the solution for p-groups.

2. Properties of wreath products

2.1. *Functoriality.* The family of semiabelian groups can also be defined using wreath products. Let us recall the definition of a wreath product. Here and throughout the text the actions of groups on sets are all right actions.

Definition 2.1. Let G and H be two groups that act on the sets X and Y, respectively. The (*permutational*) *wreath product* $H \wr_X G$ is the set $H^X \times G = \{(f, g) \mid f : X \to H, g \in G\}$ which is a group with respect to the multiplication

$$(f_1, g_1)(f_2, g_2) = (f_1 f_2^{g_1^{-1}}, g_1 g_2),$$

where $f_2^{g_1^{-1}}$ is defined by $f_2^{g_1^{-1}}(x) = f_2(x g_1)$ for any $g_1, g_2 \in G$, $f_1, f_2 : X \to H$, and $x \in X$. The group $H \wr_X G$ acts on the set $Y \times X$ by $(y, x) \cdot (f, g) = (y f(x), xg)$, for any $y \in Y$, $x \in X$, $f : X \to H$, $g \in G$.

Definition 2.2. The *standard* (or *regular*) *wreath product* $H \wr G$ is defined as the permutational wreath product with $X = G$, $Y = H$, and the right regular actions.

The functoriality of the arguments of a wreath product will play an important role in the sequel. The following five lemmas are devoted to these functoriality properties.

Definition 2.3. Let G be a group that acts on X and Y. A map $\phi : X \to Y$ is called a G-map if $\phi(xg) = \phi(x)g$ for every $g \in G$ and $x \in X$.

Note that for such ϕ, we also have $\phi^{-1}(y)g = \{xg \mid \phi(x) = y\} = \{x' \mid \phi(x'g^{-1}) = y\} = \{x' \mid \phi(x') = yg\} = \phi^{-1}(yg)$.

Lemma 2.4. *Let G be a group that acts on the finite sets X, Y and let A be an abelian group. Then every G-map $\phi : X \to Y$ induces a homomorphism $\tilde{\phi} : A \wr_X G \to A \wr_Y G$ by defining $(\tilde{\phi}(f, g)) = (\hat{\phi}(f), g)$ for every $f : X \to A$ and $g \in G$, where $\hat{\phi}(f) : Y \to A$ is defined by*

$$\hat{\phi}(f)(y) = \prod_{x \in \phi^{-1}(y)} f(x),$$

for every $y \in Y$. Furthermore, if ϕ is surjective then $\tilde{\phi}$ is an epimorphism.

Proof. Let us show the above $\tilde{\phi}$ is indeed a homomorphism. For this we claim $\tilde{\phi}((f_1, g_1)(f_2, g_2)) = \tilde{\phi}(f_1, g_1)\tilde{\phi}(f_2, g_2)$ for every $g_1, g_2 \in G$ and $f_1, f_2 : X \to A$. By definition:

$$\tilde{\phi}(f_1, g_1)\tilde{\phi}(f_2, g_2) = (\hat{\phi}(f_1), g_1)(\hat{\phi}(f_2), g_2) = (\hat{\phi}(f_1)\hat{\phi}(f_2)^{g_1^{-1}}, g_1g_2),$$

while $\tilde{\phi}((f_1, g_1)(f_2, g_2)) = \tilde{\phi}(f_1 f_2^{g_1^{-1}}, g_1g_2) = (\hat{\phi}(f_1 f_2^{g_1^{-1}}), g_1g_2)$. We shall show that $\hat{\phi}(f_1 f_2) = \hat{\phi}(f_1)\hat{\phi}(f_2)$ and $\hat{\phi}(f^g) = \hat{\phi}(f)^g$ for every $f_1, f_2, f : X \to A$ and $g \in G$. Clearly this will imply the claim. The first assertion follows since

$$\hat{\phi}(f_1 f_2)(y) = \prod_{x\in\phi^{-1}(y)} f_1(x) f_2(x) = \prod_{x\in\phi^{-1}(y)} f_1(x) \prod_{x\in\phi^{-1}(y)} f_2(x) = \hat{\phi}(f_1)(y)\hat{\phi}(f_2)(y).$$

As to the second assertion we have

$$\hat{\phi}(f^g)(y) = \prod_{x\in\phi^{-1}(y)} f^g(x) = \prod_{x\in\phi^{-1}(y)} f(xg^{-1}) = \prod_{x'g\in\phi^{-1}(y)} f(x') = \prod_{x'\in\phi^{-1}(y)g^{-1}} f(x').$$

Since ϕ is a G-map we have $\phi^{-1}(y)g^{-1} = \phi^{-1}(yg^{-1})$ and thus

$$\hat{\phi}(f^g)(y) = \prod_{x\in\phi^{-1}(y)g^{-1}} f(x) = \prod_{x\in\phi^{-1}(yg^{-1})} f(x) = \hat{\phi}(f)^g(y).$$

This proves the second assertion and hence the claim. It is left to show that if ϕ is surjective then $\tilde{\phi}$ is surjective. Let $f' : Y \to A$ and $g' \in G$. Let us define an $f : X \to A$ that will map to f'. For every $y \in Y$ choose an element $x_y \in X$ for which $\phi(x_y) = y$ and define $f(x_y) := f'(y)$. Define $f(x) = 1$ for any $x \notin \{x_y \mid y \in Y\}$. Then clearly

$$\hat{\phi}(f)(y) = \prod_{x\in\phi^{-1}(y)} f(x) = f(x_y) = f'(y).$$

Thus, $\tilde{\phi}(f, g') = (\hat{\phi}(f), g') = (f', g')$ and $\tilde{\phi}$ is onto. □

Lemma 2.5. *Let B and C be two groups. Then there is a surjective $B \wr C$-map $\phi : B \wr C \to B \times C$ defined by $\phi(f, c) = (f(1), c)$ for every $f : C \to B, c \in C$.*

Proof. Let $(f, c), (f', c')$ be two elements of $B \wr C$. We check that $\phi((f, c)(f', c')) = \phi(f, c)(f', c')$. Indeed,

$$\begin{aligned}\phi((f, c)(f', c')) &= \phi(ff'^{c^{-1}}, cc') = (f(1)f'^{c^{-1}}(1), cc') = (f(1)f'(c), cc') \\ &= (f(1), c)(f', c) = \phi(f, c)(f', c').\end{aligned}$$

Note that the map ϕ is surjective: For every $b \in B$ and $c \in C$, one can choose a function $f_b : C \to B$ for which $f_b(1) = b$. One has $\phi(f_b, c) = (b, c)$. □

The following lemma appears in [Meldrum 1995, Part I, Chapter I, Theorem 4.13] and describes the functoriality of the first argument in the wreath product.

Lemma 2.6. *Let G, A, B be groups and $h : A \to B$ a homomorphism* (*resp. epimorphism*)*. Then there is a naturally induced homomorphism* (*resp. epimorphism*) *$h_* : A \wr G \to B \wr G$ given by $h_*(f, g) = (h \circ f, g)$ for every $g \in G$ and $f : G \to A$.*

The functoriality of the second argument is given in [Neftin 2009, Lemma 2.15] whenever the first argument is abelian:

Lemma 2.7. *Let A be an abelian group and let $\psi : G \to H$ be a homomorphism* (*resp. epimorphism*) *of finite groups. Then there is a homomorphism* (*resp. epimorphism*) *$\tilde{\psi} : A \wr G \to A \wr H$ that is defined by $\tilde{\psi}(f, g) = (\hat{\psi}(f), \psi(g))$ with $\hat{\psi}(f)(h) = \prod_{k \in \psi^{-1}(h)} f(k)$ for every $h \in H$.*

These functoriality properties can now be joined to give a connection between different bracketing of iterated wreath products:

Lemma 2.8. *Let A, B, C be finite groups and A abelian. Then there are epimorphisms*

$$A \wr (B \wr C) \to (A \wr B) \wr C \to (A \times B) \wr C.$$

Proof. Let us first construct an epimorphism $h_* : (A \wr B) \wr C \to (A \times B) \wr C$. Define $h : A \wr B \to A \times B$ by

$$h(f, b) = \Bigl(\prod_{x \in B} f(x), b\Bigr),$$

for any $f : B \to A$, $b \in B$. Since A is abelian h is a homomorphism. For every $a \in A$, let $f_a : B \to A$ be the map $f_a(b') = 0$ for any $1 \neq b' \in B$ and $f_a(1) = a$. Then clearly $h(f_a, b) = (a, b)$ for any $a \in A$, $b \in B$ and hence h is onto. By Lemma 2.6, h induces an epimorphism $h_* : (A \wr B) \wr C \to (A \times B) \wr C$. To construct the epimorphism $A \wr (B \wr C) \to (A \wr B) \wr C$, we shall use the associativity of the permutational wreath product (see [Meldrum 1995, Theorem 3.2]). Using this associativity one has

$$(A \wr B) \wr C = (A \wr_B B) \wr_C C \cong A \wr_{B \times C} (B \wr_C C).$$

It is now left to construct an epimorphism:

$$A \wr (B \wr C) = A \wr_{B \wr C} (B \wr C) \to A \wr_{B \times C} (B \wr C).$$

By Lemma 2.5, there is a $B \wr C$-map $\phi : B \wr C \to B \times C$ and hence by Lemma 2.4 there is an epimorphism $A \wr_{B \wr C} (B \wr C) \to A \wr_{B \times C} (B \wr C)$. □

Let us iterate Lemma 2.8. Let $G_1, \dots, G_n$ be groups. The *ascending iterated standard wreath product* of $G_1, \dots, G_n$ is defined as

$$\bigl(\cdots((G_1 \wr G_2) \wr G_3) \wr \cdots\bigr) \wr G_n,$$

and the *descending iterated standard wreath product* of $G_1, \dots, G_n$ is defined as

$$G_1 \wr (G_2 \wr (\cdots \wr (G_{n-1} \wr G_n) \cdots)).$$

These two iterated wreath products are not isomorphic in general, as the standard wreath product is not associative (as opposed to the permutation wreath product). We shall abbreviate and write $G_1 \wr (G_2 \wr \cdots \wr G_n)$ to refer to the descending wreath product and $(G_1 \wr \cdots \wr G_{r-1}) \wr G_r$ to refer to the ascending wreath product.

By iterating the epimorphism in Lemma 2.8 one obtains

Corollary 2.9. *Let $A_1, \dots, A_r$ be abelian groups. Then $(A_1 \wr \cdots \wr A_{r-1}) \wr A_r$ is an epimorphic image of $A_1 \wr (A_2 \wr \cdots \wr A_r)$.*

Proof. By induction on r. The cases $r = 1, 2$ are trivial; assume $r \geq 3$. By the induction hypothesis there is an epimorphism

$$\pi_1' : A_1 \wr (A_2 \wr \cdots \wr A_{r-1}) \to (A_1 \wr \cdots \wr A_{r-2}) \wr A_{r-1}.$$

By Lemma 2.6, π_1' induces an epimorphism $\pi_1 : (A_1 \wr (A_2 \wr \cdots \wr A_{r-1})) \wr A_r \to (A_1 \wr \cdots \wr A_{r-1}) \wr A_r$. Applying Lemma 2.8 with $A = A_1$, $B = A_2 \wr (A_3 \wr \cdots \wr A_{r-1})$, and $C = A_r$, one obtains an epimorphism

$$\pi_2 : A_1 \wr (A_2 \wr \cdots \wr A_r) \to (A_1 \wr (A_2 \wr \cdots \wr A_{r-1})) \wr A_r.$$

Taking the composition $\pi = \pi_1 \pi_2$ one obtains an epimorphism

$$\pi : A_1 \wr (A_2 \wr \cdots \wr A_r) \to (A_1 \wr \cdots \wr A_{r-1}) \wr A_r. \qquad \square$$

2.2. ***Dimension under epimorphisms.*** Let us examine how the "dimension" d behaves under the homomorphisms in Lemma 2.8 and Corollary 2.9. By [Kaplan and Lev 2003, Theorem 2.1], for any finite group G that is not perfect, i.e., $[G, G] \neq G$, where $[G, G]$ denotes the commutator subgroup of G, one has $\mathrm{d}(G) = \mathrm{d}(G/[G, G])$. According to our definitions, for a perfect group G, $\mathrm{d}(G/[G, G]) = \mathrm{d}(\{1\}) = 0$, but if G is nontrivial, $\mathrm{d}(G) \geq 1$. As nontrivial semiabelian groups are not perfect, this difference will not affect any of the arguments in the sequel.

Definition 2.10. Let G be a finite group and p a prime. Define $\mathrm{d}_p(G)$ to be the rank of the p-Sylow subgroup of $G/[G, G]$, i.e., $\mathrm{d}_p(G) := \mathrm{d}((G/[G, G])(p))$.

Note that if G is not perfect one has $\mathrm{d}(G) = \max_p(\mathrm{d}_p(G))$.

Let p be a prime. An epimorphism $f : G \to H$ is called d-preserving (resp. d_p-preserving) if $\mathrm{d}(G) = \mathrm{d}(H)$ (resp. $\mathrm{d}_p(G) = \mathrm{d}_p(H)$).

Lemma 2.11. *Let G and H be two finite groups. Then*:

$$H \wr G/[H \wr G, H \wr G] \cong H/[H, H] \times G/[G, G].$$

Proof. Applying Lemmas 2.6 and 2.7 one obtains an epimorphism

$$H \wr G \to H/[H, H] \wr G/[G, G].$$

By Lemma 2.8 (applied with $C = 1$) there is an epimorphism

$$H/[H, H] \wr G/[G, G] \to H/[H, H] \times G/[G, G].$$

Composing these epimorphisms one obtains an epimorphism

$$\pi : H \wr G \to H/[H, H] \times G/[G, G],$$

that sends an element $(f : G \to H, g) \in H \wr G$ to

$$\Big(\prod_{x \in G} f(x)[H, H], g[G, G]\Big) \in H/[H, H] \times G/[G, G].$$

The image of π is abelian and hence $\ker(\pi)$ contains $K := [H \wr G, H \wr G]$.

Let us show $K \supseteq \ker(\pi)$. Let $(f, g) \in \ker(\pi)$. Then $g \in [G, G]$ and $\prod_{x \in G} f(x) \in [H, H]$. As $g \in [G, G]$, it suffices to show that the element $f = (f, 1) \in H \wr G$ is in K. Let $g_1, \dots, g_n$ be the elements of G, and for every $i = 1, \dots, n$ let f_i be the function for which $f_i(g_i) = f(g_i)$ and $f(g_j) = 1$ for every $j \neq i$. One can write f as $\prod_{i=1}^n f_i$. Now for every $i = 1, \dots, n$, the function $f_{1,i} = f_i^{g_i^{-1}}$ satisfies $f_{1,i}(1) = f(g_i)$ and $f_{1,i}(g_j) = 1$ for every $j \neq 1$. Thus f_i is a product of an element in $[H^{|G|}, G]$ and $f_{i,1}$. So, f is a product of elements in $[H^{|G|}, G]$ and $f' = \prod_{i=1}^n f_{1,i}$. But $f'(1) = \prod_{x \in G} f(x) \in [H, H]$ and $f'(g_i) = 1$ for every $i \neq 1$ and hence $f' \in [H^{|G|}, H^{|G|}]$. Thus, $f \in K$ as required and $K = \ker \pi$. □

The following is an immediate conclusion:

Corollary 2.12. *Let G and H be two finite groups. Then*

$$\mathrm{d}_p(H \wr G) = \mathrm{d}_p(H) + \mathrm{d}_p(G)$$

for any prime p.

So, for groups A, B, C as in Lemma 2.8, we have

$$\mathrm{d}_p(A \wr (B \wr C)) = \mathrm{d}_p((A \times B) \wr C) = \mathrm{d}_p(A \times B \times C) = \mathrm{d}_p(A) + \mathrm{d}_p(B) + \mathrm{d}_p(C)$$

for every p. In particular, the epimorphisms in Lemma 2.8 are d-preserving.

The same observation holds for Corollary 2.9, so one has:

Lemma 2.13. *Let $A_1, \dots, A_r$ be finite abelian groups. Then*

$$\mathrm{d}_p(A_1 \wr (A_2 \wr \cdots \wr A_r)) = \mathrm{d}_p((A_1 \wr \cdots \wr A_{r-1}) \wr A_r) = \mathrm{d}_p(A_1 \times \cdots \times A_r)$$

are all $\sum_{i=1}^r \mathrm{d}_p(A_i)$ for any prime p.

For cyclic groups $A_1, \dots, A_r$, $\mathrm{d}_p(A_1 \wr (A_2 \wr \cdots \wr A_r))$ is simply the number of cyclic groups among $A_1, \dots, A_r$ whose p-part is nontrivial. Thus:

Corollary 2.14. *Let $C_1, \dots, C_r$ be finite cyclic groups and $G = C_1 \wr (C_2 \wr \cdots \wr C_r)$. Then $\mathrm{d}(G) = \max_{p \mid |G|} \mathrm{d}\big(C_1(p) \wr (C_2(p) \wr \cdots \wr C_r(p))\big)$.*

Let us apply Lemma 2.8 in order to connect between descending iterated wreath products of abelian and cyclic groups:

Proposition 2.15. *Let $A_1, \dots, A_r$ be finite abelian groups and let A_i have invariant factors $C_{i,j}$ for $j = 1, \dots, l_i$, i.e., $A_i = \prod_{j=1}^{l_i} C_{i,j}$ and $|C_{i,j}|$ divides $|C_{i,j+1}|$ for $i = 1, \dots, r$ and $j = 1, \dots, l_i - 1$. There is an epimorphism from the descending iterated wreath product $\tilde{G} := \wr_{i=1}^{r} \wr_{j=1}^{l_i} C_{i,j}$ (where the groups $C_{i,j}$ are ordered lexicographically: $C_{1,1}, C_{1,2}, \dots, C_{1,l_1}, C_{2,1}, \dots, C_{r,l_r}$) to $G := A_1 \wr (A_2 \wr \cdots \wr A_r)$.*

Proof. Assume $A_1 \neq \{0\}$ (otherwise A_1 can be simply omitted). Let us prove the assertion by induction on $\sum_{i=1}^{r} l_i$. Let $G_2 = A_2 \wr (A_3 \wr \cdots \wr A_k)$. Write $A_1 = C_{1,1} \times A_1'$. By Lemma 2.8, there is an epimorphism

$$\pi_1 : C_{1,1} \wr (A_1' \wr G_2) \to (C_{1,1} \times A_1') \wr G_2 = A_1 \wr G_2 = G.$$

By applying the induction hypothesis to $A_1', A_2, \dots, A_r$, there is an epimorphism π_2' from the descending iterated wreath product $\tilde{G}_2 = \wr_{j=2}^{l_1} C_{1,j} \wr (\wr_{i=2}^{r} \wr_{j=1}^{l_i} C_{i,j})$ to $A_1' \wr G_2$. By Lemma 2.7, π_2' induces an epimorphism $\pi_2 : C_{1,1} \wr \tilde{G}_2 \to C_{1,1} \wr (A_1' \wr G_2)$. Taking the composition $\pi = \pi_2 \pi_1$, we obtain the required epimorphism: $\pi : \tilde{G} = C_{1,1} \wr \tilde{G}_2 \to G$. $\square$

Remark 2.16. Note that

$$\mathrm{d}_p(\tilde{G}) = \sum_{i=1}^{r} \sum_{j=1}^{l_i} \mathrm{d}_p(C_{i,j}) = \sum_{i=1}^{r} \mathrm{d}_p(A_i) = \mathrm{d}_p(G)$$

for every p and hence π is d-preserving.

Therefore, showing G is a d-preserving epimorphic image of an iterated wreath product of abelian groups is equivalent to showing G is a d-preserving epimorphic image of an iterated wreath product of finite cyclic groups.

3. Wreath length

The following lemma is essential for the definition of wreath length:

Lemma 3.1. *Let G be a finite semiabelian group. Then G is a homomorphic image of a descending iterated wreath product of finite cyclic groups, i.e., there are finite cyclic groups $C_1, \dots, C_r$ and an epimorphism $C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.*

Proof. By Proposition 2.15 it suffices to show G is an epimorphic image of a descending iterated wreath product of finite abelian groups. We prove this by induction on $|G|$, the case $G = \{1\}$ being trivial. By Theorem 2.3 of [Dentzer 1995], we have $G = A_1 H$ with A_1 an abelian normal subgroup and H a proper semiabelian subgroup of G. First, there is an epimorphism

$$\pi_1 : A_1 \wr H \to A_1 H = G.$$

By induction there are abelian groups $A_2, \dots, A_r$ and an epimorphism $\pi_2' : A_2 \wr (A_3 \wr \cdots \wr A_r) \to H$. By Lemma 2.6, π_2' can be extended to an epimorphism $\pi_2 : A_1 \wr (A_2 \wr \cdots \wr A_r) \to A_1 \wr H$. So, by taking the composition $\pi = \pi_1\pi_2$ one obtains the required epimorphism $\pi : A_1 \wr (A_2 \wr \cdots \wr A_r) \to G$. □

Definition 3.2. Let G be a finite semiabelian group. Define the *wreath length* $\mathrm{wl}(G)$ of G to be the smallest positive integer r such that there are finite cyclic groups $C_1, \dots, C_r$ and an epimorphism $C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.

Let $\tilde{G} = C_1 \wr (C_2 \wr \cdots \wr C_r)$ and $\pi : \tilde{G} \to G$ an epimorphism. Then, by Corollary 2.14,

$$\mathrm{d}(G) \le \mathrm{d}(\tilde{G}) \le r.$$

In particular $\mathrm{d}(G) \le \mathrm{wl}(G)$.

Proposition 3.3. *Let $C_1, \dots, C_r$ be nontrivial finite cyclic groups. Then*

$$\mathrm{wl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r.$$

Let $\mathrm{dl}(G)$ denote the derived length of a (finite) solvable group G, i.e., the smallest positive integer n such that the n-th higher commutator subgroup of G (the n-th element in the derived series $G = G^{(0)} \ge G^{(1)} = [G, G] \ge \cdots \ge G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \ge \cdots$) is trivial. In order to prove this proposition we will use the following lemma:

Lemma 3.4. *Let $C_1, \dots, C_r$ be nontrivial finite cyclic groups. Then*

$$\mathrm{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r.$$

Proof. It is easy (by induction) to see that $\mathrm{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) \le r$. We turn to the reverse inequality. By Corollary 2.9, it suffices to prove it for the ascending iterated wreath product $G = (C_1 \wr \cdots \wr C_{r-1}) \wr C_r$. We prove this by induction on r. The case $r = 1$ is trivial. Assume $r \ge 1$. Write $G_1 := (C_1 \wr \cdots \wr C_{r-2}) \wr C_{r-1}$ so that $G = G_1 \wr C_r$. By the induction hypothesis, $\mathrm{dl}(G_1) = r - 1$. View G as the semidirect product $G_1^r \rtimes C_r$. For any $g \in G_1$, the element $t_g := (g, g^{-1}, 1, 1, \dots, 1) \in G_1^r$ lies in $[G_1^r, C_r]$ and hence in $[G_1^r, C_r] \le G' \le G_1^r$. Let $H = \{t_g \mid g \in G_1\}$. The projection map $G_1^r \to G_1$ onto the first copy of G_1 in G_1^r maps H onto G_1. Since $H \le G'$, the projection map also maps G' onto G_1. Now $\mathrm{dl}(G_1) = r - 1$ by the induction hypothesis. It follows that $\mathrm{dl}(G') \ge r - 1$, whence $\mathrm{dl}(G) \ge r$. □

Proof of Proposition 3.3. We first observe that $\mathrm{wl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) \le r$ by definition. If $C_1 \wr (C_2 \wr \cdots \wr C_r)$ were a homomorphic image of a shorter descending iterated wreath product $C_1' \wr (C_2' \wr \cdots \wr C_s')$, then by Lemma 3.4,

$$s = \mathrm{dl}(C_1' \wr (C_2' \wr \cdots \wr C_s')) \ge \mathrm{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r > s,$$

a contradiction. □

Combining Proposition 3.3 with Corollary 2.14 we have:

Corollary 3.5. *Let $C_1, \dots, C_r$ be finite cyclic groups and $G = C_1 \wr (C_2 \wr \cdots \wr C_r)$. Then* $\mathrm{wl}(G) = \mathrm{d}(G)$ *if and only if there is a prime p for which $p \mid |C_1|, \dots, |C_r|$.*

All examples of groups G with $\mathrm{wl}(G) = \mathrm{d}(G)$ arise from Corollary 3.5:

Proposition 3.6. *Let G be a finite semiabelian group. Then* $\mathrm{wl}(G) = \mathrm{d}(G)$ *if and only if there is a prime p, finite cyclic groups $C_1, \dots, C_r$ for which $p \mid |C_i|$, $i = 1, \dots, r$, and a* d*-preserving epimorphism $\pi : C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.*

Proof. Let $d = \mathrm{d}(G)$. The equality $d = \mathrm{wl}(G)$ holds if and only if there are finite cyclic groups $C_1, C_2, \dots, C_d$ and an epimorphism $\pi : \tilde{G} = C_1 \wr (C_2 \wr \cdots \wr C_d) \to G$. Assume the latter holds. Clearly $d \le \mathrm{d}(\tilde{G})$ but by Corollary 2.14 applied to $\tilde{G}$ we also have $\mathrm{d}(\tilde{G}) \le d$. It follows that π is d-preserving. Since $\mathrm{d}(G) = \max_p(\mathrm{d}_p(G))$, there is a prime p for which $d = \mathrm{d}_p(G)$ and hence $\mathrm{d}_p(\tilde{G}) = d$. Thus, $p \mid |C_i|$ for all $i = 1, \dots, r$.

Let us prove the converse. Assume there is a prime p, finite cyclic groups $C_1, \dots, C_r$ for which $p \mid |C_i|$, $i = 1, \dots, r$, and a d-preserving epimorphism $\pi : \tilde{G} := C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$. Since $p \mid |C_i|$, it follows that $\mathrm{d}_p(\tilde{G}) = r$. As $\mathrm{d}_p(\tilde{G}) \le \mathrm{d}(\tilde{G}) \le r$, it follows that $\mathrm{d}(G) = \mathrm{d}(\tilde{G}) = r$. In particular $\mathrm{wl}(G) \le r = \mathrm{d}(G)$ and hence $\mathrm{wl}(G) = \mathrm{d}(G)$. □

Remark 3.7. Let G be a semiabelian p-group. By [Neftin 2009, Corollary 2.15], G is a d-preserving image of an iterated wreath product of abelian subgroups of G (following the proof one can observe that the abelian groups were actually subgroups of G). So, by Proposition 2.15, G is a d-preserving epimorphic image of $\tilde{G} := C_1 \wr (C_2 \wr \cdots \wr C_k)$ for cyclic subgroups $C_1, \dots, C_k$ of G. By applying Proposition 3.6 one obtains $\mathrm{wl}(G) = \mathrm{d}(G)$.

Remark 3.8. Throughout the proof of [Neftin 2009, Corollary 2.15] one can use the minimality assumption posed on the decompositions to show directly that the abelian groups $A_1, \dots, A_r$, for which there is a d-preserving epimorphism $A_1 \wr (A_2 \wr \cdots \wr A_r) \to G$, can be actually chosen to be cyclic.

We generalize Remark 3.7 to nilpotent groups:

Proposition 3.9. *Let G be a finite nilpotent semiabelian group. Then* $\mathrm{wl}(G) = \mathrm{d}(G)$.

Proof. Let $d = \mathrm{d}(G)$. Let $p_1, \dots, p_k$ be the primes dividing $|G|$ and let P_i be the p_i-Sylow subgroup of G for every $i = 1, \dots, k$. So, $G \cong \prod_{i=1}^k P_i$. By Remark 3.7, there are cyclic p_i-groups $C_{i,1}, \dots, C_{i,r_i}$ and a d-preserving epimorphism $\pi_i : C_{i,1} \wr (C_{i,2} \wr \cdots \wr C_{i,r_i}) \to P_i$ for every $i = 1, \dots, k$. In particular for any $i = 1, \dots, k$, $r_i = \mathrm{d}(P_i) = \mathrm{d}_p(G) \le d$. For any $i = 1, \dots, k$ and any $d \ge j > r_i$, set $C_{i,j} = \{1\}$. For any $j = 1, \dots, d$ define $C_j = \prod_{i=1}^k C_{i,j}$.

We claim G is an epimorphic image of $\tilde{G} = C_1 \wr (C_2 \wr \cdots \wr C_d)$. To prove this claim it suffices to show every P_i is an epimorphic image of $\tilde{G}$ for every $i = 1, \dots, k$. As $C_{i,j}$ is an epimorphic image of C_j for every $j = 1, \dots, d$ and every $i = 1, \dots, k$, one can apply Lemmas 2.6 and 2.7 iteratively to obtain an epimorphism $\pi_i' : \tilde{G} \to C_{i,1} \wr (C_{i,2} \wr \cdots \wr C_{i,r})$ for every $i = 1, \dots, k$. Taking the composition $\pi_i'\pi_i$ gives the required epimorphism and proves the claim. As G is an epimorphic image of an iterated wreath product of $\mathrm{d}(G)$ cyclic groups one has $\mathrm{wl}(G) \le \mathrm{d}(G)$ and hence $\mathrm{wl}(G) = \mathrm{d}(G)$. □

Example 3.10. Let $G = D_n = \langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma\tau\sigma = \tau^{-1}\rangle$ for $n \ge 3$. Since G is an epimorphic image of $\langle\tau\rangle \wr \langle\sigma\rangle$ and G is not abelian we have $\mathrm{wl}(G) = 2$. On the other hand $\mathrm{d}(G) = \mathrm{d}(G/[G, G])$ is 1 if n is odd and 2 if n is even. So, $G = D_3 = S_3$ is the minimal example for which $\mathrm{wl}(G) \ne \mathrm{d}(G)$.

4. A ramification bound for semiabelian groups

Theorem 4.1. *Let G be a finite semiabelian group. Then there exists a tamely ramified extension $K/\mathbb{Q}$ with $G(K/\mathbb{Q}) \cong G$ in which at most $\mathrm{wl}(G)$ primes ramify.*

The proof relies on the splitting lemma from [Kisilevsky and Sonn 2010]: Let ℓ be a rational prime, K a number field, and $\mathfrak{p}$ a prime of K that is prime to ℓ. Let $I_{K,\mathfrak{p}}$ denote the group of fractional ideals prime to $\mathfrak{p}$, let $P_{K,\mathfrak{p}}$ denote the subgroup of principal ideals that are prime to $\mathfrak{p}$, and let $P_{K,\mathfrak{p},1}$ be the subgroup of principal ideals (α) with $\alpha \equiv 1 \pmod{\mathfrak{p}}$. Let $\bar{P}_{\mathfrak{p}}$ denote $P_{K,\mathfrak{p}}/P_{K,\mathfrak{p},1}$. The ray class group $Cl_{K,\mathfrak{p}}$ is defined to be $I_{K,\mathfrak{p}}/P_{K,\mathfrak{p},1}$. Now, as $I_{K,\mathfrak{p}}/P_{K,\mathfrak{p}} \cong Cl_K$, one has the short exact sequence

$$1 \longrightarrow \bar{P}_{\mathfrak{p}}^{(\ell)} \longrightarrow Cl_{K,\mathfrak{p}}^{(\ell)} \longrightarrow Cl_K^{(\ell)} \longrightarrow 1, \tag{4-1}$$

where $A^{(\ell)}$ denotes the ℓ-primary component of an abelian group A. Let us describe a sufficient condition for the splitting of (4-1). Let $\mathfrak{a}_1, \dots, \mathfrak{a}_r \in I_{K,\mathfrak{p}}$, and let $\tilde{\mathfrak{a}}_1, \dots, \tilde{\mathfrak{a}}_r$ be their classes in $Cl_{K,\mathfrak{p}}^{(\ell)}$ with images $\bar{\mathfrak{a}}_1, \dots, \bar{\mathfrak{a}}_r$ in $Cl_K^{(\ell)}$, so that $Cl_K^{(\ell)} = \langle\bar{\mathfrak{a}}_1\rangle \times \langle\bar{\mathfrak{a}}_2\rangle \times \cdots \times \langle\bar{\mathfrak{a}}_r\rangle$. Let $\ell^{m_i} := |\langle\bar{\mathfrak{a}}_i\rangle|$ and let $a_i \in K$ satisfy $\mathfrak{a}_i^{\ell^{m_i}} = (a_i)$, for $i = 1, \dots, r$.

Lemma 4.2 [Kisilevsky and Sonn 2006]. *Let $\mathfrak{p}$ be a prime of K and let $K' = K(\sqrt[\ell^{m_i}]{a_i} \mid i = 1, \dots, r)$. If $\mathfrak{p}$ splits completely in K' then the sequence (4-1) splits.*

The splitting of (4-1) was used in [Kisilevsky and Sonn 2010] to construct cyclic ramified extensions at one prime only. Let $m = \max\{1, m_1, \dots, m_r\}$. Let U_K denote the units in $\mathbb{O}_K$.

Lemma 4.3 [Kisilevsky and Sonn 2010]. *Let $K'' = K(\mu_{\ell^m}, \sqrt[\ell^m]{\xi}, \sqrt[\ell^{m_i}]{a_i} \mid \xi \in U_K, i = 1, \dots, r)$ and let $\mathfrak{p}$ be a prime of K which splits completely in K''. Then there is a cyclic ℓ^m-extension of K that is totally ramified at $\mathfrak{p}$ and is not ramified at any other prime of K.*

Corollary 4.4. *Let K be a number field, n a positive integer. Then there exists a finite extension K''' of K such that if $\mathfrak{p}$ is any prime of K that splits completely in K''', then there exists a cyclic extension L/K of degree n in which $\mathfrak{p}$ is totally ramified and $\mathfrak{p}$ is the only prime of K that ramifies in L.*

Proof. Let $n = \prod_\ell \ell^{m(\ell)}$ be the decomposition of n into primes. Let K''' be the composite of the fields $K'' = K''(\ell)$ in Lemma 4.3 ($m = m(\ell)$). Let $L(\ell)$ be the cyclic extension of degree $\ell^{m(\ell)}$ yielded by Lemma 4.3. The composite $L = \prod L(\ell)$ has the desired property. □

Proof of Theorem 4.1. By definition, G is a homomorphic image of a descending iterated wreath product of cyclic groups $C_1 \wr (C_2 \wr \cdots \wr C_r)$, $r = \mathrm{wl}(G)$. Without loss of generality $G \cong C_1 \wr (C_2 \wr \cdots \wr C_r)$ is itself a descending iterated wreath product of cyclic groups. Proceed by induction on r. For $r = 1$, G is cyclic of order, say, N. If p is a rational prime $\equiv 1 \pmod N$, then the field of p-th roots of unity $\mathbb{Q}(\mu_p)$ contains a subfield L cyclic over $\mathbb{Q}$ with Galois group G and exactly one ramified prime, namely p. Thus the theorem holds for $r = 1$.

Assume $r > 1$ and the theorem holds for $r - 1$. Let $K_1/\mathbb{Q}$ be a tamely ramified Galois extension with $G(K_1/\mathbb{Q}) \cong G_1$, where G_1 is the descending iterated wreath product $C_2 \wr (C_3 \wr \cdots \wr C_r)$, such that the ramified primes in K_1 are a subset of $\{p_2, \ldots, p_r\}$. By Corollary 4.4, there exists a prime $p = p_1$ not dividing the order of G which splits completely in K_1''', the field supplied for K_1 by Corollary 4.4, and let $\mathfrak{p} = \mathfrak{p}_1$ be a prime of K_1 dividing p. By Corollary 4.4, there exists a cyclic extension L/K_1 with $G(L/K_1) \cong C_1$ in which $\mathfrak{p}$ is totally ramified and in which $\mathfrak{p}$ is the only prime of K_1 which ramifies in L.

Now $\mathfrak{p}$ has $|G_1|$ distinct conjugates $\{\sigma(\mathfrak{p}) \mid \sigma \in G(K_1/\mathbb{Q})\}$ over K_1. For each $\sigma \in G(K_1/\mathbb{Q})$, the conjugate extension $\sigma(L)/K_1$ is well-defined, since $K_1/\mathbb{Q}$ is Galois. Let M be the composite of the $\sigma(L)$, $\sigma \in G(K_1/\mathbb{Q})$. For each σ, $\sigma(L)/K_1$ is cyclic of degree $|C_1|$, ramified only at $\sigma(\mathfrak{p})$, and $\sigma(\mathfrak{p})$ is totally ramified in $\sigma(L)/K_1$. It now follows (see, e.g., [Kisilevsky and Sonn 2010, Lemma 1]) that the fields $\{\sigma(L) \mid \sigma \in G(K_1/\mathbb{Q})\}$ are linearly disjoint over K_1, hence $G(M/\mathbb{Q}) \cong C_1 \wr G_1 \cong G$. Since the only primes of K_1 ramified in M are $\{\sigma(\mathfrak{p}) \mid \sigma \in G(K_1/\mathbb{Q})\}$, the only rational primes ramified in M are $p_1, p_2, \ldots, p_n$. □

Corollary 4.5. *The minimal ramification problem has a positive solution for all finite semiabelian groups G for which* $\mathrm{wl}(G) = \mathrm{d}(G)$. *Precisely, any finite semiabelian group G for which* $\mathrm{wl}(G) = \mathrm{d}(G)$ *can be realized tamely as a Galois group over the rational numbers with exactly* $\mathrm{d}(G)$ *ramified primes.*

By Proposition 3.9, we have:

Corollary 4.6. *The minimal ramification problem has a positive solution for all finite nilpotent semiabelian groups.*

5. Arithmetic consequences

In this section we examine some arithmetic consequences of a positive solution to the minimal ramification problem. Specifically, given a group G, the existence of infinitely many minimally tamely ramified G-extensions $K/\mathbb{Q}$ is reinterpreted in some cases in terms of some open problems in algebraic number theory. We will be most interested in the case $\mathrm{d}(G) = 1$.

Proposition 5.1. *Let q and ℓ be distinct primes. Let $K/\mathbb{Q}$ be a cyclic extension of degree $n := [K : \mathbb{Q}] \geq 2$ with $(n, q\ell) = 1$. Suppose that $K/\mathbb{Q}$ is totally and tamely ramified at a unique prime $\mathfrak{l}$ dividing ℓ. Then q divides the class number h_K of K if and only if there exists an extension L/K satisfying the following*:

(1) *$L/\mathbb{Q}$ is a Galois extension with* nonabelian *Galois group $G = G(L/\mathbb{Q})$.*

(2) *The degree $[L : K] = q^s$ is a power of q.*

(3) *$L/\mathbb{Q}$ is (tamely) ramified only at primes over ℓ.*

Proof. First suppose that q divides h_K. Let K_0 be the q-Hilbert class field of K, i.e., K_0/K is the maximal unramified abelian q-extension of K. Then $K_0/\mathbb{Q}$ is a Galois extension with Galois group $G := G(K_0/\mathbb{Q})$, and $H := G(K_0/K) \simeq (C_K)_q \neq 0$, the q-part of the ideal class group of K. Then $[G, G]$ is contained in H. If $[G, G] \subsetneq H$, then the fixed field of $[G, G]$ would be an abelian extension of $\mathbb{Q}$ which contains an unramified q-extension of $\mathbb{Q}$, which is impossible. Hence $[G, G] = H \neq 0$ and so G is a nonabelian group, and $L = K_0$ satisfies (1), (2), and (3) of the statement.

Conversely suppose that there is an extension L/K satisfying (1), (2), and (3) of the statement. Since $H = G(L/K)$ is a q-group, there is a sequence of normal subgroups $H = H_0 \supset H_1 \supset H_2 \cdots \supset H_s = 0$ with H_i/H_{i+1} a cyclic group of order q. Let L_i denote the fixed field of H_i so that $K = L_0 \subset \cdots \subset L_s = L$. Let m be the largest index such that $L_m/\mathbb{Q}$ is totally ramified (necessarily at ℓ). If $m = s$, then $L/\mathbb{Q}$ is totally and tamely ramified at ℓ and so the inertia group $T(\mathfrak{L}/(\ell)) = G$, where in this case $\mathfrak{L}$ is the unique prime of L dividing ℓ. Since $L/\mathbb{Q}$ is tamely ramified it follows that $T(\mathfrak{L}/(\ell))$ is cyclic, but this contradicts the hypothesis that G is nonabelian. Therefore it follows that $m < s$, and so L_{m+1}/L_m is unramified and therefore q must divide the class number h_{L_m}. Then a result of [Iwasawa 1956] implies that q divides all of the class numbers $h_{L_{m-1}}, \ldots, h_{L_0} = h_K$. $\square$

We now apply this to the case that $G \neq \{1\}$ is a quotient of the regular wreath product $C_q \wr C_p$ where p and q are distinct primes. Then $\mathrm{d}(G) = 1$.

The existence of infinitely many minimally tamely ramified G-extensions $L/\mathbb{Q}$ would by Proposition 5.1 imply the existence of infinitely many cyclic extensions $K/\mathbb{Q}$ of degree $[K : \mathbb{Q}] = p$ ramified at a unique prime $\ell \neq p, q$ for which q divides the class number h_K. (If there were only finitely many distinct such cyclic extensions $K/\mathbb{Q}$, then the number of ramified primes ℓ would be bounded, and there would be an absolute upper bound on the possible discriminants of the distinct fields $L/\mathbb{Q}$. By Hermite's theorem, this would mean that the number of such G-extensions $L/\mathbb{Q}$ would be bounded).

The question of whether there is an infinite number of cyclic degree p extensions (or even one) of $\mathbb{Q}$ whose class number is divisible by q is in general open at this time.

For $p=2$, it is known that there are infinitely many quadratic fields (see [Ankeny and Chowla 1955]), with class numbers divisible by q, but it is not known that this occurs for quadratic fields with prime discriminant.

This latter statement is also a consequence of Schinzel's hypothesis as is shown in [Plans 2004]. There is also some numerical evidence that the heuristic of Cohen-Lenstra should be statistically independent of the primality of the discriminant [Jacobson et al. 1995; te Riele and Williams 2003]. If this were true, then one would expect that there is a positive density of primes ℓ for which the cyclic extension of degree p and conductor ℓ would have class number divisible by q.

For $p=3$ it has been proved in [Bhargava 2005] that there are infinitely many cubic fields $K/\mathbb{Q}$ for which 2 divides their class numbers. That there are infinitely many cyclic cubics with prime squared discriminants whose class numbers are even (or more generally divisible by some fixed prime q) seems out of reach at this time.

In our view, there is significant arithmetic interest in solving the minimal ramification problem for other groups. See also [Harbater 1994; Jones and Roberts 2008; Rabayev 2009].

References

[Ankeny and Chowla 1955] N. C. Ankeny and S. Chowla, "On the divisibility of the class number of quadratic fields", *Pacific J. Math.* **5** (1955), 321–324. MR 19,18f Zbl 0065.02402

[Bhargava 2005] M. Bhargava, "The density of discriminants of quartic rings and fields", *Ann. of Math.* (2) **162**:2 (2005), 1031–1063. MR 2006m:11163 Zbl 1159.11045

[Dentzer 1995] R. Dentzer, "On geometric embedding problems and semiabelian groups", *Manuscripta Math.* **86**:2 (1995), 199–216. MR 96c:12006 Zbl 0836.12002

[Harbater 1994] D. Harbater, "Galois groups with prescribed ramification", pp. 35–60 in *Arithmetic geometry* (Tempe, AZ, 1993), edited by N. Childress and J. W. Jones, Contemp. Math. **174**, Amer. Math. Soc., Providence, RI, 1994. MR 96a:12008 Zbl 0815.11053

[Iwasawa 1956] K. Iwasawa, "A note on class numbers of algebraic number fields", *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258. MR 18,644d Zbl 0074.03002

[Jacobson et al. 1995] M. J. Jacobson, Jr., R. F. Lukes, and H. C. Williams, "An investigation of bounds for the regulator of quadratic fields", *Experiment. Math.* **4** (1995), 211–225. MR 97d:11173 Zbl 0859.11057

[Jones and Roberts 2008] J. W. Jones and D. P. Roberts, "Number fields ramified at one prime", pp. 226–239 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2010b:11152 Zbl 05279289

[Kaplan and Lev 2003] G. Kaplan and A. Lev, "On the dimension and basis concepts in finite groups", *Comm. Algebra* **31**:6 (2003), 2707–2717. MR 2004f:20060 Zbl 1038.20020

[Kisilevsky and Sonn 2006] H. Kisilevsky and J. Sonn, "Abelian extensions of global fields with constant local degree", *Math. Res. Lett.* **13**:4 (2006), 599–605. MR 2007e:11130 Zbl 1158.11045

[Kisilevsky and Sonn 2010] H. Kisilevsky and J. Sonn, "On the minimal ramification problem for ℓ-groups", *Compos. Math.* **146**:3 (2010), 599–606. MR 2644928 Zbl 1197.11150

[Meldrum 1995] J. D. P. Meldrum, *Wreath products of groups and semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics **74**, Longman, Harlow, 1995. MR 97j:20030 Zbl 0833.20001

[Neftin 2009] D. Neftin, "On semiabelian p-groups", preprint, 2009. arXiv 0908.1472v2

[Plans 2004] B. Plans, "On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$", *Pacific J. Math.* **215**:2 (2004), 381–391. MR 2005d:12005 Zbl 1064.11072

[Rabayev 2009] D. Rabayev, *Polynomials with roots mod n for all n*, Master's Thesis, Technion, 2009.

[te Riele and Williams 2003] H. te Riele and H. Williams, "New computations concerning the Cohen–Lenstra heuristics", *Experiment. Math.* **12** (2003), 99–113. MR 2005d:11183 Zbl 1050.11096

Communicated by Hendrik W. Lenstra
Received 2009-12-20 Revised 2010-06-24 Accepted 2010-08-01

kisilev@mathstat.concordia.ca *Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve Blvd West, Montreal, QC H3G 1M8, Canada*

neftind@tx.technion.ac.il *Department of Mathematics, Technion – Israel Institute of Technology, 32000 Haifa, Israel*
http://www.technion.ac.il/~neftind/

sonn@math.technion.ac.il *Department of Mathematics, Technion – Israel Institute of Technology, 32000 Haifa, Israel*
http://www.math.technion.ac.il/~sonn/

ALGEBRA AND NUMBER THEORY 4:8(2010)

Remarks on modular symbols for Maass wave forms

Yuri I. Manin

To Professor F. Hirzebruch, with friendship and admiration, for his anniversary.

In this paper I introduce modular symbols for Maass wave cusp forms. They appear in the guise of finitely additive functions on the boolean algebra generated by intervals with nonpositive rational ends, with values in analytic functions (pseudomeasures in the sense of Manin and Marcolli). We explain the basic issues and draw an analogy with the p-adic case. We then construct the new modular symbols, followed by the related Lévy–Mellin transforms. This work builds on the fundamental study of Lewis and Zagier (2001).

0. Introduction

0.0. ***Summary.*** Maass wave cusp forms can be considered as analogs of classical cusp forms that have "complex weights" determined by the spectrum of the hyperbolic Laplace operator on the upper complex half-plane. In particular, Maass eigenforms with respect to all Hecke operators define interesting Dirichlet series, exactly as in the classical case.

Dirichlet series related to classical cusp forms admit p-adic analytic continuation. An efficient way to construct this continuation is based on the theory of modular symbols, which allows one to define first p-adic pseudomeasures and then integrate them in order to construct a p-adic version of the Mellin transform (the Mazur–Mellin transform; see [Mazur and Swinnerton-Dyer 1974; Višik and Manin 1974]).

In Section 1 we introduce modular symbols for Maass forms. We also transfer the construction of p-adic pseudomeasures back to the archimedean domain, and introduce the notion of ∞-adic integration and the respective Lévy–Mellin transform.

We argue that in the real analog of $\mathbb{Z}_p$ — the segment [0, 1] — the boolean algebra of closed/open p-adic subsets must be replaced by the boolean algebra of finite

MSC2000: 11F37.

Keywords: Maass modular forms, modular symbols.

unions of intervals with rational ends, on which modular symbols, both classical and new, form a finitely additive pseudomeasure that can be used for Mellin-type integration. This is the theme of Section 2.

An important role in this theory is played by continued fractions and the dynamical system based on them. In the last subsections I show that the respective transfer operator can be treated as the "Hecke operator T_1" corresponding to the "prime" in characteristic zero, and that the modified Brjuno function in the theory of linearization of holomorphic maps [Marmi et al. 2001; 2006] can be used for the calculation of derivatives of classical Dirichlet series related to cusp forms, replacing the eta function appearing in [Goldfeld 1995].

These ideas are explained in more detail below. In the proofs, I make heavy use of the fundamental study [Lewis and Zagier 2001].

0.1. ***Period polynomials and period functions.*** Let $u(\tau) \in S_{2k}(\mathrm{SL}(2,\mathbb{Z}))$ be a cusp form of integer *weight* $2k > 0$ for the full modular group. This means that it is holomorphic in the upper half-plane, the tensor $u(\tau)(d\tau)^k$ is $\mathrm{SL}(2,\mathbb{Z})$-invariant, and $u(\tau)$ vanishes at cusps.

Its *period polynomial* is defined as the integral

$$\psi(z) = \psi_u(z) := \int_0^{i\infty} u(\tau)(z-\tau)^{2k-2}\,d\tau. \tag{0.1}$$

Here z is, for the time being, an auxiliary formal variable.

One remarkable discovery in the theory of modular functions was the possibility of developing versions for a certain set of *complex weights* $2s$ (replacing the former $2-2k$). This spectrum consists of the (doubled) zeroes of Selberg's zeta function $Z(s)$ of $\mathrm{SL}(2,\mathbb{Z})$ acting on the upper half-plane, or equivalently, those values of s for which the Mayer transfer operator $\mathcal{L}_s^2$ [Mayer 1991a; 1991b] has 1 as its eigenvalue: see [Lewis and Zagier 1997] for a short review and [Lewis and Zagier 2001] for a comprehensive exposition.

0.2. ***Classical modular symbols.*** The classical modular symbols of weight $2k$ for $\mathrm{SL}(2,\mathbb{Z})$, in one of their guises, can be defined simply as the integrals

$$\int_\alpha^\beta u(\tau)(z-\tau)^{2k-2}\,d\tau, \tag{0.2}$$

where this time $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$ are arbitrary cusps, and the integration is taken along, say, the hyperbolic geodesic connecting β to α.

More precisely, the modular symbol $\{\alpha, \beta\}_k$ (for the full modular group) is the integral (0.2) considered as a linear map

$$\{\alpha, \beta\}_k : S_{2k}(\mathrm{SL}(2,\mathbb{Z})) \to \mathbb{C}[z]. \tag{0.3}$$

In the next subsections, we will briefly recall the number-theoretic motivations for considering (0.3). A geometric interpretation of (0.3), after a dualization, runs as follows: this integral expresses the pairing between the Hodge cohomology and the Betti homology of the moduli space $\overline{M}_{1,2k-2}$ of elliptic curves with marked points. (See [Shokurov 1980a; 1980b] for a version involving Kuga varieties rather than moduli spaces.)

The modular symbols (0.3) satisfy the simple functional equations

$$\{\alpha, \beta\}_k + \{\beta, \gamma\}_k + \{\gamma, \alpha\}_k = 0, \quad \{\alpha, \beta\}_k + \{\beta, \alpha\}_k = \{\alpha, \alpha\}_k = 0. \tag{0.4}$$

Thus they can be extended to a $\mathbb{C}[z]$-valued finitely additive function on the boolean algebra generated by (positively oriented) segments with rational ends in $\mathbb{P}^1(\mathbb{R})$. We sometimes call such a function a *pseudomeasure*, as in [Manin and Marcolli 2008]. The variable change formula applied to (0.2) leads to an additional property of this particular pseudomeasure, which we call its *modularity*:

$$\{g(\alpha), g(\beta)\}_k = g\{\alpha, \beta\}_k. \tag{0.5}$$

Here $g \in \mathrm{SL}(2, \mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q})$ by fractional linear transformations, and on polynomials of degree at most $2k - 2$ by a natural twisted action.

A pseudomeasure can in principle take values in any abelian group, and the modularity condition (0.5) makes sense if this group is a left $\mathrm{SL}(2, \mathbb{Z})$-module. If the group of values has no 2- and 3-torsion, the last two equations in (0.4) follow from the first one.

0.3. ***Modular symbols for Maass cusp forms.*** Our first goal is to extend the definition of $\{\alpha, \beta\}_k$ to complex weights for which there exist nontrivial Maass cusp forms. We take the formula (0.2) as our starting point and look for its analogs in Lewis–Zagier theory. We are interested mostly in complex critical zeroes/weights for which $\mathrm{Re}\, s = \frac{1}{2}$.

Tracing parallels with the classical theory, one should keep in mind that certain classical objects have more (or less) than one parallel in the new setting.

For example, the most straightforward analogs of $u(\tau) \in S_{2k}(\mathrm{SL}(2, \mathbb{Z}))$ are apparently Maass wave cusp forms [1949] — smooth $\mathrm{SL}(2, \mathbb{Z})$-invariant functions on H satisfying the hyperbolic Laplace equation $\Delta u = s(1-s)u$ and certain growth and vanishing conditions. An appropriate version of the period polynomial (0.1) for such a form is its period function $\psi_u(z)$, this time a holomorphic function of our former auxiliary variable z.

However, the relationship between u and ψ_u, as it is first explained in [Lewis and Zagier 2001, Chapter I, Section 1], does not look at all like (0.1) and passes through three intermediate steps: $u \leftrightarrow L_\varepsilon \leftrightarrow f \leftrightarrow \psi$.

To the contrary, the structure of (0.1) is reproduced in the formula

$$\psi(z) = \int_{-\infty}^{0} (z-t)^{-2s} U(t)\, dt \tag{0.6}$$

(see [Lewis and Zagier 2001, p. 221]), in which $U(t)\,dt$ denotes a certain distribution on $\mathbb{R}$, called the *boundary value* of $u(\tau)$. Therefore, it is this distribution that in our context seems to be a more adequate analog of a classical cusp form, the more so that its SL(2, $\mathbb{Z}$)-invariance property involves an explicitly weighted action of the modular group,

$$U\Big(\frac{at+b}{ct+d}\Big) = |ct+d|^{2-2s} U(t), \tag{0.7}$$

whereas a Maass form is simply SL(2, $\mathbb{Z}$)-invariant.

Formula (0.6) seems to offer a straightforward way to define the modular symbol — just consider the integrals

$$\int_{\alpha}^{\beta} (z-t)^{-2s} U(t)\, dt.$$

Formal manipulations with such integrals are simple and seemingly prove (0.4) and (0.5); we reproduce them for their heuristic value. However, these calculations cannot be taken literally, because the characteristic functions of the intervals with rational ends do not belong to the space of test functions for the distribution.

Thus we have to find a way around this difficulty.

In fact, there are at least two different ways. One of them starts with the three-term functional equation for the period function $\psi(z)$, proceeds with pure algebra, and works also for Lewis–Zagier's "period-like functions".

Another method is applicable only to the period functions of Maass forms u and uses the Lewis–Zagier formula of the form

$$\psi(z) = \int_{-\infty}^{0} \{u, R_z^s\}(\tau)$$

where the integrand is a closed 1-form depending on z as a parameter (its structure is described in the main text below). One can then integrate this form along a path that may this time connect two arbitrary cusps, thus getting another analog of (0.2).

These two constructions form the content of Section 1.

0.4. ***The Mellin transform and classical modular symbols.*** Now we will explain some of our motivations.

Briefly, we want to describe a construction presenting the Maass Dirichlet series as an integral over, say, [0, 1/2], formally similar to the Mazur–Mellin transform in the theory of p-adic interpolation. We call such a representation the ∞-*adic*

Lévy–Mellin transform [Manin and Marcolli 2008]. The integration measure in both cases is constructed out of modular symbols.

Here is a sketch of the classical p-adic constructions. The classical theory of modular symbols, as presented in [Manin 1972; 1973], started with the following observations. Suppose that we are interested in the calculation of some values (say, at integer points ρ) of a Dirichlet series

$$L_\kappa(\rho) = \sum_{n=1}^{\infty} a_n \kappa(n) n^{-\rho}, \tag{0.8}$$

where (a_n) is a certain "arithmetic" function, and κ is an additive character of $\mathbb{Z}$ of finite order. In the standard approach one first introduces the Fourier series

$$u_\kappa(\tau) := \sum_{n=1}^{\infty} a_n \kappa(n) e^{2\pi i n \tau} \tag{0.9}$$

and then works with the Mellin transform

$$\Lambda_\kappa(\rho) := \int_0^{i\infty} u_\kappa(\tau) \Big(\frac{\tau}{i}\Big)^{\rho-1} d\tau, \tag{0.10}$$

which is related to (0.8) by the simple formula $\Lambda(\rho) = i(2\pi)^{-\rho}\Gamma(\rho)L(\rho)$.

Now, let $u(\tau) := u_{\kappa_0}(\tau)$ where κ_0 is identically 1. Clearly, $u_\kappa(\tau) = u(\tau+\alpha)$ for a rational number α such that $\kappa(n) = e^{2\pi i \alpha n}$, so we can write, shifting the integration path,

$$\Lambda_\kappa(\rho) := \int_\alpha^{i\infty} u(\tau) \Big(\frac{\tau-\alpha}{i}\Big)^{\rho-1} d\tau. \tag{0.11}$$

Thus, if $\rho \geq 1$ is an integer, varying κ in (0.8) reduces to replacing $\tau^{\rho-1}$ in (0.10) by an arbitrary polynomial of degree $\leq \rho - 1$ and allowing the integration paths $(\alpha, i\infty)$ with an arbitrary rational α.

Furthermore, if $u \in S_{2k}(\mathrm{SL}(2,\mathbb{Z}))$ as above, and $1 \leq \rho \leq 2k-1$, applying to α the "continued fractions trick", we can replace $(\alpha, i\infty)$ by a sum of geodesic paths in the upper half-plane, joining pairwise cusps of the form $g^{-1}(0)$ and $g^{-1}(i\infty)$, where g varies in $\mathrm{SL}(2,\mathbb{Z})$, and then return to $(0, i\infty)$ by transforming the integrand via $\tau \mapsto g\tau$. Thus, in particular, all values of (0.8) corresponding to integer ρ inside the critical strip and arbitrary characters κ, can be expressed as linear combinations of modular symbols *with rational coefficients*, and span a finite-dimensional space over $\mathbb{Q}$.

0.5. ***The p-adic Mellin–Mazur transform.*** Such expressions were used in [Manin 1973; 1974] to produce a p-adic interpolation of values (0.8). This problem will make sense if (after an appropriate normalization) these values lie in a finitely generated $\mathbb{Z}$-module, so the basic problem is to control the denominators.

As we already said, the main tool for such an interpolation was a p-adic integral (the Mellin–Mazur transform) with respect to a *p-adic pseudomeasure* (see below) constructed using modular symbols. This transform integrates $\tau^{\rho-1}$ twisted by κ against this pseudomeasure, and for finite order κ produces the classical values $L_\kappa(\rho)$ more or less by definition. (In fact, one works usually with Dirichlet characters in place of κ, but the only difference consists in the appearance of auxiliary Gauss sums).

Here are some details.

(a) *The p-adic integration domain and a naive pseudomeasure.* The following tentative construction applies to any (absolutely convergent) series of the type (0.8) considered as a function of variable κ with fixed ρ.

At the first approximation, consider $\mathbb{Z}_p$ with $\mathbb{Z}$ densely embedded in it. The boolean algebra of closed/open subsets of $\mathbb{Z}_p$ is generated by the *primitive subsets* $a + p^m\mathbb{Z}_p$, for $m = 0, 1, 2, \ldots$ and a ranging over all classes modulo p^m. Put

$$\mu_L(a + p^m\mathbb{Z}_p) := \sum_{n \equiv a \bmod p^m} a_n n^{-\rho}. \tag{0.12}$$

Any two primitive subsets either do not intersect, or one of them is contained in the other. If one primitive subset I is a disjoint union of a finite family of other primitive subsets I_j, then $\mu_L(I) = \sum_j \mu_L(I_j)$. Thus μ_L extends to a $\mathbb{C}$-valued finitely additive function on the boolean algebra of closed/open subsets of $\mathbb{Z}_p$. We will call such objects *pseudomeasures* on $\mathbb{Z}_p$.

Generally, there is no chance that such a pseudomeasure will tend p-adically to zero when $m \to \infty$, even if its values lie in a finite-dimensional $\mathbb{Q}$-space. As explained in [Manin 1973], a Mazur's p-adic integral of a function against such a pseudomeasure typically converges not because the smaller primitive subsets have asymptotically vanishing pseudomeasure, but because in a typical Riemann sum, *many approximately equal terms* of not very large p-adic size are involved, and the *quantity of summands* $\approx p^m$*, tending to zero p-adically*, produces an unconventional nonarchimedean convergence effect.

If the pseudomeasure of small subsets does not tend to zero, the best one may hope for is that it will be *bounded*, i.e., its values will lie in a $\mathbb{Z}$-module of finite type. Even this usually will not happen: for example, one can suspect that

$$\mu_L(p^m\mathbb{Z}) = \sum_{n \equiv 0 \bmod p^m} a_n n^{-\rho} = p^{-m\rho} \sum_n a_{np^m} n^{-\rho}$$

will have denominator of order $p^{-m\rho}$.

A radical way to avoid this danger is to postulate that $a_n = 0$ if n is divisible by p. One can achieve this cheaply, if L admits an Euler product: simply discard the p-th Euler factor of L.

(Notice an interesting archimedean analogy: the Mellin transform Λ in (0.10) produces L *supplemented* by the initially missing "Euler factor at arithmetical infinity", where that phrase mean, as usual, the archimedean valuation of $\mathbb{Q}$.)

Returning to $L_{(p)} := L$ *divided by its p-factor*, we may from now on look only at the group of p-adic units $\mathbb{Z}_p^* \subset \mathbb{Z}_p$ by which our pseudomeasure is now supported.

We repeat, in conclusion, that the classical values (0.8) are tautologically integrals of the locally constant function κ against our pseudomeasure (0.12). (Of course, this is why chose it in the first place.) Only when we start to interpolate and allow, say, continuous p-adically valued multiplicative characters in place of κ will we need the basics of such p-adic integration.

(b) *Normalized p-adic pseudomeasure.* Now let L be the Mellin transform of an $\mathrm{SL}(2, \mathbb{Z})$-cusp form of weight $2k$ as above. Representing the characteristic function of the set $a + p^m\mathbb{Z}$ by a linear combination of the additive characters κ modulo p^m, and calculating $\Lambda_\kappa(\rho)$ as in (0.4), we see that $\mu_L(a+p^m\mathbb{Z}_p)$ is a linear combination of modular symbols $\{bp^{-m}, i\infty\}$, $b \in \mathbb{Z}$.

Conversely, we may take an appropriate linear combination of such measures and obtain the one that was used in [Manin 1973; 1974], namely

$$\mu_p(a + p^m\mathbb{Z}_p) := \varepsilon^{-m}\{ap^{-m}, i\infty\}_k - p^{2k-2}\varepsilon^{-m+1}\{ap^{-m+1}, i\infty\}_k. \tag{0.13}$$

Here ε is a root of the (inverted) p-factor of L: $\varepsilon^2 - a_p\varepsilon + p^{2k-1} = 0$. If one of the two roots is a p-adic unit, we get a bounded measure. In any case, its growth can be controlled. The appearance of two summands and ε in (0.13) is a slightly more sophisticated solution than the total discarding of the p-th Euler factor.

0.6. ***The ∞-adic Lévy–Mellin transform.*** As suggested in [Manin and Marcolli 2008], we make the following replacements in the picture sketched above.

Replace p by arithmetic infinity. Replace $\mathbb{Z}_p^*$ by the semiinterval $(0, 1]$.

Call the classical Farey intervals with ends $(g^{-1}(i\infty), g^{-1}(0))$, $g \in \mathrm{SL}(2, \mathbb{Z})$, *primitive segments.* They will be our replacement for the residue classes $a+p^m\mathbb{Z}_p$. Exactly as residue classes, two open primitive segments either do not intersect, or one of them is contained in another. For an abelian group W, call a pseudomeasure a W-valued finitely additive function on segments with rational ends (see additional details below).

A typical pseudomeasure in this sense is the modular symbol itself:

$$\mu(\alpha, \beta) = \{\alpha, \beta\}_k;$$

in particular, $\mu(\alpha, \infty) = \{\alpha, \infty\}_k$, which may be compared to (0.13).

As in the p-adic case, the pseudomeasure of a small segment is not small in the archimedean sense. However, now we cannot hope to compensate for this by the nonarchimedean effect referred to above.

Instead, we suggest using the following general feature of our constructions:

The Mellin transform of a cusp form, after suitable normalization, can be naturally written as the sum over rational numbers in (0, 1] *of values of a certain arithmetic function a:*

$$A := \sum_{\beta\in(0,1]\cap\mathbb{Q}} a(\beta). \tag{0.14}$$

The values $a(p/q)$ involved here are essentially modular symbols divided by a power of the denominator q. For details, see Section 2.

Generally, a convergent series of the form (0.14) gives rise to an archimedean integral in two related ways:

(i) *The first construction.* We can define a pseudomeasure $\mu = \mu_a$ on the boolean algebra generated by segments with *irrational* ends in [0, 1] putting

$$\mu(\alpha, \beta) := \sum_{\gamma\in(\alpha,\beta)\cap\mathbb{Q}} a(\gamma) \tag{0.15}$$

so that

$$A = \int_0^1 d\mu. \tag{0.16}$$

One can also treat (0.14) as a distribution on an appropriate space of test functions.

This is a direct analog of (0.12), however, it is not the version that we will use in this paper.

(ii) *The second construction.* Let r be a function defined on pairs of positive coprime integers (p, q), $p < q$ and decreasing sufficiently fast. For a real number ξ, denote by $q_i(\xi)$ the denominator of the i-th convergent to ξ, $i \geq 0$. We can introduce the Lévy 1-form $l(\xi)d\xi$, associated to r and defined on $(0, \frac{1}{2}]$ by the prescription

$$l(\xi) = l_r(\xi) = \sum_{i=0}^{\infty} r\big(q_i(\xi), q_{i+1}(\xi)\big). \tag{0.17}$$

According to a lemma by P. Lévy, for any pair (p, q) as above, the set of all $\xi \in (0, \frac{1}{2}]$ for which there exists i with $(p, q) = (q_i(\xi), q_{i+1}(\xi))$, fills a primitive semiinterval of length $1/((p+q)q)$. Moreover, this i is uniquely defined. Therefore, when $r(p, q)$ decreases sufficiently rapidly to assure convergence, we get

$$\int_0^{1/2} l_r(\xi)d\xi = \sum_{\alpha=p/q\in(0,1]} \frac{r(p, q)}{(p+q)q}. \tag{0.18}$$

In particular, we get A from (0.14) if we choose

$$r(p, q) := a(p/q)(p+q)q. \tag{0.19}$$

When A comes from a modular form (classical or Maass), so that the summands $a(\beta)$ are concocted of (classical or Maass) modular symbols, we will call the integral in (0.12) the ∞*-adic Lévy–Mellin transform.*

The Lévy functions and their generalizations appear also in a different context: that of linearizations of the germs of analytic diffeomorphisms of one complex variable z with an indifferent fixed point. For example, a germ with linear part $e^{2\pi i\xi}z$ is linearizable if and only if the Brjuno number of ξ,

$$b(\xi) := \sum_{i=0}^{\infty} \frac{\log q_{n+1}(\xi)}{q_n(\xi)}, \tag{0.20}$$

is finite. In fact, an interesting theory is developed/reviewed in [Marmi et al. 2001; 2006] for another Brjuno function $B(\xi)$, which differs from $b(\xi)$ by $O(1)$, but satisfies a functional equation and has a complex version closely resembling some constructions in the theory of modular forms. In our context, it can be used for calculation of the derivative of some classical L-series at certain points. This looks like an interesting variation on the subject of the Lévy–Mellin transform.

0.7. ***A summary of p-adic/∞-adic analogies.*** For clarity, we summarize the suggested analogies as follows:

$$\begin{array}{rcl}
\mathbb{Z}_p^* & \Longleftrightarrow & (0,1] \\
\cup & & \cup \\
\mathbb{Z} & \Longleftrightarrow & \mathbb{Q}\cap(0,1] \\
a+p^m\mathbb{Z}_p & \Longleftrightarrow & \text{primitive (Farey) segments} \\
\displaystyle\sum_{m=1}^{\infty}\frac{a_m}{m^\rho} & \Longleftrightarrow & \displaystyle\sum_{0<p/q\le 1}\frac{a(p/q)}{q^\rho} \\
\text{Mazur–Mellin transform} & \Longleftrightarrow & \text{Lévy–Mellin transform}
\end{array}$$

1. Pseudomeasures associated with period-like functions

1.1. ***A heuristic construction.*** For the moment, we adopt the viewpoint of [Lewis and Zagier 2001, Chapter II, Section 5]. Fix a complex number s such that $s(1-s)$ is an eigenvalue of the standard hyperbolic Laplace operator on $\mathbb{C}$ producing a $\mathrm{PSL}(2,\mathbb{Z})$-invariant Maass wave form $u(z) = u_s(z)$, $z \in H$. Define complex powers by the usual formula $t^s := e^{s\log t}$ where the branch of the logarithm is determined by the normalization $-\pi < \arg t \le \pi$. As shown in [Lewis and Zagier 1997], there exists a distribution $U(t) = U_s(t)$ on $\mathbb{R}$ whose values on the test functions of t given by

$$(\mathrm{Im}\,z)^s|z-t|^{-2s}, \quad (z-t)^{-2s}, \quad \chi_{(-\infty,0)}(t)(z-t)^{-2s}$$

(where z enters as a parameter) are respectively $u(z)$ (the initial Maass form), a function $f(z)$ holomorphic in $\mathbb{C}\setminus\mathbb{R}$, and a *period function* $\psi(z)$ defined and holomorphic in $\mathbb{C}' := \mathbb{C}\setminus(-\infty,0]$. Here χ is the characteristic function of $\mathbb{R}_-$; in other words,

$$\psi(z) = \int_{-\infty}^{0} (z-t)^{-2s}U(t)\,dt. \tag{1.1}$$

The distribution U is automorphic in the following sense: for all

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

we have

$$U\left(\frac{at+b}{ct+d}\right) = |ct+d|^{2-2s}U(t). \tag{1.2}$$

Thus, (1.1) has the same structure as (0.1).

Now consider only $g \in \mathrm{SL}(2,\mathbb{Z})$ *with nonnegative entries*. Then for any $z \in \mathbb{C}'$ we have also $gz := (az+b)/(cz+d) \in \mathbb{C}'$. From (1.2) we find formally

$$\psi(gz) = \int_{-\infty}^{0} (gz-t)^{-2s}U(t)\,dt = \int_{g^{-1}(-\infty)}^{g^{-1}(0)} (gz-g\tau)^{-2s}U(g\tau)\,d(g\tau). \tag{1.3}$$

A direct calculation using (1.2) reduces the integrand to the form

$$\left[\frac{z-\tau}{(cz+d)(c\tau+d)}\right]^{-2s} |c\tau+d|^{-2s+2}U(\tau)\frac{d\tau}{|c\tau+d|^2}. \tag{1.4}$$

Since $a \neq 0$, we have

$$g^{-1}(-\infty) = -\frac{d}{c} < -\frac{b}{a} = g^{-1}(0),$$

and hence for $\tau \in (g^{-1}(-\infty), g^{-1}(0))$ we have $c\tau+d > 0$. This shows that all terms involving $c\tau+d$ in (1.4) cancel, so that finally we find formally

$$\psi(gz) = (cz+d)^{2s}\int_{-d/c}^{-b/a} (z-\tau)^{-2s}U(\tau)\,d\tau. \tag{1.5}$$

Thus if $(\alpha,\beta) = (g^{-1}(-\infty), g^{-1}(0))$ with g as above, and if we put

$$\mu(\alpha,\beta)(z) := (cz+d)^{-2s}\psi(gz) = \int_{\alpha}^{\beta} (z-t)^{-2s}U(t)\,dt, \tag{1.6}$$

then for three intervals (α,β), (β,γ), (α,γ) of this type, we would have from (1.6)

$$\mu(\alpha,\beta)(z) + \mu(\beta,\gamma)(z) = \mu(\alpha,\gamma)(z). \tag{1.7}$$

As we will see, all primitive intervals in $\mathbb{R}_-$ are of this form, so we have formally constructed a premeasure (see below) on (the left half of) $\mathbb{P}^1(\mathbb{R})$, extendable to a pseudomeasure on this half with values in the space of holomorphic functions on $\mathbb{C}'$, in view of [Manin and Marcolli 2008, Theorem 1.8].

The weak point of this reasoning, about which the word "formally" is supposed to warn the reader, is this: the functions $\chi_{(\alpha,\beta)}(t)(z-t)^{-2s}$ generally do not belong to the space of test functions as defined in [Lewis and Zagier 1997, p. 225]. Therefore the integrals on the right-hand sides of (1.5) and (1.6) a priori make no sense.

Our heuristic reasoning is in fact a simple extension of the formal argument of [Lewis and Zagier 1997, p. 222], "proving" the three-term functional equation for $\psi(z)$.

In the next subsections, we will provide a precise construction of the pseudomeasures, whose values on the intervals considered above are given by

$$\mu\big(g^{-1}(-\infty), g^{-1}(0)\big)(z) := (cz+d)^{-2s}\psi(gz) \tag{1.8}$$

without appealing to the integral representation (1.6), but making use of the theory developed in [Lewis and Zagier 1997].

1.2. ***Preliminaries: left primitive segments.*** We recall some notions and facts from [Manin and Marcolli 2008]. We consider $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ as points of an affine line with a fixed coordinate z. Completing this line by one point $\infty = -\infty = i\infty$, we get points of the projective line $\mathbb{P}^1(\mathbb{Q}) \subset \mathbb{P}^1(\mathbb{R}) \subset \mathbb{P}^1(\mathbb{C})$ (Riemannian sphere). The group $\mathrm{GL}(2, \mathbb{C})$ acts on $\mathbb{P}^1(\mathbb{C})$ by fractional linear transformations. *Segments* are defined as nonempty connected subsets of $\mathbb{P}^1(\mathbb{R})$. A segment is called infinite if ∞ is in its closure; otherwise it is called finite. The boundary of each segment generally consists of an unordered pair of points (α, β) in $\mathbb{P}^1(\mathbb{R})$. We will identify a segment with the *ordered* pair of its ends: the additional element of structure is its orientation from α to β. For our purposes, it is usually inessential whether one or two boundary points belong to the segment. In this section we will consider mostly *left* segments, that is, ones for which $-\infty \le \alpha$ and $\beta \le 0$. One-point segments are sometimes called improper ones.

A segment is called *rational* if its ends are in $\mathbb{P}^1(\mathbb{Q})$, and *primitive*, or Farey, if it is of the form $(g(\infty), g(0))$ for some $g \in \mathrm{GL}(2, \mathbb{Z})$.

A *pseudomeasure with values in an abelian group W* is a finitely additive W-valued function on the boolean algebra of rational segments, vanishing on improper segments. We extended it to oriented segments by the condition that $\mu(\alpha, \beta) = -\mu(\beta, \alpha)$.

In this section, we will construct pseudomeasures supported by left segments. Each such pseudomeasure is defined by its restriction to the set P of positively oriented left primitive segments. We will use the following enumeration of the latter.

Denote by $S \subset \mathrm{SL}(2,\mathbb{Z})$ the subsemigroup of matrices with nonnegative entries a, b, c, and d. For any $g \in S$, $(g^{-1}(-\infty), g^{-1}(0))$ is in P. In fact, if $c \neq 0$,

$$g^{-1}(\infty) = \frac{d}{-c} < g^{-1}(0) = \frac{-b}{a},$$

because $ad - bc = 1$. If $c = 0$, then $a = d = 1$, and again

$$g^{-1}(\infty) = -\infty < g^{-1}(0) = -b.$$

Finally, the case $a = 0$ does not occur in S.

One easily sees that this map $S \to P$: $g \mapsto (g^{-1}(-\infty), g^{-1}(0))$ is in fact a bijection.

1.3. ***Preliminaries: the slash operators of complex weight.*** Here we summarize the considerations of [Lewis and Zagier 2001, p. 240] and [Hilgert et al. 2005, Section 3]. They determine a partial map

$$(\varphi, g) \mapsto \varphi|_s g, \tag{1.9}$$

allowing us to make sense of and correctly calculate expressions such as those appearing in (1.4) and (1.6). For proofs, see [Hilgert et al. 2005].

(i) *Definition domain.* The argument $\varphi = \varphi(z)$ in (1.9) can be an arbitrary function holomorphic in some domain of the form $\mathbb{C} \setminus (-\infty, r]$, $r \in \mathbb{R}$. Such functions form a $\mathbb{C}$-algebra which we will denote $\mathcal{F}$. Period functions $\psi = \psi_s$ belong to $\mathcal{F}$.

Hilgert et al. call any point r such that $\varphi \in \mathcal{F}$ is holomorphic in $\mathbb{C} \setminus (-\infty, r]$ a *branching point* of φ.

The argument g in (1.9) can be any $(2, 2)$-matrix $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with integer entries and nonzero determinant such that either $c > 0$ or else $c = 0$ and $a, d > 0$. Denote by $\mathcal{G}$ the set of such matrices. The set S describing left primitive segments in Section 1.2 is a subset of $\mathcal{G}$. When $g \in \mathcal{G}$ and $s \in \mathbb{C}$, the function $(cz + d)^s$ belongs to $\mathcal{F}$.

A pair $(\varphi, g) \in \mathcal{F} \times \mathcal{G}$ belongs to the definition domain $\mathcal{DS}$ of the slash operator (1.9) if φ admits a branching point r such that either $a - cr > 0$, or $a - cr = 0$ and $dr - b < 0$. For a period function $\varphi = \psi$, we can take $r = 0$, and g will do if $a > 0$ or if $a = 0$ and $b > 0$.

Let $\mathcal{G}^+$ be the set of matrices in $\mathcal{G}$ such that $b, d \geq 0$ and either $a > 0$, or $a = 0$ and $b > 0$. Again, $S \subset \mathcal{G}^+$. Denote by $\mathcal{F}_0$ the subspace of $\mathcal{F}$ admitting 0 as a branch point. Then $\mathcal{F}_0 \times \mathcal{G}^+ \subset \mathcal{DS}$.

(ii) *Slash operator of weight s.* It is the map $\mathcal{DS} \to \mathcal{F}$ defined by

$$(\varphi(z), g) \mapsto (\varphi|_s g)(z) := |\det g|^s (cz + d)^{-2s} \varphi(gz). \tag{1.10}$$

It is well defined. Moreover, it sends $\mathcal{F}_0 \times \mathcal{G}^+$ to $\mathcal{F}_0$.

(iii) *Properties of the slash operator.* The basic property is that slash operator is an honest action: if $g_1, g_2 \in \mathcal{G}$ and $(\varphi, g_1), (\varphi|_s g_1, g_2), (\varphi, g_1 g_2) \in \mathcal{D}\mathcal{S}$, then

$$\varphi|_s(g_1 g_2) = (\varphi|_s g_1)|_s g_2.$$

(Formally, it is the associativity of the triple product of φ, g_1, g_2.) Applying this to $\mathcal{F}_0 \times \mathcal{G}^+$, one can check that $|_s$ defines a right action of the multiplicative semigroup $\mathcal{G}^+$ on $\mathcal{F}_0$ [Hilgert et al. 2005, Remark 3.4].

From Section 1.2 one sees that if $(g^{-1}(-\infty), g^{-1}(0))$ is a left primitive segment, then $g \in \mathcal{G}^+$. Since $\psi \in \mathcal{F}_0$ in the first equality of (1.6), this expression for $\mu(\alpha, \beta)(z)$ (disregarding the second equality and the poorly defined integral) makes sense, and the slash action can be further iterated.

1.4. ***The premeasures related to period-like functions.*** Choose a complex number s and a function $\psi(z) \in \mathcal{F}_0$ satisfying the three term functional equation

$$\psi(z) = \psi(z+1) + (z+1)^{-2s}\psi\left(\frac{z}{z+1}\right). \tag{1.11}$$

Thus, ψ is a period-like function in the sense of [Lewis and Zagier 2001, Chapter III].

For a left primitive segment $(\alpha, \beta) = (g^{-1}(-\infty), g^{-1}(0))$, put

$$\tilde{\mu}(\alpha, \beta)(z) = (cz+d)^{-2s}\psi(gz) = \psi|_s(z). \tag{1.12}$$

Consider now the three left primitive segments $(\alpha, \beta) = (g_1^{-1}(-\infty), g_1^{-1}(0))$, $(\beta, \gamma) = (g_2^{-1}(-\infty), g_2^{-1}(0))$, and $(\alpha, \gamma) = (g_3^{-1}(-\infty), g_3^{-1}(0))$. In plain words, the third segment is broken into two others by a point β in the middle.

Lemma 1.4.1. *We have*

$$\tilde{\mu}(\alpha, \beta)(z) + \tilde{\mu}(\beta, \gamma)(z) = \tilde{\mu}(\alpha, \gamma)(z). \tag{1.13}$$

Proof. Case 1. $(\alpha, \beta, \gamma) = (-\infty, -1, 0)$. In this case

$$g_1 = T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad g_2 = T' := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad g_3 = I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and (1.13) coincides with (1.11) which can be written as

$$\psi|_s I = \psi|_s T + \psi|_s T'. \tag{1.14}$$

Case 2. $g_1 = Tg$, $g_2 = T'g$, and $g_3 = g$, where $g \in \mathrm{SL}(2, \mathbb{Z})$ is a matrix with nonnegative entries. In this case, (1.13) reads

$$\psi|_s g = \psi|_s Tg + \psi|_s T'g,$$

which obviously holds in view of (1.14) and the associativity of the slash operator restricted to $\mathcal{F}_0 \times \mathcal{G}^+$.

General case. In fact, the previous case *is* general: we necessarily have $g_1 = Tg_3$ and $g_2 = T'g_3$.

Let us check this for the case when $\alpha \neq -\infty$ leaving the remaining case to the reader. Put $\alpha = d/-c$ and $\gamma = -b/a$ as in Section 1.2 where (a, b, c, d) are the entries of g_3. Then the only possible value of β is $\beta = -(b+d)/(a+c) = (b+d)/-(a+c)$ as is well known from the classical theory of Farey series. This fact directly translates into $g_1 = Tg_3$ and $g_2 = T'g_3$. □

Remark. Notice that if $\psi(z)$ is an actual period function for a Maass wave form, the lemma becomes obvious in view of the integral representation of $\psi(z)$ proven in [Lewis and Zagier 2001, Chapter II, Section 1]. The relevant formula on p. 212 of that reference, with ψ_1 replace by ψ and a change in sign, is

$$(c\zeta + d)^{-2s}\psi(g\zeta) = \int_{g^{-1}(\infty)}^{g^{-1}(0)} \{u, R^s_\zeta\}(z). \tag{1.15}$$

In this formula, we integrate a closed form along an arbitrary path leaving ζ and $\bar{\zeta}$ to the right of it. Additivity (1.13) becomes evident.

We will use this integral representation in the next section.

1.4.2. *The premeasure on left segments.* To define a premeasure in the sense of [Manin and Marcolli 2008], *supported by the subset of left primitive segments*, it remains to complete (1.12) of the function $\tilde{\mu}$ by putting for $\alpha < \beta \leq 0$

$$\tilde{\mu}(\beta, \alpha) := -\tilde{\mu}(\alpha, \beta), \quad \tilde{\mu}(\alpha, \alpha) = 0.$$

One easily checks that (1.13) continues to hold on this extended domain.

1.5. ***The pseudomeasure related to a period-like function.*** Now we can state the main result of this section.

Theorem 1.5.1. *There exists a unique finitely additive function μ with values in $\mathcal{F}_0$ coinciding with $\tilde{\mu}$ on left primitive segments and vanishing on all rational segments in* $(0, \infty)$.

Sketch of proof. We recall the plan of the proof of [Manin and Marcolli 2008, Theorem 1.8]. It consists of the following steps.

(1) Using the "continued fractions trick", we show that for any nonpositive rational (or infinite) α and β one can find a sequence of rational nonpositive numbers $\alpha_0 = \alpha, \alpha_1, \dots, \alpha_n = \beta$ such that (α_i, α_{i+1}) is a left primitive segment for all $i = 0, \dots, n-1$. Such a sequence is called a primitive chain connecting α to β.

(2) Having chosen such a primitive chain, we put

$$\mu(\alpha, \beta) := \sum_{i=0}^{n-1} \tilde{\mu}(\alpha_i, \alpha_{i+1}). \tag{1.16}$$

(3) The fact that (1.16) does not depend on the choice of the connecting primitive chain is checked by proving that any two chains can be transformed one to another by using "elementary moves" compatible with relations that hold for $\tilde{\mu}$. An elementary move essentially replaces a Farey interval $\left(\frac{a}{c}, \frac{b}{d}\right)$ by the chain $\left(\frac{a}{c}, \frac{a+b}{c+d}\right), \left(\frac{a+b}{c+d}, \frac{b}{d}\right)$, or vice versa.

(4) Finally, we have to check that (1.16) implies finite additivity and the sign change after the change of orientation. This is straightforward.

1.6. ***Modularity.*** Let Γ be a subgroup of $\mathrm{SL}(2, \mathbb{Z})$ and W a left Γ-module.

In [Manin and Marcolli 2008], a pseudomeasure μ with values in W is called Γ*-modular* if for all $g \in \Gamma$ and $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$ we have

$$\mu(g\alpha, g\beta) = g\mu(\alpha, \beta).$$

It was checked that such pseudomeasures correspond to parabolic 1-cocycles.

In our context, this is replaced by the following property: for all g with $g^{-1} \in S$ and any left segment (α, β),

$$\mu(g^{-1}(\alpha), g^{-1}(\beta)) = \mu(\alpha, \beta)|_s g. \tag{1.17}$$

In fact, it suffices to check this for left primitive segments, say

$$(\alpha, \beta) = (h^{-1}(-\infty), h^{-1}(0)),$$

in which case we have

$$\begin{aligned}\mu\big(g^{-1}(\alpha), g^{-1}(\beta)\big) &= \mu\big((hg)^{-1}(-\infty), (hg)^{-1}(0)\big)\\ &= \psi|_s(hg) = (\psi|_s h)|_s g = \mu(\alpha, \beta)|_s g.\end{aligned}$$

Since the right slash action of g can be considered as the left action of g^{-1}, we can say that (1.17) expresses the modularity of μ with respect to the multiplicative semigroup $S^{-1} \subset \mathrm{SL}(2, \mathbb{Z})$.

2. Maass L-functions and their Mellin–Lévy transforms

2.1. ***Maass L-series as sums over rational numbers.*** Let $u = u_s$ be a Maass cusp form, which is an eigenfunction with respect to all Hecke operators

$$T_m := \sum_{\substack{ad=m \\ 0<b\le d}} \begin{pmatrix} a & -b \\ 0 & d \end{pmatrix} \tag{2.1}$$

acting via the slash operator of weight 0: $u \mapsto u|_0 T_m = \lambda_m u$.

Put

$$L_u(\rho) := \sum_{m=1}^{\infty} \frac{\lambda_m}{m^\rho}. \tag{2.2}$$

The action of the Hecke operators on u induces an action on the period functions, which can be explicitly described by a nice formula, for example, as in [Mühlenbruch 2004]. However, we will need a different expression, involving the pseudomeasure μ_u, and we will start with an heuristic derivation of it, as in Section 1.1.

Let us formally apply the slash operator $|_{-s}$ of (1.10) to the boundary measure $U(t)\,dt$ and denote the resulting action upon the respective period function ψ by T_m^*. In this heuristic calculation we "define" ψ by (1.1). The choice of weight $-s$ is motivated by the invariance property (1.2). We get

$$\begin{aligned}(\psi \mid T_m^*)(\zeta) &:= \int_{-\infty}^{0} (\zeta - t)^{-2s} (U(t)\,dt|_{-s} T_m) \\ &= \sum_{\substack{ad=m\\ 0<b\le d}} \left(\frac{d}{a}\right)^s \int_{-\infty}^{0} (\zeta - t)^{-2s} U\left(\frac{at-b}{d}\right) d\left(\frac{at-b}{d}\right).\end{aligned}$$

Make the change of variable $\tau = \dfrac{at-b}{d}$. The last integral takes the form

$$\begin{aligned}\sum_{\substack{ad=m\\ 0<b\le d}} \left(\frac{d}{a}\right)^s &\int_{-\infty}^{-b/d} \left(\zeta - \frac{d\tau+b}{a}\right)^{-2s} U(\tau)\,d\tau \\ &= \sum_{\substack{ad=m\\ 0<b\le d}} \left(\frac{d}{a}\right)^s \int_{-\infty}^{-b/d} \left(\frac{dz+b}{a} - \frac{d\tau+b}{a}\right)^{-2s} U(\tau)\,d\tau,\end{aligned}$$

where $z = \dfrac{a\zeta - b}{d}$. The integral in the last sum can be rewritten as

$$\left(\frac{a}{d}\right)^{2s} \int_{-\infty}^{-b/d} (\zeta - \tau)^{-2s} U(\tau)\,d\tau.$$

Thus, heuristically,

$$\begin{aligned}(\psi \mid T_m^*)(\zeta) = (\mu(-\infty, 0) \mid T_m^*)(\zeta) &= \sum_{\substack{ad=m\\ 0<b\le d}} \left(\frac{a}{d}\right)^s \mu\left(-\infty, -\frac{b}{d}\right)\left(\frac{a\zeta-b}{d}\right) \\ &= \sum_{\substack{ad=m\\ 0<b\le d}} \mu\left(-\infty, -\frac{b}{d}\right)\Big|_s \begin{pmatrix} a & -b \\ 0 & d \end{pmatrix} (\zeta). \end{aligned} \tag{2.3}$$

This expression is useful for our purposes because it allows us to represent the (somewhat normalized) Dirichlet series $L_u(s)$ as a natural sum over rational numbers. We will state now the respective theorem:

Theorem 2.2. *We have*

$$\psi(z)\sum_{m=1}^{\infty}\frac{\lambda_m}{m^\rho} = \zeta(\rho-s)\,\zeta(\rho+s)\sum_{q=1}^{\infty}\frac{1}{q^\rho}\sum_{\substack{0<p\le q\\(p,q)=1}}\mu(-\infty,-p/q)|_s\begin{pmatrix}1 & -p\\ 0 & q\end{pmatrix}(z). \tag{2.4}$$

Proof. Step 1. First, we have to supply an honest proof of (2.3). In [Lewis and Zagier 2001, Chapter II, Section 2], the authors construct a differential 1-form $\{u, R_\zeta^s\}(z)$ which we invoked at the end of Lemma 1.4.1. It has the following properties:

(i) $\{u, R_\zeta^s\}(z)$ is a closed smooth form of z varying in the complex upper half-plane H. It depends on the parameter $\zeta\in\mathbb{C}$ holomorphically when $z\neq\zeta,\bar\zeta$. Generally it is multivalued, but a well-defined branch can be chosen on the complement in H of a path joining ζ to $\bar\zeta$.

(ii) The period function $\psi(\zeta)$, $\zeta\in H$ for u (up to a constant proportionality factor) can be then written as an integral:

$$\psi(\zeta)=\int_{-\infty}^{0}\{u, R_\zeta^s\}(z) \tag{2.5}$$

taken along any path in H leaving ζ to the left of it.

Now assume that $u|_0 T_m=\lambda_m u$ for T_m from (2.1) and a constant λ_m. Then we have from (2.5) and (2.1)

$$\lambda_m\psi(\zeta)=\int_{-\infty}^{0}\Big\{\sum_{\substack{ad=m\\0<b\le d}}u\Big(\frac{az-b}{d}\Big), R_\zeta^s\Big\}(z). \tag{2.6}$$

For each a, b, and d fixed, we first want to make the implicit argument z of R_ζ^s the same as that of u, i.e., $(az-b)/d$. We have (see [Lewis and Zagier 2001, p. 211]):

$$R_\zeta(z)=\frac{i}{2}\big((z-\zeta)^{-1}-(\bar z-\zeta)^{-1}\big)= \frac{a}{d}\cdot\frac{i}{2}\bigg(\Big(\frac{az-b}{d}-\frac{a\zeta-b}{d}\Big)^{-1}-\Big(\frac{a\bar z-b}{d}-\frac{a\zeta-b}{d}\Big)^{-1}\bigg)=\frac{a}{d}R_\xi\Big(\frac{az-b}{d}\Big),$$

where $\xi:=(a\zeta-b)/d$.

Substituting this into (2.6), we obtain

$$\lambda_m\psi(\zeta)=\sum_{\substack{ad=m\\0<b\le d}}\Big(\frac{a}{d}\Big)^s\int_{-\infty}^{0}\Big\{u\Big(\frac{az-b}{d}\Big), R^s_{(a\zeta-b)/d}\Big(\frac{az-b}{d}\Big)\Big\}. \tag{2.7}$$

Considering now $z \mapsto (az-b)/d$ as a holomorphic change of variables, we infer from [Lewis and Zagier 2001, Lemma, p. 210] that the integrand in the respective term of (2.7) can be rewritten as

$$\{u,\, R^s_{(a\zeta-b)/d}\}\left(\frac{az-b}{d}\right).$$

Hence, finally,

$$\begin{aligned}\lambda_m \psi(\zeta) &= \sum_{\substack{ad=m\\0<b\le d}} \left(\frac{a}{d}\right)^s \int_{-\infty}^{-b/d} \{u,\, R^s_{(a\zeta-b)/d}\}(z)\\ &= \sum_{\substack{ad=m\\0<b\le d}} \mu(-\infty, -b/d)|_s \begin{pmatrix} a & -b\\ 0 & d\end{pmatrix}(\zeta).\end{aligned} \tag{2.8}$$

This is formula (2.3), written for u which is an eigenfunction of T_m, and its respective period function.

Step 2. Multiply (2.8) by $m^{-\rho}$ and sum over all $m = 1, 2, \ldots$. Again replacing the free variable ζ by z, to avoid confusion with Riemann's zeta, we obtain

$$\psi(z)\sum_{m=1}^{\infty}\frac{\lambda_m}{m^\rho} = \sum_{m=1}^{\infty}\frac{1}{m^\rho}\sum_{\substack{ad=m\\0<b\le d}} \mu(-\infty, -b/d)|_s \begin{pmatrix} a & -b\\ 0 & d\end{pmatrix}(z). \tag{2.9}$$

Each matrix in (2.9) can be uniquely written in the following way:

$$\begin{pmatrix} a & -b\\ 0 & d\end{pmatrix} = \begin{pmatrix} d_2 & -pd_1\\ 0 & qd_1\end{pmatrix} = \begin{pmatrix} 1 & -p\\ 0 & q\end{pmatrix}\begin{pmatrix} 1 & 0\\ 0 & d_1\end{pmatrix}\begin{pmatrix} d_2 & 0\\ 0 & 1\end{pmatrix}, \tag{2.10}$$

where $m = d_1 d_2 q$, $d_i \ge 1$, and $0 < p \le q$, $(p, q) = 1$. Moreover, the arbitrary quadruple (d_1, d_2, p, q) satisfying these conditions produces one term in (2.9).

From (2.10) and the associativity of the slash operator (1.10) it follows that

$$|_s \begin{pmatrix} a & -b\\ 0 & d\end{pmatrix} = |_s \begin{pmatrix} 1 & -p\\ 0 & q\end{pmatrix}\cdot d_1^{-s} d_2^{s}.$$

Hence we can rewrite (2.9) as follows:

$$\psi(z)\sum_{m=1}^{\infty}\frac{\lambda_m}{m^\rho} = \sum_{q,d_1,d_2=1}^{\infty}\frac{1}{q^\rho d_1^{\rho-s} d_2^{\rho+s}}\sum_{\substack{0<p\le q\\(p,q)=1}} \mu(-\infty, -p/q)|_s \begin{pmatrix} 1 & -p\\ 0 & q\end{pmatrix}(z). \tag{2.11}$$

This last expression is seen to be equal to the right-hand side of (2.4), concluding the proof. □

2.3. ***The Lévy–Mellin transform.*** Now put

$$r_u(p,q) := (p+q)q^{1-\rho}\mu(-\infty,-p/q)|_s \begin{pmatrix}1 & -p\\ 0 & q\end{pmatrix}(z)\cdot\psi(z)^{-1}$$

and

$$l_u(\xi) := \sum_{i=0}^{\infty}\sum_{i=0}^{\infty} r\big(q_i(\xi), q_{i+1}(\xi)\big).$$

From (2.4) and (0.18) we get:

Corollary 2.3.1. *Let u be a Maass cusp form, $\Delta u = s(1-s)u$, and $u \mid T_m = \lambda_m u$ for all $m \geq 1$. Put*

$$\Lambda_u(\rho) := \zeta(\rho-s)^{-1}\zeta(\rho+s)^{-1}\sum_{m=1}^{\infty}\frac{\lambda_m}{m^\rho}.$$

Then

$$\Lambda_u(\rho) = \int_0^{1/2} l_u(\xi)\,d\xi.$$

Remark 2.3.2. The class of series of the form (0.18) involving modular symbols includes also the Eisenstein series of [Goldfeld 1999]. They certainly deserve further study.

2.4. ***Hecke operators on period functions via continued fractions.*** Consider the sequence of normalized convergents b/d as in [Manin and Marcolli 2008, (1.5)]. When $0 < b/d < 1$, it starts with

$$-\infty = \frac{1}{0} =: \frac{b_{-1}}{d_{-1}},\quad 0 = \frac{0}{1} =: \frac{b_0}{d_0}, \dots, b/d = \frac{b_n}{d_n},$$

where $n = n(b/d)$ is the length of the continued fraction expansion.

The following sequence of left primitive segments $I_k = I_k(b/d)$ connects $-\infty$ to $-b/d$. We order their ends from the left one to the right one, and put a minus before those that should be run in the opposite direction in our chain:

$$I_0 = (-\infty, 0) = \left(-\frac{b_{-1}}{d_{-1}}, -\frac{b_0}{d_0}\right),\quad I_1 = -\left(-\frac{b_1}{d_1}, -\frac{b_0}{d_0}\right),$$
$$I_2 = \left(-\frac{b_1}{d_1}, -\frac{b_2}{d_2}\right),\quad I_3 = -\left(-\frac{b_3}{d_3}, -\frac{b_2}{d_2}\right),$$

and generally

$$I_k = (-1)^k\left(-\frac{b_{k-\varepsilon_k}}{d_{k-\varepsilon_k}}, -\frac{b_{k-\varepsilon_{k+1}}}{d_{k-\varepsilon_{k+1}}}\right)$$

where $\varepsilon_k = 1$ for even k and $\varepsilon_k = 0$ for odd k.

This means that

$$(-1)^k I_k = \big(g_k^{-1}(-\infty), g_k^{-1}(0)\big) \tag{2.12}$$

where

$$g_k = g_{k,b/d} = \begin{pmatrix} d_{k-\varepsilon_{k+1}} & b_{k-\varepsilon_{k+1}} \\ d_{k-\varepsilon_k} & b_{k-\varepsilon_k} \end{pmatrix} \in S. \tag{2.13}$$

Therefore, (2.8) can be rewritten as

$$\lambda_m \psi(\zeta) = \sum_{\substack{ad=m\\0<b\le d}} \left(\frac{a}{d}\right)^s \sum_{k=0}^{n(b/d)} (-1)^k \int_{-\infty}^0 \{u(g_{k,b/d}(z)),\, R^s_{(a\zeta-b)/d}(g_{k,b/d}(z))\}. \tag{2.14}$$

We have $u(g_{k,b/d}(z)) = u(z)$ and

$$R^s_{(a\zeta-b)/d}(g_{k,b/d}(z)) = \left(d_{k-\varepsilon_k} g^{-1}_{k,b/d}\left(\frac{a\zeta-b}{d}\right) + b_{k-\varepsilon_k}\right)^{2s} R^s_{g^{-1}_{k,b/d}((a\zeta-b)/d)}(z). \tag{2.15}$$

This follows from the formula (2.6) on [Lewis and Zagier 2001, p. 211] and (2.13). To shorten notation, set

$$j_k(b/d,\zeta)^{2s} := \left(d_{k-\varepsilon_k} g^{-1}_{k,b/d}\left(\frac{a\zeta-b}{d}\right) + b_{k-\varepsilon_k}\right)^{2s}. \tag{2.16}$$

Then we get

$$\begin{aligned}\lambda_m \psi(\zeta) &= \sum_{\substack{ad=m\\0<b\le d}} \left(\frac{a}{d}\right)^s \sum_{k=0}^{n(b/d)} (-1)^k j_k(b/d,\zeta)^{2s} \int_{-\infty}^0 \{u(z),\, R^s_{g^{-1}_{k,b/d}((a\zeta-b)/d)}(z)\} \\ &= \sum_{\substack{ad=m\\0<b\le d}} \left(\frac{a}{d}\right)^s \sum_{k=0}^{n(b/d)} (-1)^k j_k(b/d,\zeta)^{2s} \psi\left(g^{-1}_{k,b/d}\left(\frac{a\zeta-b}{d}\right)\right). \end{aligned} \tag{2.17}$$

In order to deduce from (2.17) a nice explicit formula for λ_m, as was done in [Manin 1973] for the coefficients of the classical cusp forms, one could use an appropriate linear functional on functions of ζ. In the classical case, it was the highest coefficient (or the constant term) of the period polynomial.

In the Maass case, one could try to use asymptotic behaviors at 0 or ∞. Other forms of Hecke operators, as (2.18), might be useful.

2.5. ***Hecke operators and transfer operator.*** In [Mühlenbruch 2004] it is shown, using the method of [Choie and Zagier 1993], that the Hecke operators acting on period functions for the full modular group can be written in the nice form

$$T_m^+ = \sum_{\substack{a>c\ge 0\\ d>b\ge 0\\ ad-bc=m}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2.18}$$

Of course, they act on $\psi(z)$ via $|_s$ in our notation. (Mühlenbruch denotes this slash operator by $|_{2s}$.) In particular, for $m=1$ we have $T_m^+ = I$.

However, if we change the summation domain slightly, replacing $a > c \geq 0$ by $a \geq c > 0$, then the equations for case $m = 1$ will admit the following solutions. From $ad = 1 + bc \leq 1 + (d-1)a$ it follows that $a = c = 1$ and $d = b + 1 \geq 1$ so that we will get the operator

$$T_1^* := \sum_{b=0}^{\infty} \begin{pmatrix} 1 & b \\ 1 & b+1 \end{pmatrix}. \tag{2.19}$$

This correction is not as ad hoc as it seems. In fact, if we compare it with the Atkin–Lehner operators for the group $\Gamma_0(N)$ and p/N,

$$U_p := T_p - p \cdot \mathrm{id},$$

we will see that T_1^* imitates the "characteristic 1" Atkin–Lehner operator corresponding to the "improper prime $p = 1$", with eigenvalue 1 on ψ:

Claim 2.5.1. If $\psi(z)$ is a period function for a Maass cusp form of weight s with $\operatorname{Re} s > 0$, $s \neq \frac{1}{2}$, then

$$\psi|_s T_1^*(z) = \psi(z). \tag{2.20}$$

Proof. Assume moreover that

$$\psi^\tau(z) := \psi|_s \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}(z) = \varepsilon\psi(z), \quad \varepsilon = \pm 1, \tag{2.21}$$

so that ψ is even or odd. This is not a restriction because any ψ is the sum of an even and an odd period function.

According to [Lewis and Zagier 2001, p. 255], the function

$$h(z) := \psi(z+1) = \psi|_s \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(z) \tag{2.22}$$

satisfies the equation

$$\varepsilon h|_s \left(\sum_{n=1}^{\infty} \begin{pmatrix} 0 & 1 \\ 1 & n \end{pmatrix} \right)(z) = h(z). \tag{2.23}$$

Substituting first (2.22) into (2.23), and then (2.21) into the resulting identity, yields

$$\psi|_s \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}|_s \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}|_s \left(\sum_{n=1}^{\infty} \begin{pmatrix} 0 & 1 \\ 1 & n \end{pmatrix} \right)(z) = \psi|_s \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(z). \tag{2.24}$$

The associativity of the slash operator and the identity

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & n \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n-1 \\ 0 & n \end{pmatrix}$$

establish (2.20). $\square$

2.6. ***The Brjuno function and derivatives of the classical L-functions.*** The Brjuno function of (0.20) is defined in this context as a generalized Lévy sum

$$B(\xi) := \sum_{j=0}^{\infty} |p_j(\xi) - q_j(\xi)\xi| \log \frac{p_{j-1}(\xi) - q_{j-1}(\xi)\xi}{q_j(\xi)\xi - p_j(\xi)}. \tag{2.25}$$

This series diverges on a set of measure 0. Outside it converges to a measurable function, continuous at irrational points, with period 1 [Marmi et al. 2006].

The values of derivatives of Mellin transforms of classical forms were studied by D. Goldfeld [1995] and Diamantis [1999]. Goldfeld's idea consisted in replacing the $\log y$ initially appearing in the Mellin expression for the first derivative by the logarithm of the η-function, or a combination of such, to enhance the modular properties of the integrand. The same game can be played with the Brjuno function in place of the η-function.

Consider a classical cusp form $u(z)$ for $\mathrm{SL}(2, Z)$ of integral weight $2k = w + 2$ as on page 1092. Let $L_u(s)$ be its Mellin transform.

Proposition 2.6.1. *We have*

$$L'_u(w/2+2) = C\left(-\int_0^1 u(iy)y^{w/2}B(y)\,dy + \int_1^\infty u(iy)y^{w/2-1}B(y)\,dy\right), \tag{2.26}$$

where

$$C = \frac{(2\pi)^{(w+4)/2}}{\Gamma((w+2)/2)}(1+i^{w+2}).$$

Proof. An easy calculation shows that $B(\xi)$ satisfies the functional equation

$$B(\xi) = -\log \xi + \xi B(\xi^{-1}), \quad \xi \in (0, 1). \tag{2.27}$$

Therefore, we have

$$\int_0^\infty u(iy)y^{w/2}\log y\,dy$$
$$= \int_0^1 u(iy)y^{w/2}\big(-B(y)+yB(y^{-1})\big)\,dy + \int_1^\infty u(iv)v^{w/2}\big(v^{-1}B(v)-B(v^{-1})\big)\,dv.$$

In the second summand of the second integrand, make the change of variable $v = y^{-1}$, and combine it with the first summand of the first integrand. Similarly, in the second summand of the first integrand, make the change of variable $y = v^{-1}$, and combine it with the first summand of the second integrand. This will result in

$$(1+i^{w+2})\left(-\int_0^1 u(iy)y^{w/2}B(y)\,dy + \int_1^\infty u(iy)y^{w/2-1}B(y)\,dy\right).$$

The remaining factor in C comes from the Mellin transform. □

Acknowledgement. I am grateful to Don Zagier, who read a preliminary draft of this paper and suggested a number of corrections and complements.

References

[Choie and Zagier 1993] Y. Choie and D. Zagier, "Rational period functions for PSL(2, **Z**)", pp. 89–108 in *A tribute to Emil Grosswald: number theory and related analysis*, edited by M. Knopp and M. Sheingorn, Contemp. Math. **143**, Amer. Math. Soc., Providence, RI, 1993. MR 94g:11033 Zbl 0790.11044

[Diamantis 1999] N. Diamantis, "Special values of higher derivatives of L-functions", *Forum Math.* **11**:2 (1999), 229–252. MR 2000a:11075 Zbl 0932.11032

[Goldfeld 1995] D. Goldfeld, "Special values of derivatives of L-functions", pp. 159–173 in *Number theory* (Halifax, NS, 1994), edited by K. Dilcher, CMS Conf. Proc. **15**, Amer. Math. Soc., Providence, RI, 1995. MR 96h:11039 Zbl 0845.11021

[Goldfeld 1999] D. Goldfeld, "Zeta functions formed with modular symbols", pp. 111–121 in *Automorphic forms, automorphic representations, and arithmetic* (Fort Worth, TX, 1996), edited by R. S. Doran et al., Proc. Sympos. Pure Math. **66**, Amer. Math. Soc., Providence, RI, 1999. MR 2000g:11039 Zbl 0934.11026

[Hilgert et al. 2005] J. Hilgert, D. Mayer, and H. Movasati, "Transfer operators for $\Gamma_0(n)$ and the Hecke operators for the period functions of PSL(2, $\mathbb{Z}$)", *Math. Proc. Cambridge Philos. Soc.* **139**:1 (2005), 81–116. MR 2006c:11057 Zbl 1129.11022

[Lewis and Zagier 1997] J. Lewis and D. Zagier, "Period functions and the Selberg zeta function for the modular group", pp. 83–97 in *The mathematical beauty of physics* (Saclay, 1996), edited by J. M. Drouffe and J. B. Zuber, Adv. Ser. Math. Phys. **24**, World Sci. Publ., River Edge, NJ, 1997. MR 99c:11108 Zbl 1058.11544

[Lewis and Zagier 2001] J. Lewis and D. Zagier, "Period functions for Maass wave forms, I", *Ann. of Math.* (2) **153**:1 (2001), 191–258. MR 2003d:11068 Zbl 1061.11021

[Maass 1949] H. Maass, "Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen", *Math. Ann.* **121** (1949), 141–183. MR 11,163c Zbl 0033.11702

[Manin 1972] Y. I. Manin, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 19–66. In Russian; translated in *Math. USSR-Izv.* **6** (1972), 19–64. MR 47 #3396 Zbl 0243.14008

[Manin 1973] Y. I. Manin, "The periods of modular forms and p-adic Hecke series", *Mat. Sb.* (*N.S.*) **92(134)** (1973), 378–401. In Russian; translated in *Math. USSR-Sb.* **21**:3 (1973), 371–393. MR 49 #10638 Zbl 0293.14007

[Manin 1974] Y. I. Manin, "The values of p-adic Hecke series at integer points of the critical strip", *Math. USSR, Sb.* **22**:4 (1974), 631–637. Zbl 0304.14013

[Manin and Marcolli 2008] Y. I. Manin and M. Marcolli, "Modular shadows and the Lévy–Mellin ∞-adic transform", pp. 189–238 in *Modular forms on Schiermonnikoog*, edited by B. Edixhoven et al., Cambridge Univ. Press, 2008. MR 2512362 Zbl 05503855

[Marmi et al. 2001] S. Marmi, P. Moussa, and J.-C. Yoccoz, "Complex Brjuno functions", *J. Amer. Math. Soc.* **14**:4 (2001), 783–841. MR 2003a:37061 Zbl 1051.37021

[Marmi et al. 2006] S. Marmi, P. Moussa, and J.-C. Yoccoz, "Some properties of real and complex Brjuno functions", pp. 601–623 in *Frontiers in number theory, physics, and geometry, I*, edited by P. Cartier et al., Springer, Berlin, 2006. MR 2009d:37071 Zbl 1134.37018

[Mayer 1991a] D. H. Mayer, “Continued fractions and related transformations”, pp. 175–222 in *Ergodic theory, symbolic dynamics, and hyperbolic spaces* (Trieste, 1989), edited by T. Bedford et al., Oxford Sci. Publ., Oxford Univ. Press, New York, 1991. MR 1130177 Zbl 0755.58034

[Mayer 1991b] D. H. Mayer, “The thermodynamic formalism approach to Selberg's zeta function for PSL(2, **Z**)”, *Bull. Amer. Math. Soc.* (*N.S.*) **25**:1 (1991), 55–60. MR 91j:58130 Zbl 0729.58041

[Mazur and Swinnerton-Dyer 1974] B. Mazur and P. Swinnerton-Dyer, “Arithmetic of Weil curves”, *Invent. Math.* **25** (1974), 1–61. MR 50 #7152 Zbl 0281.14016

[Mühlenbruch 2004] T. Mühlenbruch, “Hecke operators on period functions for the full modular group”, *Int. Math. Res. Not.* **2004**:77 (2004), 4127–4145. MR 2005k:11089 Zbl 1065.11031

[Shokurov 1980a] V. V. Shokurov, “Shimura integrals of cusp forms”, *Izv. Akad. Nauk SSSR Ser. Mat.* **44**:3 (1980), 670–718, 720. MR 82b:10029 Zbl 0444.14030

[Shokurov 1980b] V. V. Shokurov, “A study of the homology of Kuga varieties”, *Izv. Akad. Nauk SSSR Ser. Mat.* **44**:2 (1980), 443–464, 480. In Russian; translated in *Math. USSR-Izv.* **16**:2 (1981), 399–418. MR 82f:14023

[Višik and Manin 1974] M. M. Višik and Y. I. Manin, “p-adic Hecke series of imaginary quadratic fields”, *Mat. Sb.* (*N.S.*) **95(137)** (1974), 357–383, 471. In Russian; translated in *Math. USSR, Sb.* **24** (1976), 345–371. MR 51 #8078

Communicated by Peter Sarnak
Received 2010-01-12 Accepted 2010-10-01

manin@mpim-bonn.mpg.de *Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany*

Department of Mathematics, Northwestern University, Evanston, IL 60208-2730, United States

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@mathscipub.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 4 No. 8 2010